EFOS

CLI Command Reference

User Guide
Software Release 3.4.3

Broadcom, the pulse logo, Connecting everything, Avago Technologies, Avago, and the A logo are among the trademarks of Broadcom and/or its affiliates in the United States, certain other countries, and/or the EU. sFlow is a registered trademark of InMon Corporation.

Copyright © 2018 Broadcom. All Rights Reserved.

The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, please visit www.broadcom.com.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

Table of Contents

Chapter 1: Introduction 57

1.1 About Ethernet Fabric Operating System Software 57

Chapter 2: Using the Command-Line Interface 58

2.1 Command Syntax 58

2.2 Command Conventions 58

2.3 Common Parameter Values 59

2.4 Slot/Port Naming Convention 59

2.5 Using the No Form of a Command 60

2.6 Executing Show Commands 60

2.7 CLI Output Filtering 60

2.8 EFOS Modules 61

2.9 Command Modes 62

2.10 Command Completion and Abbreviation 65

2.11 CLI Error Messages 65

2.12 CLI Line-Editing Conventions 66

2.13 Using CLI Help 67

2.14 Accessing the CLI 67

Chapter 3: Management Commands 68

3.1 Network Interface Commands 68

3.1.0.1 enable (Privileged EXEC access) 68

3.1.0.2 do (Privileged EXEC commands) 68

3.1.0.3 serviceport ip 69

3.1.0.4 serviceport protocol 69

3.1.0.5 serviceport protocol dhcp 69

3.1.0.6 network parms 69

3.1.0.7 network protocol 70

3.1.0.8 network protocol dhcp 70

3.1.0.9 network mac-address 70

3.1.0.10 network mac-type 70

3.1.0.11 show network 71

3.1.0.12 show serviceport 72

3.2 IPv6 Management Commands 73

3.2.0.1 serviceport ipv6 enable 73

3.2.0.2 network ipv6 enable 73

3.2.0.3 serviceport ipv6 address 74

3.2.0.4 serviceport ipv6 gateway 74

3.2.0.5 serviceport ipv6 neighbor 75

3.2.0.6 network ipv6 neighbor 75
3.2.0.7 network ipv6 address 76
3.2.0.8 network ipv6 gateway 76
3.2.0.9 show network ipv6 neighbors 77
3.2.0.10 show serviceport ipv6 neighbors 77
3.2.0.11 show network ipv6 dhcp statistics 78
3.2.0.12 show serviceport ipv6 dhcp statistics 79
3.2.0.13 clear network ipv6 dhcp statistics 80
3.2.0.14 clear serviceport ipv6 dhcp statistics 80
3.2.0.15 ping ipv6 80
3.2.0.16 ping ipv6 interface 80
3.2.0.17 traceroute 81
3.2.0.18 traceroute ipv6 83
3.2.0.19 ipv6 dhcp relay 83
3.3 Console Port Access Commands 84
3.3.0.1 configuration 84
3.3.0.2 line 84
3.3.0.3 serial baudrate 84
3.3.0.4 serial timeout 85
3.3.0.5 show serial 85
3.4 Telnet Commands 86
3.4.0.1 ip telnet server enable 86
3.4.0.2 ip telnet port 86
3.4.0.3 telnet 86
3.4.0.4 transport input telnet 87
3.4.0.5 transport output telnet 87
3.4.0.6 session-limit 87
3.4.0.7 session-timeout 88
3.4.0.8 telnetcon maxsessions 88
3.4.0.9 telnetcon timeout 88
3.4.0.10 show telnet 89
3.4.0.11 show telnetcon 89
3.5 Secure Shell Commands 90
3.5.0.1 ip ssh 90
3.5.0.2 ip ssh port 90
3.5.0.3 ip ssh server enable 90
3.5.0.4 sshcon maxsessions 91
3.5.0.5 sshcon timeout 91
3.5.0.6 show ip ssh 91
3.6 Management Security Commands 93

3.6.0.1 crypto key generate rsa 93
3.6.0.2 crypto key generate dsa 93
3.7 Access Commands 94
3.7.0.1 disconnect 94
3.7.0.2 efos-show 94
3.7.0.3 linuxsh 94
3.7.0.4 show loginsession 94
3.7.0.5 show loginsession long 95
3.8 AAA Commands 96
3.8.0.1 aaa authentication login 96
3.8.0.2 aaa authentication enable 97
3.8.0.3 aaa authorization commands 98
3.8.0.4 authorization commands 99
3.8.0.5 enable authentication 100
3.8.0.6 aaa ias-user username 100
3.8.0.7 aaa session-id 101
3.8.0.8 aaa accounting 101
3.8.0.9 aaa accounting update 102
3.8.0.10 password (AAA IAS User Configuration) 103
3.8.0.11 clear aaa ias-users 104
3.8.0.12 show aaa ias-users 104
3.8.0.13 accounting 104
3.8.0.14 show accounting 105
3.8.0.15 show accounting methods 105
3.8.0.16 show accounting update 106
3.8.0.17 show authorization methods 106
3.8.0.18 login authentication 107
3.9 User Account and Password Commands 108
3.9.0.1 username (Global Config) 108
3.9.0.2 username name nopassword 109
3.9.0.3 username unlock 109
3.9.0.4 show users 109
3.9.0.5 show users long 110
3.9.0.6 show users accounts 110
3.9.0.7 show users login-history 111
3.9.0.8 password 111
3.9.0.9 password (Line Configuration) 111
3.9.0.10 password (User EXEC) 112
3.9.0.11 enable password 112
3.9.0.12 passwords min-length 113

3.9.0.13 passwords history 113
3.9.0.14 passwords aging 114
3.9.0.15 passwords lock-out 114
3.9.0.16 passwords strength-check 114
3.9.0.17 passwords strength maximum consecutive-characters 115
3.9.0.18 passwords strength maximum repeated-characters 115
3.9.0.19 passwords strength minimum uppercase-letters 115
3.9.0.20 passwords strength minimum lowercase-letters 115
3.9.0.21 passwords strength minimum numeric-characters 116
3.9.0.22 passwords strength minimum special-characters 116
3.9.0.23 passwords strength minimum character-classes 116
3.9.0.24 passwords strength exclude-keyword 117
3.9.0.25 show passwords configuration 117
3.9.0.26 show passwords result 117
3.10 SNMP Commands 118
3.10.0.1 snmp-server 118
3.10.0.2 snmp-server community 118
3.10.0.3 snmp-server community-group 119
3.10.0.4 snmp-server enable traps violation 119
3.10.0.5 snmp-server enable traps 120
3.10.0.6 snmp-server enable traps bgp 120
3.10.0.7 snmp-server enable traps linkmode 120
3.10.0.8 snmp-server enable traps multiusers 121
3.10.0.9 snmp-server enable traps stpmode 121
3.10.0.10 snmp-server engineID local 121
3.10.0.11 snmp-server filter 122
3.10.0.12 snmp-server group 122
3.10.0.13 snmp-server host 123
3.10.0.14 snmp-server port 124
3.10.0.15 snmp-server proxy 124
3.10.0.16 snmp-server trapsend 124
3.10.0.17 snmp-server user 125
3.10.0.18 snmp-server view 125
3.10.0.19 snmp-server v3-host 126
3.10.0.20 snmptrap source-interface 126
3.10.0.21 show snmp 127
3.10.0.22 show snmp engineID 127
3.10.0.23 show snmp filters 128
3.10.0.24 show snmp group 128
3.10.0.25 show snmp-server 128

3.10.0.26 show snmp user 129
3.10.0.27 show snmp views 129
3.10.0.28 show trapflags 129
3.10.0.29 show snmptrap source-interface 130
3.11 RADIUS Commands 130
3.11.0.1 aaa server radius dynamic-author 130
3.11.0.2 authentication command bounce-port ignore 131
3.11.0.3 auth-type 131
3.11.0.4 authorization network radius 132
3.11.0.5 clear radius dynamic-author statistics 132
3.11.0.6 client 132
3.11.0.7 debug aaa coa 133
3.11.0.8 debug aaa pod 133
3.11.0.9 ignore server-key 133
3.11.0.10 ignore session-key 133
3.11.0.11 port (Dynamic Authorization Mode) 134
3.11.0.12 radius accounting mode 134
3.11.0.13 radius server attribute 135
3.11.0.14 radius server attribute 32 include-in-access-req 136
3.11.0.15 radius server attribute 44 include-in-access-req 136
3.11.0.16 radius server deadtime 137
3.11.0.17 radius server dead-criteria 137
3.11.0.18 radius server host 138
3.11.0.19 radius server host link-local 139
3.11.0.20 radius server host test 140
3.11.0.21 radius server key 140
3.11.0.22 radius server load-balance 141
3.11.0.23 radius server msgauth 142
3.11.0.24 radius server primary 142
3.11.0.25 radius server retransmit 143
3.11.0.26 radius source-interface 143
3.11.0.27 radius server timeout 144
3.11.0.28 server-key 144
3.11.0.29 radius server vsa send 145
3.11.0.30 show radius 145
3.11.0.31 show radius servers 147
3.11.0.32 show radius accounting 149
3.11.0.33 show radius accounting servers 151
3.11.0.34 show radius accounting statistics 151
3.11.0.35 show radius source-interface 153

3.11.0.36 show radius statistics 153
3.12 TACACS+ Commands 155
3.12.0.1 tacacs-server host 155
3.12.0.2 tacacs-server host link-local 155
3.12.0.3 tacacs-server key 156
3.12.0.4 tacacs-server keystring 156
3.12.0.5 tacacs-server timeout 156
3.12.0.6 key 157
3.12.0.7 keystring 157
3.12.0.8 port (TACACS Config Mode) 157
3.12.0.9 priority 158
3.12.0.10 tacacs-server source-interface 158
3.12.0.11 timeout 158
3.12.0.12 show tacacs 159
3.12.0.13 show tacacs source-interface 159
3.13 Configuration Scripting Commands 160
3.13.0.1 script apply 160
3.13.0.2 script delete 161
3.13.0.3 script list 161
3.13.0.4 script show 161
3.13.0.5 script validate 161
3.14 Pre-login Banner, System Prompt, and Host Name Commands 162
3.14.0.1 copy (pre-login banner) 162
3.14.0.2 set prompt 162
3.14.0.3 set clibanner 162
3.14.0.4 show clibanner 162
3.14.0.5 hostname 163
3.15 Front Panel TAP Interfaces 164
3.15.0.1 fpti 164
3.15.0.2 show port fpti 164
Chapter 4: Utility Commands 166
4.1 AutoInstall Commands 166
4.1.0.1 boot autoinstall 166
4.1.0.2 boot host retrycount 167
4.1.0.3 boot host dhcp 167
4.1.0.4 boot host autosave 167
4.1.0.5 boot host autoreboot 168
4.1.0.6 erase startup-config 168
4.1.0.7 erase factory-defaults 168
4.1.0.8 erase application 168

4.1.0.9 show autoinstall 168
4.2 Application Commands 169
4.2.0.1 application install 169
4.2.0.2 application start 170
4.2.0.3 application stop 170
4.2.0.4 show application 170
4.2.0.5 show application files 170
4.3 CLI Output Filtering Commands 171
4.3.0.1 show xxx|include “string” 171
4.3.0.2 show xxx|include “string” exclude “string2” 171
4.3.0.3 show xxx|exclude “string” 171
4.3.0.4 show xxx|begin “string” 171
4.3.0.5 show xxx|section “string” 172
4.3.0.6 show xxx|section “string” “string2” 172
4.3.0.7 show xxx|section “string” include “string2” 172
4.4 Dual Image Commands 173
4.4.0.1 delete 173
4.4.0.2 boot system 173
4.4.0.3 show bootvar 173
4.4.0.4 filedescr 173
4.4.0.5 update bootcode 173
4.5 System Information and Statistics Commands 174
4.5.0.1 load-interval 174
4.5.0.2 show arp switch 174
4.5.0.3 dir 174
4.5.0.4 show eventlog 175
4.5.0.5 show hardware 175
4.5.0.6 show slot 176
4.5.0.7 environment temprange 176
4.5.0.8 environment trap 177
4.5.0.9 show environment 177
4.5.0.10 show version 177
4.5.0.11 show version bootloader 178
4.5.0.12 show platform vpd 178
4.5.0.13 show interface 179
4.5.0.14 show interfaces status 180
4.5.0.15 show interfaces traffic 180
4.5.0.16 show interface counters 182
4.5.0.17 show interface ethernet 183
4.5.0.18 show mac-addr-table 188

4.5.0.19 process cpu threshold 189
4.5.0.20 show process app-list 190
4.5.0.21 show process proc-list 190
4.5.0.22 show process app-resource-list 191
4.5.0.23 show process cpu threshold 192
4.5.0.24 show running-config 192
4.5.0.25 show running-config interface 193
4.5.0.26 show 194
4.5.0.27 show sysinfo 196
4.5.0.28 show tech-support 196
4.5.0.29 length value 197
4.5.0.30 terminal length 197
4.5.0.31 show terminal length 197
4.5.0.32 memory free low-watermark processor 198
4.5.0.33 clear mac-addr-table 198
4.6 Logging Commands 199
4.6.0.1 logging buffered 199
4.6.0.2 logging buffered wrap 199
4.6.0.3 logging cli-command 199
4.6.0.4 logging console 200
4.6.0.5 logging host 200
4.6.0.6 logging host reconfigure 201
4.6.0.7 logging host remove 201
4.6.0.8 logging persistent 201
4.6.0.9 logging protocol 201
4.6.0.10 logging syslog 202
4.6.0.11 logging syslog port 202
4.6.0.12 logging syslog source-interface 202
4.6.0.13 show logging 203
4.6.0.14 show logging buffered 204
4.6.0.15 show logging hosts 204
4.6.0.16 show logging persistent 205
4.6.0.17 show logging traplogs 205
4.6.0.18 clear logging buffered 206
4.7 Email Alerting and Mail Server Commands 207
4.7.0.1 logging email 207
4.7.0.2 logging email urgent 207
4.7.0.3 logging email message-type to-addr 207
4.7.0.4 logging email from-addr 208
4.7.0.5 logging email message-type subject 208

4.7.0.6 logging email logtime 208
4.7.0.7 logging traps 209
4.7.0.8 logging email test message-type 209
4.7.0.9 show logging email config 209
4.7.0.10 show logging email statistics 210
4.7.0.11 clear logging email statistics 210
4.7.0.12 mail-server 210
4.7.0.13 security 210
4.7.0.14 port (Mail Server Config Mode) 211
4.7.0.15 username (Mail Server Config) 211
4.7.0.16 password (Mail Server Config Mode) 211
4.7.0.17 show mail-server config 211
4.8 System Utility and Clear Commands 212
4.8.0.1 clear config 212
4.8.0.2 clear config interface 212
4.8.0.3 clear counters 212
4.8.0.4 clear ip access-list counters 212
4.8.0.5 clear ipv6 access-list counters 212
4.8.0.6 clear mac access-list counters 213
4.8.0.7 clear pass 213
4.8.0.8 clear traplog 213
4.8.0.9 clear vlan 213
4.8.0.10 clear vlan stats 213
4.8.0.11 logout 214
4.8.0.12 ping 214
4.8.0.13 quit 215
4.8.0.14 reload 215
4.8.0.15 dying-gasp 216
4.8.0.16 show dying-gasp 216
4.8.0.17 copy 217
4.8.0.18 file verify 220
4.8.0.19 write memory 221
4.8.0.20 ip scp server enable 221
4.9 Simple Network Time Protocol Commands 222
4.9.0.1 sntp broadcast client poll-interval 222
4.9.0.2 sntp client mode 222
4.9.0.3 sntp client port 223
4.9.0.4 sntp unicast client poll-interval 223
4.9.0.5 sntp unicast client poll-timeout 223
4.9.0.6 sntp unicast client poll-retry 224

4.9.0.7 sntp server 224
4.9.0.8 sntp source-interface 224
4.9.0.9 show sntp 225
4.9.0.10 show sntp client 225
4.9.0.11 show sntp server 225
4.9.0.12 show sntp source-interface 226
4.10 Time Zone Commands 227
4.10.0.1 clock set 227
4.10.0.2 clock summer-time date 227
4.10.0.3 clock summer-time recurring 228
4.10.0.4 clock timezone 228
4.10.0.5 show clock 229
4.10.0.6 show clock detail 229
4.11 DHCP Server Commands 231
4.11.0.1 ip dhcp pool 231
4.11.0.2 client-identifier 231
4.11.0.3 client-name 231
4.11.0.4 default-router 232
4.11.0.5 dns-server 232
4.11.0.6 hardware-address 232
4.11.0.7 host 233
4.11.0.8 lease 233
4.11.0.9 network (DHCP Pool Config) 233
4.11.0.10 bootfile 234
4.11.0.11 domain-name 234
4.11.0.12 domain-name enable 234
4.11.0.13 netbios-name-server 235
4.11.0.14 netbios-node-type 235
4.11.0.15 next-server 236
4.11.0.16 option 236
4.11.0.17 ip dhcp excluded-address 236
4.11.0.18 ip dhcp ping packets 237
4.11.0.19 service dhcp 237
4.11.0.20 ip dhcp bootp automatic 237
4.11.0.21 ip dhcp conflict logging 238
4.11.0.22 clear ip dhcp binding 238
4.11.0.23 clear ip dhcp server statistics 238
4.11.0.24 clear ip dhcp conflict 238
4.11.0.25 show ip dhcp binding 239
4.11.0.26 show ip dhcp global configuration 239

4.11.0.27 show ip dhcp pool configuration 239
4.11.0.28 show ip dhcp server statistics 240
4.11.0.29 show ip dhcp conflict 241
4.12 DNS Client Commands 242
4.12.0.1 ip domain lookup 242
4.12.0.2 ip domain name 242
4.12.0.3 ip domain list 242
4.12.0.4 ip name server 243
4.12.0.5 ip name source-interface 243
4.12.0.6 ip host 244
4.12.0.7 ip domain retry 244
4.12.0.8 ip domain timeout 244
4.12.0.9 clear host 245
4.12.0.10 show hosts 245
4.13 IP Address Conflict Commands 246
4.13.0.1 ip address-conflict-detect run 246
4.13.0.2 show ip address-conflict 246
4.13.0.3 clear ip address-conflict-detect 246
4.14 Serviceability Packet Tracing Commands 247
4.14.0.1 capture start 247
4.14.0.2 capture stop 247
4.14.0.3 capture file | remote | line 247
4.14.0.4 capture remote port 248
4.14.0.5 capture file size 248
4.14.0.6 capture line wrap 248
4.14.0.7 show capture packets 249
4.14.0.8 cpu-traffic direction interface 249
4.14.0.9 cpu-traffic direction match cust-filter 249
4.14.0.10 cpu-traffic direction match srcip 250
4.14.0.11 cpu-traffic direction match dstip 250
4.14.0.12 cpu-traffic direction match tcp 250
4.14.0.13 cpu-traffic direction match udp 251
4.14.0.14 cpu-traffic mode 251
4.14.0.15 cpu-traffic trace 251
4.14.0.16 show cpu-traffic 252
4.14.0.17 show cpu-traffic interface 253
4.14.0.18 show cpu-traffic summary 253
4.14.0.19 show cpu-traffic trace 253
4.14.0.20 clear cpu-traffic 254
4.14.0.21 debug aaa accounting 254

4.14.0.22 debug aaa authorization commands....254
4.14.0.23 debug arp....255
4.14.0.24 debug auto-voip....255
4.14.0.25 debug clear....255
4.14.0.26 debug console....256
4.14.0.27 debug crashlog....256
4.14.0.28 debug crashlog kernel....257
4.14.0.29 debug crashlog kernel upload....257
4.14.0.30 debug dcbx packet....257
4.14.0.31 debug debug-config....257
4.14.0.32 debug dhcp packet....258
4.14.0.33 debug dot1x packet....258
4.14.0.34 debug igmpsnooping packet....258
4.14.0.35 debug igmpsnooping packet transmit....259
4.14.0.36 debug igmpsnooping packet receive....259
4.14.0.37 debug ip acl....260
4.14.0.38 debug ip bgp....260
4.14.0.39 debug ipv6 dhcp....261
4.14.0.40 debug ipv6 ospfv3 packet....261
4.14.0.41 debug ip vrrp....262
4.14.0.42 debug isdp packet....262
4.14.0.43 debug lacp packet....263
4.14.0.44 debug mldsnooping packet....263
4.14.0.45 debug ospf packet....263
4.14.0.46 debug ping packet....265
4.14.0.47 debug sflow packet....266
4.14.0.48 debug spanning-tree bpdu....266
4.14.0.49 debug spanning-tree bpdu receive....266
4.14.0.50 debug spanning-tree bpdu transmit....267
4.14.0.51 debug tacacs....268
4.14.0.52 debug telnetd start....268
4.14.0.53 debug telnetd stop....268
4.14.0.54 debug transfer....268
4.14.0.55 debug udld events....269
4.14.0.56 debug udld packet receive....269
4.14.0.57 debug udld packet transmit....269
4.14.0.58 show debugging....269
4.14.0.59 exception core-file....270
4.14.0.60 exception dump active-port....270
4.14.0.61 exception dump filepath....271

4.14.0.62 exception dump nfs 271
4.14.0.63 exception dump tftp-server 271
4.14.0.64 exception kernel-dump 272
4.14.0.65 exception kernel-dump path 272
4.14.0.66 exception protocol 272
4.14.0.67 exception switch-chip-register 273
4.14.0.68 exception dump ftp-server 273
4.14.0.69 exception dump compression 273
4.14.0.70 exception nmi 274
4.14.0.71 show exception kernel-dump 274
4.14.0.72 show exception kernel-dump list 274
4.14.0.73 show exception kernel-dump log 274
4.14.0.74 mbuf 274
4.14.0.75 write core 275
4.14.0.76 debug exception 275
4.14.0.77 show exception 275
4.14.0.78 show exception core-dump-file 276
4.14.0.79 show exception log 276
4.14.0.80 show mbuf total 276
4.14.0.81 show msg-queue 276
4.14.0.82 debug packet-trace 277
4.14.0.83 packet-trace eth 277
4.14.0.84 packet-trace ipv4 277
4.14.0.85 packet-trace ipv6 277
4.14.0.86 packet-trace l4 277
4.14.0.87 show packet-trace ecmp 278
4.14.0.88 show packet-trace lag 278
4.14.0.89 show packet-trace packet-data 278
4.14.0.90 show packet-trace port 279
4.14.0.91 show packet-trace port eth 280
4.14.0.92 show packet-trace port ipv4 281
4.14.0.93 show packet-trace port ipv6 281
4.14.0.94 show packet-trace port tcpv4 282
4.14.0.95 show packet-trace port tcpv6 282
4.14.0.96 show packet-trace port udpv4 282
4.14.0.97 show packet-trace port udpv6 282
4.14.0.98 clear packet-trace packet-data 282
4.14.0.99 watchdog clear 283
4.14.0.100 watchdog disable 283
4.14.0.101 watchdog enable 283

4.15 BCM Shell Command 284
4.15.0.1 bcmsh 284
4.16 Cable Test Command 285
4.16.0.1 cablestatus 285
4.17 Link Debounce Commands 286
4.17.0.1 link debounce time 286
4.17.0.2 show interface debounce 286
4.18 Port Locator Commands 288
4.18.0.1 port-locator disable 288
4.18.0.2 port-locator enable 288
4.18.0.3 show port- locator 288
4.19 sFlow Commands 290
4.19.0.1 sflow receiver 290
4.19.0.2 sflow receiver owner timeout 290
4.19.0.3 sflow receiver owner notimeout 291
4.19.0.4 sflow remote-agent ip 291
4.19.0.5 sflow remote-agent monitor-session 292
4.19.0.6 sflow remote-agent port 292
4.19.0.7 sflow remote-agent source-interface 292
4.19.0.8 sflow sampler 293
4.19.0.9 sflow poller 293
4.19.0.10 sflow sampler rate 294
4.19.0.11 sflow sampler remote-agent 294
4.19.0.12 sflow source-interface 295
4.19.0.13 show sflow agent 295
4.19.0.14 show sflow pollers 296
4.19.0.15 show sflow receivers 296
4.19.0.16 show sflow remote-agents 297
4.19.0.17 show sflow remote-agents source-interface 297
4.19.0.18 show sflow samplers 298
4.19.0.19 show sflow source-interface 298
4.20 Switch Database Management Template Commands 299
4.20.0.1 sdm prefer 299
4.20.0.2 show sdm prefer 300
4.21 SFP Transceiver Commands 303
4.21.0.1 show fiber-ports optical-transceiver 303
4.21.0.2 show fiber-ports optical-transceiver-info 303
4.22 Remote Monitoring Commands 305
4.22.0.1 rmon alarm 305
4.22.0.2 rmon hcalarm 306

4.22.0.3 rmon event 307
4.22.0.4 rmon collection history 308
4.22.0.5 show rmon 308
4.22.0.6 show rmon collection history 309
4.22.0.7 show rmon events 310
4.22.0.8 show rmon history 311
4.22.0.9 show rmon log 313
4.22.0.10 show rmon statistics interfaces 314
4.22.0.11 show rmon hcalarms 315
4.23 Buffer Statistics Tracking 318
4.23.0.1 bst enable 318
4.23.0.2 bst device threshold 318
4.23.0.3 bst egress cpu-queue attach profile 318
4.23.0.4 bst egress cpu-queue create profile 319
4.23.0.5 bst egress mc-queue attach profile 319
4.23.0.6 bst egress mc-queue create profile 320
4.23.0.7 bst egress port-service-pool mc-shared create profile 320
4.23.0.8 bst egress port-service-pool uc-shared create profile 320
4.23.0.9 bst egress rqe-queue threshold 321
4.23.0.10 bst egress service-pool attach profile 321
4.23.0.11 bst egress service-pool mc-shared threshold 322
4.23.0.12 bst egress service-pool uc-shared threshold 322
4.23.0.13 bst egress uc-queue attach profile 322
4.23.0.14 bst egress uc-queue create profile 323
4.23.0.15 bst ingress pg attach profile 323
4.23.0.16 bst ingress port-pg-shared create profile 324
4.23.0.17 bst ingress port-service-pool create profile 324
4.23.0.18 bst ingress service-pool attach profile 325
4.23.0.19 bst ingress-service-pool threshold 325
4.23.0.20 bst logging 325
4.23.0.21 show bst device 326
4.23.0.22 show bst egress cpu-queue 326
4.23.0.23 show bst egress port 326
4.23.0.24 show bst egress rqe-queue 327
4.23.0.25 show bst egress service-pool 327
4.23.0.26 show bst events 327
4.23.0.27 show bst ingress port pg 328
4.23.0.28 show bst ingress port service-pool 328
4.23.0.29 show bst ingress service-pool 328
4.23.0.30 show bst status 328

4.23.0.31 show bst threshold 329
4.23.0.32 show bst threshold profiles 329
4.23.0.33 show mmu config device 330
4.23.0.34 show mmu config port 330
4.23.0.35 clear bst events 330
4.24 Statistics Application Commands 331
4.24.0.1 stats group (Global Config) 331
4.24.0.2 stats flow-based (Global Config) 332
4.24.0.3 stats flow-based reporting 333
4.24.0.4 stats group (Interface Config) 333
4.24.0.5 stats flow-based (Interface Config) 334
4.24.0.6 show stats group 334
4.24.0.7 show stats flow-based 335
4.25 In-Service Software Upgrade 337
4.25.0.1 show issu status 337
4.25.0.2 show issu status detail 337
4.26 Port and Feature Licensing Commands 339
4.26.0.1 license clear 339
4.26.0.2 debug license 339
4.26.0.3 show license file 340
4.26.0.4 show license 340
4.26.0.5 show license features 341
Chapter 5: Switching Commands 342
5.1 Port Configuration Commands 342
5.1.0.1 interface 342
5.1.0.2 auto-negotiate 342
5.1.0.3 auto-negotiate all 343
5.1.0.4 description 343
5.1.0.5 fec 343
5.1.0.6 media-type 343
5.1.0.7 mtu 344
5.1.0.8 shutdown 344
5.1.0.9 shutdown all 345
5.1.0.10 speed 345
5.1.0.11 speed all 346
5.1.0.12 show interface fec 346
5.1.0.13 show interface media-type 346
5.1.0.14 show port 347
5.1.0.15 show port description 348
5.1.0.16 hardware profile portmode 349

5.1.0.17 show interfaces hardware profile 349
5.2 Spanning Tree Protocol Commands 351
5.2.0.1 spanning-tree 351
5.2.0.2 spanning-tree auto-edge 351
5.2.0.3 spanning-tree backbonefast 351
5.2.0.4 spanning-tree cost 352
5.2.0.5 spanning-tree bpdufilter 353
5.2.0.6 spanning-tree bpdufilter default 353
5.2.0.7 spanning-tree bpduflood 353
5.2.0.8 spanning-tree bpduguard 354
5.2.0.9 spanning-tree bpdumigrationcheck 354
5.2.0.10 spanning-tree configuration name 354
5.2.0.11 spanning-tree configuration revision 355
5.2.0.12 spanning-tree edgeport 355
5.2.0.13 spanning-tree forward-time 355
5.2.0.14 spanning-tree guard 356
5.2.0.15 spanning-tree max-age 356
5.2.0.16 spanning-tree max-hops 356
5.2.0.17 spanning-tree mode 357
5.2.0.18 spanning-tree mst 357
5.2.0.19 spanning-tree mst instance 358
5.2.0.20 spanning-tree mst priority 359
5.2.0.21 spanning-tree mst vlan 359
5.2.0.22 spanning-tree port mode 359
5.2.0.23 spanning-tree port mode all 360
5.2.0.24 spanning-tree port-priority 360
5.2.0.25 spanning-tree transmit 360
5.2.0.26 spanning-tree tcnguard 361
5.2.0.27 spanning-tree uplinkfast 361
5.2.0.28 spanning-tree vlan 361
5.2.0.29 spanning-tree vlan cost 362
5.2.0.30 spanning-tree vlan forward-time 362
5.2.0.31 spanning-tree vlan hello-time 362
5.2.0.32 spanning-tree vlan max-age 363
5.2.0.33 spanning-tree vlan port-priority 363
5.2.0.34 spanning-tree vlan root 363
5.2.0.35 spanning-tree vlan priority 364
5.2.0.36 show spanning-tree 364
5.2.0.37 show spanning-tree active 365
5.2.0.38 show spanning-tree backbonefast 367

5.2.0.39 show spanning-tree brief 367
5.2.0.40 show spanning-tree interface 368
5.2.0.41 show spanning-tree mst detailed 369
5.2.0.42 show spanning-tree mst port detailed 369
5.2.0.43 show spanning-tree mst port summary 370
5.2.0.44 show spanning-tree mst port summary active 371
5.2.0.45 show spanning-tree mst summary 371
5.2.0.46 show spanning-tree summary 372
5.2.0.47 show spanning-tree uplinkfast 372
5.2.0.48 show spanning-tree vlan 373
5.3 VLAN Commands 374
5.3.0.1 vlan database 374
5.3.0.2 network mgmt_vlan 374
5.3.0.3 vlan 374
5.3.0.4 vlan acceptframe 374
5.3.0.5 vlan ingressfilter 375
5.3.0.6 vlan internal allocation 375
5.3.0.7 vlan makestatic 375
5.3.0.8 vlan name 376
5.3.0.9 vlan participation 376
5.3.0.10 vlan participation all 376
5.3.0.11 vlan port acceptframe all 377
5.3.0.12 vlan port ingressfilter all 377
5.3.0.13 vlan port pvid all 377
5.3.0.14 vlan port tagging all 378
5.3.0.15 vlan pvid 378
5.3.0.16 vlan stats 378
5.3.0.17 vlan tagging 379
5.3.0.18 show vlan 379
5.3.0.19 show vlan stats 380
5.3.0.20 show vlan internal usage 382
5.3.0.21 show vlan brief 382
5.3.0.22 show vlan port 382
5.4 Private VLAN Commands 384
5.4.0.1 switchport private-vlan 384
5.4.0.2 switchport mode private-vlan 384
5.4.0.3 private-vlan 385
5.4.0.4 show interface ethernet switchport 386
5.5 Switch Port Mode Commands 387
5.5.0.1 switchport mode 387

5.5.0.2 switchport trunk allowed vlan 387
5.5.0.3 switchport trunk native vlan 388
5.5.0.4 switchport access vlan 388
5.5.0.5 show interfaces switchport 389
5.5.0.6 show interfaces switchport 390
5.6 VLAN Mapping Commands 391
5.6.0.1 switchport mapping vlan 391
5.6.0.2 show interfaces vlan mapping 391
5.7 Double VLAN Commands 392
5.7.0.1 dvlan-tunnel ethertype (Interface Config) 392
5.7.0.2 dvlan-tunnel ethertype primary-tpid 392
5.7.0.3 mode dot1q-tunnel 393
5.7.0.4 mode dvlan-tunnel 393
5.7.0.5 show dot1q-tunnel 394
5.7.0.6 show dvlan-tunnel 394
5.8 Provisioning (IEEE 802.1p) Commands 395
5.8.0.1 vlan port priority all 395
5.8.0.2 vlan priority 395
5.9 Protected Ports Commands 396
5.9.0.1 switchport protected (Global Config) 396
5.9.0.2 switchport protected (Interface Config) 396
5.9.0.3 show switchport protected 397
5.9.0.4 show interfaces switchport 397
5.10 Port-Based Network Access Control Commands 398
5.10.0.1 aaa authentication dot1x default 398
5.10.0.2 clear dot1x statistics 398
5.10.0.3 clear radius statistics 398
5.10.0.4 dot1x eapolflood 398
5.10.0.5 authentication dynamic-vlan enable 399
5.10.0.6 authentication event no-response action authorize vlan 399
5.10.0.7 authentication event fail action authorize vlan 399
5.10.0.8 clear authentication sessions 400
5.10.0.9 dot1x max-reauth-req 400
5.10.0.10 dot1x max-req 400
5.10.0.11 authentication max-users 401
5.10.0.12 authentication periodic 401
5.10.0.13 authentication port-control 401
5.10.0.14 authentication port-control all 402
5.10.0.15 authentication host-mode 402
5.10.0.16 authentication host-mode all 403

5.10.0.17 mab 403
5.10.0.18 dot1x system-auth-control 403
5.10.0.19 authentication monitor 404
5.10.0.20 dot1x software version 404
5.10.0.21 dot1x timeout 404
5.10.0.22 dot1x user 405
5.10.0.23 authentication event server dead action 406
5.10.0.24 authentication event server dead action authorize voice 406
5.10.0.25 authentication event server alive action 407
5.10.0.26 authentication violation 407
5.10.0.27 mab request format attribute 1 407
5.10.0.28 authentication critical recovery max-reauth 408
5.10.0.29 authentication enable 409
5.10.0.30 authentication order 409
5.10.0.31 authentication priority 409
5.10.0.32 authentication timer restart 410
5.10.0.33 authentication timer reauthenticate 410
5.10.0.34 clear authentication statistics 410
5.10.0.35 clear authentication authentication-history 411
5.10.1 802.1X Supplicant Commands 412
5.10.1.1 dot1x pae 412
5.10.1.2 dot1x supplicant port-control 412
5.10.1.3 dot1x max-start 412
5.10.1.4 dot1x supplicant user 413
5.10.2 Authentication Show Commands 414
5.10.2.1 show authentication 414
5.10.2.2 show authentication authentication-history 414
5.10.2.3 show authentication clients 415
5.10.2.4 show authentication interface 416
5.10.2.5 show authentication methods 417
5.10.2.6 show authentication statistics 418
5.10.2.7 show dot1x 418
5.10.2.8 show dot1x users 421
5.10.2.9 show mab 422
5.10.3 Deprecated IEEE 802.1X Commands 423
5.11 Microsoft Active Directory Authentication Commands 424
5.11.1 Global Configuration Commands 424
5.11.1.1 ldap-server host 424
5.11.1.2 ldap authentication bind-first 424
5.11.1.3 ldap search-map 425

5.11.2 LDAP Search Map Mode Config Commands 426
5.11.2.1 userprofile attribute-name 426
5.11.2.2 no userprofile 426
5.11.3 Privileged Exec mode Config Commands 426
5.11.3.1 debug ldap 426
5.11.4 Show Commands 427
5.11.4.1 show ldap-server 427
5.11.4.2 show ldap-search-map 427
5.11.4.3 show ldap-server statistics 428
5.12 Task-based Authorization 429
5.12.0.1 usergroup 429
5.12.0.2 taskgroup 429
5.12.0.3 username usergroup 429
5.12.0.4 description (User Group Mode) 430
5.12.0.5 inherit usergroup 430
5.12.0.6 taskgroup (User Group Mode) 430
5.12.0.7 description (Task Group Mode) 430
5.12.0.8 inherit taskgroup 431
5.12.0.9 task [read] [write] [debug] [execute] 431
5.12.0.10 show aaa usergroup 432
5.12.0.11 show aaa taskgroup 432
5.12.0.12 show aaa userdb 433
5.13 Cut-Through (ASF) Commands 434
5.13.0.1 cut-through mode 434
5.13.0.2 show cut-through mode 434
5.14 Asymmetric Flow Control Commands 435
5.14.0.1 flowcontrol 435
5.14.0.2 show flowcontrol 435
5.15 Storm-Control Commands 437
5.15.0.1 storm-control broadcast 437
5.15.0.2 storm-control broadcast action 438
5.15.0.3 storm-control broadcast level 438
5.15.0.4 storm-control broadcast rate 438
5.15.0.5 storm-control multicast 439
5.15.0.6 storm-control multicast action 439
5.15.0.7 storm-control multicast level 440
5.15.0.8 storm-control multicast rate 440
5.15.0.9 storm-control unicast 441
5.15.0.10 storm-control unicast action 441
5.15.0.11 storm-control unicast level 442

5.15.0.12 storm-control unicast rate 442
5.15.0.13 show storm-control 442
5.16 Link Dependency Commands 444
5.16.0.1 link state track 444
5.16.0.2 link state group 444
5.16.0.3 link state group downstream 445
5.16.0.4 link state group upstream 445
5.16.0.5 show link state group 445
5.16.0.6 show link state group detail 446
5.17 Link Local Protocol Filtering Commands 447
5.17.0.1 llpf 447
5.17.0.2 show llpf interface all 447
5.18 MVR Commands 448
5.18.0.1 mvr 448
5.18.0.2 mvr group 448
5.18.0.3 mvr immediate 448
5.18.0.4 mvr mode 449
5.18.0.5 mvr querytime 449
5.18.0.6 mvr type 449
5.18.0.7 mvr vlan 449
5.18.0.8 mvr vlan group 450
5.18.0.9 show mvr 450
5.18.0.10 show mvr members 450
5.18.0.11 show mvr interface 451
5.18.0.12 show mvr traffic 451
5.18.0.13 debug mvr trace 452
5.18.0.14 debug mvr packet 452
5.19 Port-Channel/LAG (802.3ad) Commands 453
5.19.0.1 port-channel 453
5.19.0.2 addport 453
5.19.0.3 deleteport (Interface Config) 453
5.19.0.4 deleteport (Global Config) 454
5.19.0.5 lacp admin key 454
5.19.0.6 lacp collector max-delay 454
5.19.0.7 lacp actor admin key 454
5.19.0.8 lacp actor admin state 455
5.19.0.9 lacp actor port priority 455
5.19.0.10 lacp partner admin key 456
5.19.0.11 lacp partner admin state 456
5.19.0.12 lacp partner port id 456

5.19.0.13 lacp partner port priority 457
5.19.0.14 lacp partner system-id 457
5.19.0.15 lacp partner system priority 457
5.19.0.16 interface lag 458
5.19.0.17 ip resilient-hashing 458
5.19.0.18 port-channel resilient-hashing 458
5.19.0.19 port-channel static 459
5.19.0.20 port lacpmode 459
5.19.0.21 port lacpmode enable all 459
5.19.0.22 port lacptimeout (Interface Config) 460
5.19.0.23 port lacptimeout (Global Config) 460
5.19.0.24 port-channel adminmode 461
5.19.0.25 port-channel linktrap 461
5.19.0.26 port-channel load-balance 461
5.19.0.27 port-channel min-links 462
5.19.0.28 port-channel name 462
5.19.0.29 port-channel system priority 462
5.19.0.30 show hashdest 463
5.19.0.31 show ip resilient-hashing 464
5.19.0.32 show lacp actor 465
5.19.0.33 show lacp partner 465
5.19.0.34 show port-channel brief 465
5.19.0.35 show port-channel 466
5.19.0.36 show port-channel counters 467
5.19.0.37 show port-channel resilient-hashing 468
5.19.0.38 show port-channel system priority 468
5.19.0.39 clear port-channel counters 468
5.19.0.40 clear port-channel all counters 468
5.20 VPC Commands 469
5.20.0.1 vpc domain 469
5.20.0.2 feature vpc 469
5.20.0.3 peer detection enable 470
5.20.0.4 peer detection interval 470
5.20.0.5 peer-keepalive destination 470
5.20.0.6 peer-keepalive enable 471
5.20.0.7 peer-keepalive timeout 471
5.20.0.8 role priority 471
5.20.0.9 system-mac 472
5.20.0.10 system-priority 472
5.20.0.11 vpc 473

5.20.0.12 vpc peer-link 473
5.20.0.13 show running-config vpc 473
5.20.0.14 show vpc 474
5.20.0.15 show vpc brief 474
5.20.0.16 show vpc consistency-parameters 475
5.20.0.17 show vpc peer-keepalive 477
5.20.0.18 show vpc role 477
5.20.0.19 show vpc statistics 478
5.20.0.20 clear vpc statistics 479
5.20.0.21 debug vpc peer-keepalive 479
5.20.0.22 debug vpc peer-link data-message 479
5.20.0.23 debug vpc peer-link control-message async 479
5.20.0.24 debug vpc peer-link control-message bulk 479
5.20.0.25 debug vpc peer-link control-message ckpt 479
5.20.0.26 debug vpc peer detection 480
5.21 Port Mirroring 481
5.21.0.1 monitor session source 481
5.21.0.2 monitor session destination 482
5.21.0.3 monitor session filter 483
5.21.0.4 monitor session mode 483
5.21.0.5 no monitor session 484
5.21.0.6 no monitor 484
5.21.0.7 remote-span 485
5.21.0.8 show monitor session 485
5.21.0.9 show vlan remote-span 488
5.21.0.10 monitor session type erspan-source 488
5.21.0.11 monitor session type erspan-destination 488
5.22 Encapsulated Remote Switched Port Analyzer Commands 490
5.22.1 ERSPAN Destination Configuration Commands 490
5.22.1.1 source 490
5.22.1.2 destination 490
5.22.1.3 ip address 491
5.22.1.4 erspan-id 491
5.22.1.5 origin ip address 491
5.22.1.6 ip ttl 492
5.22.1.7 ip dscp 492
5.22.1.8 ip prec 492
5.22.1.9 reflector-port 493
5.22.2 ERSPAN Source Configuration Commands 493
5.22.2.1 destination interface 493

5.22.2.2 source 493
5.22.2.3 ip address 494
5.22.2.4 erspan-id 494
5.23 Static MAC Filtering 495
5.23.0.1 macfilter 495
5.23.0.2 macfilter adddest 495
5.23.0.3 macfilter adddest all 496
5.23.0.4 macfilter addsrc 496
5.23.0.5 macfilter addsrc all 497
5.23.0.6 show mac-address-table static 497
5.23.0.7 show mac-address-table staticfiltering 497
5.24 DHCP L2 Relay Agent Commands 499
5.24.0.1 dhcp l2relay 499
5.24.0.2 dhcp l2relay circuit-id subscription-name 499
5.24.0.3 dhcp l2relay circuit-id vlan 499
5.24.0.4 dhcp l2relay remote-id subscription-name 500
5.24.0.5 dhcp l2relay remote-id vlan 500
5.24.0.6 dhcp l2relay subscription-name 501
5.24.0.7 dhcp l2relay trust 501
5.24.0.8 dhcp l2relay vlan 502
5.24.0.9 show dhcp l2relay all 502
5.24.0.10 show dhcp l2relay circuit-id vlan 502
5.24.0.11 show dhcp l2relay interface 503
5.24.0.12 show dhcp l2relay remote-id vlan 503
5.24.0.13 show dhcp l2relay stats interface 503
5.24.0.14 show dhcp l2relay subscription interface 504
5.24.0.15 show dhcp l2relay agent-option vlan 504
5.24.0.16 show dhcp l2relay vlan 504
5.24.0.17 clear dhcp l2relay statistics interface 505
5.25 DHCP Client Commands 506
5.25.0.1 dhcp client vendor-id-option 506
5.25.0.2 dhcp client vendor-id-option-string 506
5.25.0.3 show dhcp client vendor-id-option 506
5.26 DHCP Snooping Configuration Commands 507
5.26.0.1 ip dhcp snooping 507
5.26.0.2 ip dhcp snooping vlan 507
5.26.0.3 ip dhcp snooping verify mac-address 507
5.26.0.4 ip dhcp snooping database 508
5.26.0.5 ip dhcp snooping database write-delay 508
5.26.0.6 ip dhcp snooping binding 508

5.26.0.7 ip verify binding 508
5.26.0.8 ip dhcp snooping limit 509
5.26.0.9 ip dhcp snooping log-invalid 509
5.26.0.10 ip dhcp snooping trust 509
5.26.0.11 ip verify source 510
5.26.0.12 show ip dhcp snooping 510
5.26.0.13 show ip dhcp snooping binding 511
5.26.0.14 show ip dhcp snooping database 511
5.26.0.15 show ip dhcp snooping interfaces 512
5.26.0.16 show ip dhcp snooping statistics 512
5.26.0.17 clear ip dhcp snooping binding 513
5.26.0.18 clear ip dhcp snooping statistics 513
5.26.0.19 show ip verify source 513
5.26.0.20 show ip verify interface 514
5.26.0.21 show ip source binding 514
5.27 Dynamic ARP Inspection Commands 516
5.27.0.1 ip arp inspection vlan 516
5.27.0.2 ip arp inspection validate 516
5.27.0.3 ip arp inspection validate interface 517
5.27.0.4 ip arp inspection vlan logging 517
5.27.0.5 ip arp inspection trust 517
5.27.0.6 ip arp inspection limit 518
5.27.0.7 ip arp inspection filter 518
5.27.0.8 arp access-list 518
5.27.0.9 deny ip host mac host 519
5.27.0.10 permit ip host mac host 519
5.27.0.11 show ip arp inspection 519
5.27.0.12 show ip arp inspection statistics 520
5.27.0.13 clear ip arp inspection statistics 521
5.27.0.14 show ip arp inspection interfaces 521
5.27.0.15 show arp access-list 522
5.28 IGMP Snooping Configuration Commands 523
5.28.0.1 set igmp 523
5.28.0.2 set igmp header-validation 523
5.28.0.3 set igmp interfacemode 524
5.28.0.4 set igmp fast-leave 524
5.28.0.5 set igmp groupmembership-interval 525
5.28.0.6 set igmp maxresponse 525
5.28.0.7 set igmp mcrtrexpiretime 526
5.28.0.8 set igmp mrouter 526

5.28.0.9 set igmp mrouter interface 526
5.28.0.10 set igmp report-suppression 527
5.28.0.11 show igmpsnooping 527
5.28.0.12 show igmpsnooping mrouter interface 528
5.28.0.13 show igmpsnooping mrouter vlan 529
5.28.0.14 show igmpsnooping ssm 529
5.28.0.15 show mac-address-table igmpsnooping 529
5.29 IGMP Snooping Querier Commands 530
5.29.0.1 set igmp querier 530
5.29.0.2 set igmp querier query-interval 530
5.29.0.3 set igmp querier timer expiry 531
5.29.0.4 set igmp querier version 531
5.29.0.5 set igmp querier election participate 531
5.29.0.6 show igmpsnooping querier 532
5.30 MLD Snooping Commands 534
5.30.0.1 set mld 534
5.30.0.2 set mld interfacemode 534
5.30.0.3 set mld fast-leave 535
5.30.0.4 set mld groupmembership-interval 535
5.30.0.5 set mld maxresponse 536
5.30.0.6 set mld mcrtexpiretime 536
5.30.0.7 set mld mrouter 537
5.30.0.8 set mld mrouter interface 537
5.30.0.9 show mldsnooping 537
5.30.0.10 show mldsnooping mrouter interface 538
5.30.0.11 show mldsnooping mrouter vlan 538
5.30.0.12 show mldsnooping ssm entries 539
5.30.0.13 show mldsnooping ssm stats 539
5.30.0.14 show mldsnooping ssm groups 539
5.30.0.15 show mac-address-table mldsnooping 540
5.30.0.16 clear mldsnooping 540
5.31 MLD Snooping Querier Commands 541
5.31.0.1 set mld querier 541
5.31.0.2 set mld querier query_interval 541
5.31.0.3 set mld querier timer expiry 542
5.31.0.4 set mld querier election participate 542
5.31.0.5 show mldsnooping querier 542
5.32 Port Security Commands 544
5.32.0.1 port-security 544
5.32.0.2 port-security max-dynamic 544

5.32.0.3 port-security max-static 544
5.32.0.4 port-security mac-address 545
5.32.0.5 port-security mac-address move 545
5.32.0.6 port-security mac-address sticky 545
5.32.0.7 mac-address-table limit 546
5.32.0.8 show port-security 547
5.32.0.9 show port-security dynamic 547
5.32.0.10 show port-security static 547
5.32.0.11 show port-security violation 548
5.32.0.12 show mac-address-table limit 548
5.33 LLDP (802.1AB) Commands 550
5.33.0.1 lldp transmit 550
5.33.0.2 lldp receive 550
5.33.0.3 lldp timers 550
5.33.0.4 lldp transmit-tlv 551
5.33.0.5 lldp transmit-mgmt 551
5.33.0.6 lldp notification 551
5.33.0.7 lldp notification-interval 552
5.33.0.8 clear lldp statistics 552
5.33.0.9 clear lldp remote-data 552
5.33.0.10 show lldp 552
5.33.0.11 show lldp interface 553
5.33.0.12 show lldp statistics 553
5.33.0.13 show lldp remote-device 554
5.33.0.14 show lldp remote-device detail 555
5.33.0.15 show lldp local-device 556
5.33.0.16 show lldp local-device detail 556
5.34 LLDP-MED Commands 557
5.34.0.1 lldp med 557
5.34.0.2 lldp med confignotification 557
5.34.0.3 lldp med transmit-tlv 557
5.34.0.4 lldp med all 558
5.34.0.5 lldp med confignotification all 558
5.34.0.6 lldp med faststartrepeatcount 558
5.34.0.7 lldp med transmit-tlv all 559
5.34.0.8 show lldp med 559
5.34.0.9 show lldp med interface 559
5.34.0.10 show lldp med local-device detail 560
5.34.0.11 show lldp med remote-device 561
5.34.0.12 show lldp med remote-device detail 562

5.35 Denial of Service Commands 564
5.35.0.1 dos-control all 564
5.35.0.2 dos-control sipdip 565
5.35.0.3 dos-control firstfrag 565
5.35.0.4 dos-control tcpfrag 565
5.35.0.5 dos-control tcpflag 566
5.35.0.6 dos-control l4port 566
5.35.0.7 dos-control icmp 566
5.35.0.8 dos-control smacdmac 567
5.35.0.9 dos-control tcpport 567
5.35.0.10 dos-control udpport 568
5.35.0.11 dos-control tcpflagseq 568
5.35.0.12 dos-control tcpoffset 568
5.35.0.13 dos-control tcpsyn 569
5.35.0.14 dos-control tcpsynfin 569
5.35.0.15 dos-control tcpfinurgpsh 570
5.35.0.16 dos-control icmpv4 570
5.35.0.17 dos-control icmpv6 571
5.35.0.18 dos-control icmpfrag 571
5.35.0.19 show dos-control 571
5.36 MAC Database Commands 573
5.36.0.1 bridge aging-time 573
5.36.0.2 show forwardingdb agetime 573
5.36.0.3 show mac-address-table multicast 573
5.36.0.4 show mac-address-table stats 574
5.37 ISDP Commands 575
5.37.0.1 isdp run 575
5.37.0.2 isdp holdtime 575
5.37.0.3 isdp timer 575
5.37.0.4 isdp advertise-v2 575
5.37.0.5 isdp enable 576
5.37.0.6 clear isdp counters 576
5.37.0.7 clear isdp table 576
5.37.0.8 show isdp 576
5.37.0.9 show isdp interface 577
5.37.0.10 show isdp entry 577
5.37.0.11 show isdp neighbors 577
5.37.0.12 show isdp traffic 578
5.38 Unidirectional Link Detection Commands 580
5.38.0.1 udld enable (Global Config) 580

5.38.0.2 udld message time 580
5.38.0.3 udld timeout interval 580
5.38.0.4 udld enable (Interface Config) 580
5.38.0.5 udld port 581
5.38.0.6 udld reset 581
5.38.0.7 show udld 581
5.38.0.8 show udld slot/port 582
5.39 Interface Error Disable and Auto Recovery 583
5.39.0.1 errdisable recovery cause 583
5.39.0.2 errdisable recovery interval 583
5.39.0.3 show errdisable recovery 584
5.39.0.4 show interfaces status err-disabled 584
Chapter 6: Data Center Commands 586
6.1 Data Center Bridging Exchange Protocol Commands 586
6.1.0.1 lldp dcbx version 586
6.1.0.2 lldp tlv-select dcbxp 587
6.1.0.3 lldp dcbx port-role 587
6.1.0.4 show lldp tlv-select 588
6.1.0.5 show lldp dcbx interface 588
6.2 Quantized Congestion Notification Commands 591
6.2.0.1 qcn enable 591
6.2.0.2 qcn cnm-transmit-priority 591
6.2.0.3 qcn cnpv-priority (datacenter bridging config) 592
6.2.0.4 qcn cnpv-priority alternate-priority 592
6.2.0.5 qcn cnpv-priority cp-creation 593
6.2.0.6 qcn cnpv-priority defense-mode-choice 593
6.2.0.7 qcn cnpv-priority 593
6.2.0.8 qcn cnpv-priority alternate-priority 594
6.2.0.9 qcn transmit-tlv enable 594
6.2.0.10 clear qcn statistics 595
6.2.0.11 show qcn priority 595
6.2.0.12 show qcn active priority 598
6.2.0.13 show qcn interface 598
6.2.0.14 show qcn statistics 599
6.3 Enhanced Transmission Selection Commands 600
6.3.0.1 classofservice traffic-class-group 600
6.3.0.2 traffic-class-group max-bandwidth 600
6.3.0.3 traffic-class-group min-bandwidth 601
6.3.0.4 traffic-class-group strict 602
6.3.0.5 traffic-class-group weight 603

6.3.0.6 show classofservice traffic-class-group 603
6.3.0.7 show interfaces traffic-class-group 604
6.4 FIP Snooping Commands 605
6.4.0.1 feature fip-snooping 605
6.4.0.2 fip-snooping enable 606
6.4.0.3 fip-snooping fc-map 606
6.4.0.4 fip-snooping port-mode 607
6.4.0.5 show fip-snooping 608
6.4.0.6 show fip-snooping enode 609
6.4.0.7 show fip-snooping fcf 610
6.4.0.8 show fip-snooping sessions 612
6.4.0.9 show fip-snooping statistics 614
6.4.0.10 show fip-snooping vlan 618
6.4.0.11 clear fip-snooping statistics 618
6.5 Priority-Based Flow Control Commands 620
6.5.0.1 priority-flow-control mode 620
6.5.0.2 priority-flow-control priority 621
6.5.0.3 clear priority-flow-control statistics 621
6.5.0.4 show interface priority-flow-control 622
6.6 OpenFlow Commands 624
6.6.0.1 openflow enable 624
6.6.0.2 openflow static-ip 624
6.6.0.3 openflow controller 625
6.6.0.4 openflow default-table 625
6.6.0.5 openflow ip-mode 625
6.6.0.6 openflow passive-mode 626
6.6.0.7 openflow variant 626
6.6.0.8 clear openflow ca-cert 626
6.6.0.9 show openflow 626
6.6.0.10 show openflow configured controller 627
6.6.0.11 show openflow installed flows 628
6.6.0.12 show openflow installed groups 630
6.6.0.13 show openflow table-status 631
6.7 MPLS Commands 633
6.7.0.1 mplsd bgp-advertise 633
6.7.0.2 mplsd lfdb ipv4 633
6.7.0.3 mplsd lfdb ipv6 633
6.7.0.4 mplsd lfdb layer-2 634
6.7.0.5 mplsd bgp-mpls-label 634
6.7.0.6 ipv6 mplsd bgp-mpls-label 634

6.7.0.7 clear counters mplsd 635
6.7.0.8 debug mplsd packet-capture 635
6.7.0.9 show mplsd 635
6.7.0.10 show mplsd lfdb 637
6.7.0.11 show mplsd interface 638
6.7.0.12 show mplsd tunnels 638
6.8 NVGRE/VXLAN Commands 640
6.8.0.1 nvgre enable 640
6.8.0.2 nvgre nve 640
6.8.0.3 nvgre source-ip 641
6.8.0.4 nvgre tenant-system 641
6.8.0.5 nvgre vlan 642
6.8.0.6 vxlan enable 643
6.8.0.7 vxlan source-ip 643
6.8.0.8 vxlan tenant-system 644
6.8.0.9 vxlan udp-dst-port 644
6.8.0.10 vxlan vlan 645
6.8.0.11 vxlan vtep 645
6.8.0.12 clear counters nvgre 646
6.8.0.13 clear counters vxlan 646
6.8.0.14 show nvgre 647
6.8.0.15 show nvgre nve 648
6.8.0.16 show nvgre tenant-systems 648
6.8.0.17 show nvgre tenant-systems all 649
6.8.0.18 show vxlan 650
6.8.0.19 show vxlan tenant-systems 651
6.8.0.20 show vxlan tenant-systems all 652
6.8.0.21 show vxlan vtep 653
Chapter 7: IPv4 Routing Commands 655
7.1 Address Resolution Protocol Commands 655
7.1.0.1 arp 655
7.1.0.2 arp cachesize 655
7.1.0.3 arp dynamicrenew 656
7.1.0.4 arp purge 656
7.1.0.5 resptime 657
7.1.0.6 arp retries 657
7.1.0.7 arp timeout 657
7.1.0.8 clear arp-cache 658
7.1.0.9 clear arp-switch 658
7.1.0.10 show arp 658

7.1.0.11 show arp brief 659
7.1.0.12 show arp switch 659
7.2 IP Routing Commands 660
7.2.0.1 routing 660
7.2.0.2 ip routing 660
7.2.0.3 ip address 660
7.2.0.4 ip address dhcp 661
7.2.0.5 ip default-gateway 662
7.2.0.6 ip load-sharing 662
7.2.0.7 ip ipsec-load-sharing spi 663
7.2.0.8 release dhcp 663
7.2.0.9 renew dhcp 663
7.2.0.10 renew dhcp network-port 663
7.2.0.11 renew dhcp service-port 664
7.2.0.12 ip route 664
7.2.0.13 ip route default 666
7.2.0.14 ip route distance 666
7.2.0.15 ip route net-prototype 666
7.2.0.16 ip route static bfd interface 667
7.2.0.17 ip netdirbcast 668
7.2.0.18 ip mtu 668
7.2.0.19 ip unnumbered gratuitous-arp accept 669
7.2.0.20 ip unnumbered loopback 669
7.2.0.21 encapsulation 669
7.2.0.22 show dhcp lease 670
7.2.0.23 show ip brief 670
7.2.0.24 show ip interface 671
7.2.0.25 show ip interface brief 673
7.2.0.26 show ip load-sharing 673
7.2.0.27 show ip protocols 673
7.2.0.28 show ip route 676
7.2.0.29 show ip route ecmp-groups 679
7.2.0.30 show ip route hw-failure 680
7.2.0.31 show ip route net-prototype 680
7.2.0.32 show ip route static bfd 681
7.2.0.33 show ip route summary 681
7.2.0.34 clear ip route counters 683
7.2.0.35 show ip route preferences 683
7.2.0.36 show ip stats 684
7.2.0.37 show routing heap summary 684

7.2.1 IP Event Dampening Commands 686
7.2.1.1 dampening 686
7.2.1.2 show dampening interface 686
7.2.1.3 show interface dampening 686
7.3 Unicast Reverse Path Forwarding Commands 688
7.3.0.1 system urpf enable 688
7.3.0.2 ip verify unicast source reachable-via 688
7.4 Black Hole Detection Commands 690
7.4.0.1 bhd enable 690
7.4.0.2 bhd spine-port enable 690
7.4.0.3 show bhd status 690
7.5 Policy-Based Routing Commands 692
7.5.0.1 ip policy 692
7.5.0.2 route-map 693
7.5.0.3 match ip address <access-list-number | access-list-name> 693
7.5.0.4 match length 696
7.5.0.5 match mac-list 696
7.5.0.6 set interface 697
7.5.0.7 set ip next-hop 698
7.5.0.8 set ip default next-hop 698
7.5.0.9 set ip precedence 699
7.5.0.10 show ip policy 699
7.5.0.11 show route-map 700
7.6 Router Discovery Protocol Commands 703
7.6.0.1 ip irdp 703
7.6.0.2 ip irdp address 703
7.6.0.3 ip irdp holdtime 703
7.6.0.4 ip irdp maxadvertinterval 704
7.6.0.5 ip irdp minadvertinterval 704
7.6.0.6 ip irdp preference 704
7.6.0.7 show ip irdp 705
7.7 Virtual Router Commands 706
7.7.0.1 ip vrf 706
7.7.0.2 maximum routes 706
7.7.0.3 description 707
7.7.0.4 ip vrf forwarding 707
7.7.0.5 show ip vrf 708
7.8 Virtual LAN Routing Commands 710
7.8.0.1 vlan routing 710
7.8.0.2 interface vlan 711

7.8.0.3 show ip vlan 712
7.9 Virtual Router Redundancy Protocol Commands 713
7.9.0.1 ip vrrp (Global Config) 713
7.9.0.2 ip vrrp (Interface Config) 713
7.9.0.3 ip vrrp mode 713
7.9.0.4 ip vrrp ip 714
7.9.0.5 ip vrrp accept-mode 714
7.9.0.6 ip vrrp authentication 714
7.9.0.7 ip vrrp preempt 715
7.9.0.8 ip vrrp priority 715
7.9.0.9 ip vrrp timers advertise 716
7.9.0.10 ip vrrp track interface 716
7.9.0.11 ip vrrp track ip route 716
7.9.0.12 show ip vrrp interface stats 717
7.9.0.13 show ip vrrp 718
7.9.0.14 show ip vrrp interface 718
7.9.0.15 show ip vrrp interface brief 719
7.10 VRRPv3 Commands 720
7.10.0.1 fhrp version vrrp v3 720
7.10.0.2 snmp-server enable traps vrrp 720
7.10.0.3 vrrp 721
7.10.0.4 preempt 721
7.10.0.5 accept-mode 722
7.10.0.6 priority 722
7.10.0.7 timers advertise 722
7.10.0.8 shutdown (VRRP Group Configuration) 723
7.10.0.9 address 723
7.10.0.10 track interface 724
7.10.0.11 track ip route 725
7.10.0.12 clear vrrp statistics 725
7.10.0.13 show vrrp 726
7.10.0.14 show vrrp brief 730
7.10.0.15 show vrrp statistics 731
7.11 DHCP and BOOTP Relay Commands 732
7.11.0.1 bootpdhcprelay cidoptmode 732
7.11.0.2 bootpdhcprelay maxhopcount 732
7.11.0.3 bootpdhcprelay minwaittime 732
7.11.0.4 show bootpdhcprelay 733
7.11.0.5 show ip bootpdhcprelay 733
7.12 IP Helper Commands 734

7.12.0.1 clear ip helper statistics 735
7.12.0.2 ip helper-address (Global Config) 735
7.12.0.3 ip helper-address (Interface Config) 736
7.12.0.4 ip helper enable 738
7.12.0.5 show ip helper-address 738
7.12.0.6 show ip helper statistics 739
7.13 Open Shortest Path First Commands 741
7.13.1 General OSPF Commands 741
7.13.1.1 router ospf 741
7.13.1.2 enable (OSPF) 741
7.13.1.3 network area (OSPF) 741
7.13.1.4 1583compatibility 742
7.13.1.5 area default-cost (OSPF) 742
7.13.1.6 area nssa (OSPF) 742
7.13.1.7 area nssa default-info-originate (OSPF) 742
7.13.1.8 area nssa no-redistribute (OSPF) 743
7.13.1.9 area nssa no-summary (OSPF) 743
7.13.1.10 area nssa translator-role (OSPF) 743
7.13.1.11 area nssa translator-stab-intv (OSPF) 744
7.13.1.12 area range (OSPF) 744
7.13.1.13 area stub (OSPF) 745
7.13.1.14 area stub no-summary (OSPF) 745
7.13.1.15 area virtual-link (OSPF) 746
7.13.1.16 area virtual-link authentication 746
7.13.1.17 area virtual-link dead-interval (OSPF) 746
7.13.1.18 area virtual-link hello-interval (OSPF) 747
7.13.1.19 area virtual-link retransmit-interval (OSPF) 747
7.13.1.20 area virtual-link transmit-delay (OSPF) 747
7.13.1.21 auto-cost (OSPF) 748
7.13.1.22 capability opaque 748
7.13.1.23 clear ip ospf 749
7.13.1.24 clear ip ospf configuration 749
7.13.1.25 clear ip ospf counters 749
7.13.1.26 clear ip ospf neighbor 749
7.13.1.27 clear ip ospf neighbor interface 749
7.13.1.28 clear ip ospf redistribution 749
7.13.1.29 default-information originate (OSPF) 750
7.13.1.30 default-metric (OSPF) 750
7.13.1.31 distance ospf (OSPF) 750
7.13.1.32 distribute-list out (OSPF) 751

7.13.1.33 exit-overflow-interval (OSPF) 751
7.13.1.34 external-lsdb-limit (OSPF) 751
7.13.1.35 log-adjacency-changes 752
7.13.1.36 prefix-suppression (Router OSPF Config) 752
7.13.1.37 prefix-suppression (Router OSPFv3 Config) 752
7.13.1.38 router-id (OSPF) 753
7.13.1.39 redistribute (OSPF) 753
7.13.1.40 maximum-paths (OSPF) 753
7.13.1.41 passive-interface default (OSPF) 754
7.13.1.42 passive-interface (OSPF) 754
7.13.1.43 timers pacing flood 754
7.13.1.44 timers pacing lsa-group 755
7.13.1.45 timers spf 755
7.13.1.46 trapflags (OSPF) 755
7.13.2 OSPF Interface Commands 758
7.13.2.1 ip ospf area 758
7.13.2.2 bandwidth 758
7.13.2.3 ip ospf authentication 758
7.13.2.4 ip ospf cost 759
7.13.2.5 ip ospf database-filter all out 759
7.13.2.6 ip ospf dead-interval 759
7.13.2.7 ip ospf hello-interval 760
7.13.2.8 ip ospf network 760
7.13.2.9 ip ospf prefix-suppression 760
7.13.2.10 ip ospf priority 761
7.13.2.11 ip ospf retransmit-interval 761
7.13.2.12 ip ospf transmit-delay 762
7.13.2.13 ip ospf mtu-ignore 762
7.13.3 OSPF Graceful Restart Commands 763
7.13.3.1 nsf 763
7.13.3.2 nsf restart-interval 763
7.13.3.3 nsf helper 764
7.13.3.4 nsf ietf helper disable 764
7.13.3.5 nsf helper strict-lsa-checking 765
7.13.4 OSPFv2 Stub Router Commands 765
7.13.4.1 max-metric router-lsa 765
7.13.4.2 clear ip ospf stub-router 766
7.13.5 OSPF Show Commands 767
7.13.5.1 show ip ospf 767
7.13.5.2 show ip ospf abr 770

7.13.5.3 show ip ospf area 770
7.13.5.4 show ip ospf asbr 771
7.13.5.5 show ip ospf database 772
7.13.5.6 show ip ospf database database-summary 773
7.13.5.7 show ip ospf interface 773
7.13.5.8 show ip ospf interface brief 775
7.13.5.9 show ip ospf interface stats 775
7.13.5.10 show ip ospf lsa-group 777
7.13.5.11 show ip ospf neighbor 777
7.13.5.12 show ip ospf range 779
7.13.5.13 show ip ospf statistics 780
7.13.5.14 show ip ospf stub table 781
7.13.5.15 show ip ospf traffic 781
7.13.5.16 show ip ospf virtual-link 782
7.13.5.17 show ip ospf virtual-link brief 783
7.14 ICMP Throttling Commands 784
7.14.0.1 ip unreachables 784
7.14.0.2 ip redirects 784
7.14.0.3 ipv6 redirects 784
7.14.0.4 ip icmp echo-reply 785
7.14.0.5 ip icmp error-interval 785
7.15 Bidirectional Forwarding Detection Commands 786
7.15.0.1 bfd 786
7.15.0.2 feature bfd 786
7.15.0.3 bfd echo 787
7.15.0.4 bfd interval 787
7.15.0.5 bfd slow-timer 788
7.15.0.6 ip ospf bfd 788
7.15.0.7 neighbor fall-over bfd 789
7.15.0.8 show bfd neighbors 789
7.15.0.9 debug bfd event 791
7.15.0.10 debug bfd packet 791
7.16 IP Service Level Agreement Commands 791
7.16.0.1 ip sla 791
7.16.0.2 ip sla schedule 792
7.16.0.3 track ip sla 793
7.16.1 Track Configuration Mode Commands 794
7.16.1.1 delay 794
7.16.2 IP SLA Configuration Mode Commands 795
7.16.2.1 icmp-echo 795

7.16.3 IP SLA ICMP ECHO Configuration Mode Commands 796
7.16.3.1 frequency 796
7.16.3.2 timeout 797
7.16.3.3 threshold 798
7.16.3.4 vrf (IP SLA) 799
7.16.4 Clear Commands 799
7.16.4.1 clear ip sla statistics 799
7.16.5 Show Commands 800
7.16.5.1 show ip sla configuration 800
7.16.5.2 show ip sla statistics 800
7.16.5.3 show ip route track-table 801
7.16.5.4 show ipv6 route track-table 801
7.16.5.5 show track 802
Chapter 8: IPv6 Routing Commands 804
8.1 Loopback Interface Commands 804
8.1.0.1 interface loopback 804
8.1.0.2 show interface loopback 804
8.2 Tunnel Interface Commands 806
8.2.0.1 interface tunnel 806
8.2.0.2 tunnel source 806
8.2.0.3 tunnel destination 806
8.2.0.4 tunnel mode ipv6ip 806
8.2.0.5 show interface tunnel 807
8.3 IPv6 Routing Commands 808
8.3.0.1 ipv6 hop-limit 808
8.3.0.2 ipv6 unicast-routing 808
8.3.0.3 ipv6 enable 808
8.3.0.4 ipv6 address 809
8.3.0.5 ipv6 address autoconfig 809
8.3.0.6 ipv6 address dhcp 810
8.3.0.7 ipv6 route 810
8.3.0.8 ipv6 route distance 811
8.3.0.9 ipv6 route net-prototype 812
8.3.0.10 ipv6 route static bfd interface 812
8.3.0.11 ipv6 mtu 813
8.3.0.12 ipv6 nd dad attempts 813
8.3.0.13 ipv6 nd managed-config-flag 814
8.3.0.14 ipv6 nd ns-interval 814
8.3.0.15 ipv6 nd other-config-flag 814
8.3.0.16 ipv6 nd ra-interval 815

8.3.0.17 ipv6 nd raguard attach-policy 815
8.3.0.18 ipv6 nd ra-lifetime 815
8.3.0.19 ipv6 nd ra hop-limit unspecified 816
8.3.0.20 ipv6 nd reachable-time 816
8.3.0.21 ipv6 nd router-preference 816
8.3.0.22 ipv6 nd suppress-ra 817
8.3.0.23 ipv6 nd prefix 817
8.3.0.24 ipv6 neighbor 818
8.3.0.25 ipv6 neighbors dynamicrenew 818
8.3.0.26 ipv6 nud 818
8.3.0.27 ipv6 prefix-list 819
8.3.0.28 ipv6 unreachables 820
8.3.0.29 ipv6 unresolved-traffic 820
8.3.0.30 ipv6 icmp error-interval 821
8.3.0.31 show ipv6 brief 821
8.3.0.32 show ipv6 interface 822
8.3.0.33 show ipv6 dhcp interface 824
8.3.0.34 show ipv6 nd raguard policy 825
8.3.0.35 show ipv6 neighbors 825
8.3.0.36 clear ipv6 neighbors 826
8.3.0.37 show ipv6 protocols 826
8.3.0.38 show ipv6 route 828
8.3.0.39 show ipv6 route ecmp-groups 830
8.3.0.40 show ipv6 route hw-failure 831
8.3.0.41 show ipv6 route net-prototype 831
8.3.0.42 show ipv6 route preferences 832
8.3.0.43 show ipv6 route static bfd 832
8.3.0.44 show ipv6 route summary 833
8.3.0.45 clear ipv6 route counters 835
8.3.0.46 show ipv6 snooping counters 835
8.3.0.47 show ipv6 vlan 835
8.3.0.48 show ipv6 traffic 836
8.3.0.49 clear ipv6 snooping counters 838
8.3.0.50 clear ipv6 statistics 839
8.4 OSPFv3 Commands 840
8.4.1 Global OSPFv3 Commands 840
8.4.1.1 ipv6 router ospf 840
8.4.1.2 area default-cost (OSPFv3) 840
8.4.1.3 area nssa (OSPFv3) 840
8.4.1.4 area nssa default-info-originate (OSPFv3) 840

8.4.1.5 area nssa no-redistribute (OSPFv3) 841
8.4.1.6 area nssa no-summary (OSPFv3) 841
8.4.1.7 area nssa translator-role (OSPFv3) 841
8.4.1.8 area nssa translator-stab-intv (OSPFv3) 842
8.4.1.9 area range (OSPFv3) 842
8.4.1.10 area stub (OSPFv3) 843
8.4.1.11 area stub no-summary (OSPFv3) 843
8.4.1.12 area virtual-link (OSPFv3) 843
8.4.1.13 area virtual-link dead-interval (OSPFv3) 844
8.4.1.14 area virtual-link hello-interval (OSPFv3) 844
8.4.1.15 area virtual-link retransmit-interval (OSPFv3) 844
8.4.1.16 area virtual-link transmit-delay (OSPFv3) 845
8.4.1.17 auto-cost (OSPFv3) 845
8.4.1.18 clear ipv6 ospf 845
8.4.1.19 clear ipv6 ospf configuration 846
8.4.1.20 clear ipv6 ospf counters 846
8.4.1.21 clear ipv6 ospf neighbor 846
8.4.1.22 clear ipv6 ospf neighbor interface 846
8.4.1.23 clear ipv6 ospf redistribution 846
8.4.1.24 default-information originate (OSPFv3) 846
8.4.1.25 default-metric (OSPFv3) 847
8.4.1.26 distance ospf (OSPFv3) 847
8.4.1.27 enable (OSPFv3) 847
8.4.1.28 exit-overflow-interval (OSPFv3) 848
8.4.1.29 external-lsdb-limit (OSPFv3) 848
8.4.1.30 maximum-paths (OSPFv3) 849
8.4.1.31 passive-interface default (OSPFv3) 849
8.4.1.32 passive-interface (OSPFv3) 849
8.4.1.33 redistribute (OSPFv3) 850
8.4.1.34 router-id (OSPFv3) 850
8.4.1.35 timers pacing lsa-group 850
8.4.1.36 timers throttle spf 851
8.4.1.37 trapflags (OSPFv3) 851
8.4.2 OSPFv3 Interface Commands 853
8.4.2.1 ipv6 ospf area 853
8.4.2.2 ipv6 ospf cost 853
8.4.2.3 ipv6 ospf dead-interval 853
8.4.2.4 ipv6 ospf hello-interval 854
8.4.2.5 ipv6 ospf link-lsa-suppression 854
8.4.2.6 ipv6 ospf mtu-ignore 854

8.4.2.7 ipv6 ospf network 855
8.4.2.8 ipv6 ospf prefix-suppression 855
8.4.2.9 ipv6 ospf priority 856
8.4.2.10 ipv6 ospf retransmit-interval 856
8.4.2.11 ipv6 ospf transmit-delay 856
8.4.3 OSPFv3 Graceful Restart Commands 858
8.4.3.1 nsf (OSPFv3) 858
8.4.3.2 nsf restart-interval (OSPFv3) 858
8.4.3.3 nsf helper (OSPFv3) 859
8.4.3.4 nsf ietf helper disable (OSPFv3) 859
8.4.3.5 nsf helper strict-lsa-checking (OSPFv3) 860
8.4.4 OSPFv3 Stub Router Commands 860
8.4.4.1 max-metric router-lsa 860
8.4.4.2 clear ipv6 ospf stub-router 861
8.4.5 OSPFv3 Show Commands 862
8.4.5.1 show ipv6 ospf 862
8.4.5.2 show ipv6 ospf abr 864
8.4.5.3 show ipv6 ospf area 864
8.4.5.4 show ipv6 ospf asbr 865
8.4.5.5 show ipv6 ospf database 865
8.4.5.6 show ipv6 ospf database database-summary 866
8.4.5.7 show ipv6 ospf interface 867
8.4.5.8 show ipv6 ospf interface brief 867
8.4.5.9 show ipv6 ospf interface stats 868
8.4.5.10 show ipv6 ospf lsa-group 869
8.4.5.11 show ipv6 ospf max-metric 870
8.4.5.12 show ipv6 ospf neighbor 870
8.4.5.13 show ipv6 ospf range 872
8.4.5.14 show ipv6 ospf statistics 872
8.4.5.15 show ipv6 ospf stub table 873
8.4.5.16 show ipv6 ospf virtual-link 873
8.4.5.17 show ipv6 ospf virtual-link brief 874
8.5 DHCPv6 Commands 875
8.5.0.1 ipv6 dhcp client pd 875
8.5.0.2 ipv6 dhcp conflict logging 875
8.5.0.3 ipv6 dhcp server 876
8.5.0.4 ipv6 dhcp relay destination 876
8.5.0.5 ipv6 dhcp relay remote-id 876
8.5.0.6 ipv6 dhcp pool 877
8.5.0.7 address prefix (IPv6) 877

8.5.0.8 domain-name (IPv6) 878
8.5.0.9 dns-server (IPv6) 878
8.5.0.10 prefix-delegation (IPv6) 878
8.5.0.11 show ipv6 dhcp 879
8.5.0.12 show ipv6 dhcp statistics 879
8.5.0.13 show ipv6 dhcp interface 880
8.5.0.14 show ipv6 dhcp binding 880
8.5.0.15 show ipv6 dhcp conflict 881
8.5.0.16 show ipv6 dhcp pool 881
8.5.0.17 show network ipv6 dhcp statistics 882
8.5.0.18 show serviceport ipv6 dhcp statistics 883
8.5.0.19 clear ipv6 dhcp 884
8.5.0.20 clear ipv6 dhcp binding 884
8.5.0.21 clear ipv6 dhcp conflict 884
8.5.0.22 clear network ipv6 dhcp statistics 885
8.5.0.23 clear serviceport ipv6 dhcp statistics 885
8.6 DHCPv6 Snooping Configuration Commands 886
8.6.0.1 ipv6 dhcp snooping 886
8.6.0.2 ipv6 dhcp snooping vlan 886
8.6.0.3 ipv6 dhcp snooping verify mac-address 886
8.6.0.4 ipv6 dhcp snooping database 887
8.6.0.5 ipv6 dhcp snooping database write-delay 887
8.6.0.6 ipv6 dhcp snooping binding 887
8.6.0.7 ipv6 dhcp snooping trust 887
8.6.0.8 ipv6 dhcp snooping log-invalid 888
8.6.0.9 ipv6 dhcp snooping limit 888
8.6.0.10 ipv6 verify source 888
8.6.0.11 ipv6 verify binding 889
8.6.0.12 show ipv6 dhcp snooping 889
8.6.0.13 show ipv6 dhcp snooping binding 890
8.6.0.14 show ipv6 dhcp snooping database 890
8.6.0.15 show ipv6 dhcp snooping interfaces 891
8.6.0.16 show ipv6 dhcp snooping statistics 891
8.6.0.17 clear ipv6 dhcp snooping binding 892
8.6.0.18 clear ipv6 dhcp snooping statistics 892
8.6.0.19 show ipv6 verify 892
8.6.0.20 show ipv6 verify source 893
8.6.0.21 show ipv6 source binding 894
8.7 IPv6 Policy-Based Routing Commands 895
8.7.0.1 ipv6 policy 895

8.7.0.2 match ipv6 address 896
8.7.0.3 set ipv6 next-hop 897
8.7.0.4 set ipv6 default next-hop 898
8.7.0.5 set ipv6 precedence 899
8.7.0.6 show ipv6 policy 899
Chapter 9: IP Multicast Commands 900
9.1 Multicast Commands 900
9.1.0.1 ip mcast boundary 900
9.1.0.2 ip mroute 900
9.1.0.3 ip multicast 901
9.1.0.4 ip multicast ttl-threshold 901
9.1.0.5 show ip mcast 901
9.1.0.6 show ip mcast boundary 902
9.1.0.7 show ip mcast interface 902
9.1.0.8 show ip mroute 902
9.1.0.9 show ip mcast mroute group 906
9.1.0.10 show ip mcast mroute source 907
9.1.0.11 show ip mcast mroute static 907
9.1.0.12 clear ip mroute 908
9.2 DVMRP Commands 909
9.2.0.1 ip dvmrp 909
9.2.0.2 ip dvmrp metric 909
9.2.0.3 ip dvmrp trapflags 909
9.2.0.4 ip dvmrp 910
9.2.0.5 show ip dvmrp 910
9.2.0.6 show ip dvmrp interface 910
9.2.0.7 show ip dvmrp neighbor 911
9.2.0.8 show ip dvmrp nexthop 912
9.2.0.9 show ip dvmrp prune 912
9.2.0.10 show ip dvmrp route 912
9.3 PIM Commands 914
9.3.0.1 ip pim dense 914
9.3.0.2 ip pim sparse 914
9.3.0.3 ip pim 914
9.3.0.4 ip pim hello-interval 915
9.3.0.5 ip pim bsr-border 915
9.3.0.6 ip pim bsr-candidate 916
9.3.0.7 ip pim dr-priority 916
9.3.0.8 ip pim join-prune-interval 917
9.3.0.9 ip pim rp-address 917

9.3.0.10 ip pim rp-candidate 918
9.3.0.11 ip pim ssm 918
9.3.0.12 ip pim-trapflags 919
9.3.0.13 show ip mfc 919
9.3.0.14 show ip pim 920
9.3.0.15 show ip pim ssm 921
9.3.0.16 show ip pim interface 922
9.3.0.17 show ip pim neighbor 923
9.3.0.18 show ip pim bsr-router 923
9.3.0.19 show ip pim rp-hash 924
9.3.0.20 show ip pim rp mapping 925
9.3.0.21 show ip pim statistics 926
9.4 Internet Group Message Protocol Commands 928
9.4.0.1 ip igmp 928
9.4.0.2 ip igmp router-alert-check 928
9.4.0.3 ip igmp version 928
9.4.0.4 ip igmp last-member-query-count 929
9.4.0.5 ip igmp last-member-query-interval 929
9.4.0.6 ip igmp query-interval 929
9.4.0.7 ip igmp query-max-response-time 930
9.4.0.8 ip igmp robustness 930
9.4.0.9 ip igmp startup-query-count 930
9.4.0.10 ip igmp startup-query-interval 931
9.4.0.11 show ip igmp 931
9.4.0.12 show ip igmp groups 932
9.4.0.13 show ip igmp interface 932
9.4.0.14 show ip igmp interface membership 933
9.4.0.15 show ip igmp interface stats 934
9.5 IGMP Proxy Commands 935
9.5.0.1 ip igmp-proxy 935
9.5.0.2 ip igmp-proxy unsolicit-rprt-interval 935
9.5.0.3 ip igmp-proxy reset-status 935
9.5.0.4 show ip igmp-proxy 936
9.5.0.5 show ip igmp-proxy interface 936
9.5.0.6 show ip igmp-proxy groups 937
9.5.0.7 show ip igmp-proxy groups detail 938
Chapter 10: IPv6 Multicast Commands 940
10.1 IPv6 Multicast Forwarder 940
10.1.0.1 ipv6 mroute 940
10.1.0.2 show ipv6 mroute 940

10.1.0.3 show ipv6 mroute group 941
10.1.0.4 show ipv6 mroute source 941
10.1.0.5 show ipv6 mroute static 942
10.1.0.6 clear ipv6 mroute 942
10.2 IPv6 PIM Commands 944
10.2.0.1 ipv6 pim dense 944
10.2.0.2 ipv6 pim sparse 944
10.2.0.3 ipv6 pim 944
10.2.0.4 ipv6 pim hello-interval 945
10.2.0.5 ipv6 pim bsr-border 945
10.2.0.6 ipv6 pim bsr-candidate 946
10.2.0.7 ipv6 pim dr-priority 946
10.2.0.8 ipv6 pim join-prune-interval 947
10.2.0.9 ipv6 pim rp-address 947
10.2.0.10 ipv6 pim rp-candidate 948
10.2.0.11 ipv6 pim ssm 948
10.2.0.12 show ipv6 pim 949
10.2.0.13 show ipv6 pim ssm 950
10.2.0.14 show ipv6 pim interface 950
10.2.0.15 show ipv6 pim neighbor 951
10.2.0.16 show ipv6 pim bsr-router 952
10.2.0.17 show ipv6 pim rp-hash 953
10.2.0.18 show ipv6 pim rp mapping 953
10.3 IPv6 MLD Commands 955
10.3.0.1 ipv6 mld router 955
10.3.0.2 ipv6 mld query-interval 955
10.3.0.3 ipv6 mld query-max-response-time 955
10.3.0.4 ipv6 mld last-member-query-interval 956
10.3.0.5 ipv6 mld last-member-query-count 956
10.3.0.6 ipv6 mld version 956
10.3.0.7 show ipv6 mld groups 957
10.3.0.8 show ipv6 mld interface 958
10.3.0.9 show ipv6 mld traffic 959
10.3.0.10 clear ipv6 mld counters 960
10.3.0.11 clear ipv6 mld traffic 960
10.4 IPv6 MLD-Proxy Commands 961
10.4.0.1 ipv6 mld-proxy 961
10.4.0.2 ipv6 mld-proxy unsolicit-rprt-interval 961
10.4.0.3 ipv6 mld-proxy reset-status 961
10.4.0.4 show ipv6 mld-proxy 962

10.4.0.5 show ipv6 mld-proxy interface 962
10.4.0.6 show ipv6 mld-proxy groups 963
10.4.0.7 show ipv6 mld-proxy groups detail 964
Chapter 11: Border Gateway Protocol Commands 966
11.1 BGP Commands 966
11.1.0.1 router bgp 966
11.1.0.2 address-family 966
11.1.0.3 address-family ipv4 968
11.1.0.4 address-family ipv6 968
11.1.0.5 address-family vpnv4 unicast 968
11.1.0.6 advertisement-interval (BGP Router Config) 969
11.1.0.7 advertisement-interval (IPv6 Address Family Config) 970
11.1.0.8 address-family l2vpn evpn 970
11.1.0.9 aggregate-address (BGP Router Config) 971
11.1.0.10 aggregate-address (IPv4 VRF Address Family) 972
11.1.0.11 bgp aggregate-different-meds 973
11.1.0.12 bgp always-compare-med 973
11.1.0.13 bgp bestpath as-path ignore 974
11.1.0.14 bgp client-to-client reflection 974
11.1.0.15 bgp cluster-id 975
11.1.0.16 bgp default local-preference 975
11.1.0.17 bgp fast-external-failover 976
11.1.0.18 bgp fast-internal-failover 976
11.1.0.19 bgp listen 977
11.1.0.20 bgp log-neighbor-changes 978
11.1.0.21 bgp maxas-limit 978
11.1.0.22 bgp router-id 979
11.1.0.23 default-information originate 979
11.1.0.24 default metric 980
11.1.0.25 default-originate (BGP Router Config) 980
11.1.0.26 neighbor default-originate (IPv6 Address Family Config) 981
11.1.0.27 distance (BGP Router Config) 982
11.1.0.28 distance BGP (BGP Router Config) 983
11.1.0.29 distance BGP (IPv4 VRF Address Family) 983
11.1.0.30 distance BGP (IPv6 Address Family Config) 984
11.1.0.31 distribute-list prefix in 985
11.1.0.32 distribute-list prefix out 985
11.1.0.33 enable (BGP) 986
11.1.0.34 filter-list (BGP Router Config) 986
11.1.0.35 filter-list (IPv6 Address Family Config) 987

11.1.0.36 bgp graceful-restart....987
11.1.0.37 bgp graceful-restart-helper....988
11.1.0.38 ip bgp fast-external-failover....988
11.1.0.39 maximum-paths (BGP Router Config)....989
11.1.0.40 maximum-paths (IPv4 VRF Address Family Config)....989
11.1.0.41 maximum-paths (IPv6 Address Family Config)....990
11.1.0.42 maximum-paths igbp (BGP Router Config)....990
11.1.0.43 maximum-paths igbp (IPv4 VRF Address Family Config)....991
11.1.0.44 maximum-paths igbp (IPv6 Address Family Config)....991
11.1.0.45 maximum-prefix (BGP Router Config)....992
11.1.0.46 maximum-prefix (IPv6 Address Family Config)....993
11.1.0.47 neighbor activate (IPv4 VRF/VPNv4/L2VPN Address Family Config)....993
11.1.0.48 neighbor activate (IPv6)....994
11.1.0.49 neighbor advertisement-interval (BGP Router Config)....995
11.1.0.50 neighbor allowas-in (BGP Router Config)....996
11.1.0.51 neighbor advertisement-interval (IPv4 VRF Address Family Config)....996
11.1.0.52 neighbor advertisement-interval (IPv6 Address Family Config)....997
11.1.0.53 neighbor connect-retry-interval....998
11.1.0.54 neighbor connect-retry-interval (IPv4 Address Family Config)....998
11.1.0.55 neighbor default-originate (BGP Router Config)....999
11.1.0.56 neighbor default-originate (IPv4 VRF Address Family Config)....1000
11.1.0.57 neighbor default-originate (IPv6 Address Family Config)....1000
11.1.0.58 neighbor description....1001
11.1.0.59 neighbor ebgp-multihop....1002
11.1.0.60 neighbor ebgp-multihop (IPv4 Address Family Config)....1002
11.1.0.61 neighbor filter-list (BGP Router Config)....1003
11.1.0.62 neighbor filter-list (IPv4 VRF Address Family Config)....1004
11.1.0.63 neighbor filter-list (IPv6 Address Family Config)....1004
11.1.0.64 neighbor inherit peer (BGP Router Config)....1005
11.1.0.65 neighbor inherit peer (IPv4 Address Family Config)....1006
11.1.0.66 neighbor local-as (BGP Router Config)....1006
11.1.0.67 neighbor local-as (IPv4 VRF Address Family Config)....1007
11.1.0.68 neighbor maximum-prefix (BGP Router Config)....1008
11.1.0.69 neighbor maximum-prefix (IPv4 VRF Address Family Config)....1008
11.1.0.70 neighbor maximum-prefix (IPv6 Address Family Config)....1009
11.1.0.71 neighbor next-hop-self (BGP Router Config)....1010
11.1.0.72 neighbor next-hop-self (IPv4 VRF Address Family Config)....1010
11.1.0.73 neighbor next-hop-self (IPv6 Address Family Config)....1011
11.1.0.74 neighbor password....1011
11.1.0.75 neighbor password (IPv4 VRF Address Family Config)....1012

11.1.0.76 neighbor prefix-list 1012
11.1.0.77 neighbor remote-as (BGP Router Config) 1013
11.1.0.78 neighbor remote-as (IPv6 Address Family Config) 1014
11.1.0.79 neighbor remove-private-as (BGP Router Config) 1014
11.1.0.80 neighbor remove-private-as (IPv4 VRF Address Family Config) 1015
11.1.0.81 neighbor remove-private-as (IPv6 Address Family Config) 1015
11.1.0.82 neighbor rfc5549-support 1016
11.1.0.83 neighbor route-map (BGP Router Config) 1016
11.1.0.84 neighbor route-map (IPv4 VRF Address Family Config) 1017
11.1.0.85 neighbor route-map (IPv6 Address Family Config) 1017
11.1.0.86 neighbor route-reflector-client (BGP Router Config) 1018
11.1.0.87 neighbor route-reflector-client (IPv4 VRF Address Family Config) 1018
11.1.0.88 neighbor route-reflector-client (IPv6 Address Family Config) 1019
11.1.0.89 neighbor send-community extended 1020
11.1.0.90 neighbor send-community 1020
11.1.0.91 neighbor send-community (IPv4 VRF Address Family Config) 1021
11.1.0.92 neighbor shutdown 1021
11.1.0.93 neighbor shutdown (IPv4 VRF Address Family Config) 1022
11.1.0.94 neighbor timers 1022
11.1.0.95 neighbor timers (IPv4 VRF Address Family Config) 1023
11.1.0.96 neighbor update-source 1024
11.1.0.97 neighbor update-source (IPv4 VRF Address Family Config) 1025
11.1.0.98 network (BGP Router Config) 1026
11.1.0.99 network (IPv6 Address Family Config) 1026
11.1.0.100 nv overlay evpn 1027
11.1.0.101 rd 1027
11.1.0.102 redistribute (BGP Router Config) 1028
11.1.0.103 redistribute (IPv4 VRF Address Family Config) 1029
11.1.0.104 redistribute (IPv6 Address Family Config) 1030
11.1.0.105 route-reflector-client 1031
11.1.0.106 route-target 1032
11.1.0.107 retain route-target all 1033
11.1.0.108 template peer 1034
11.1.0.109 update-source 1035
11.1.0.110 timers bgp 1035
11.1.0.111 timers policy-apply delay 1036
11.1.0.112 clear ip bgp 1037
11.1.0.113 clear ip bgp counters 1037
11.1.0.114 show ip bgp 1037
11.1.0.115 show ip bgp aggregate-address 1040

11.1.0.116 show ip bgp community 1040
11.1.0.117 show ip bgp community-list 1041
11.1.0.118 show ip bgp extcommunity-list 1041
11.1.0.119 show ip bgp listen range 1042
11.1.0.120 show ip bgp neighbors policy 1042
11.1.0.121 show ip bgp neighbors 1043
11.1.0.122 show ip bgp neighbors advertised-routes 1047
11.1.0.123 show ip bgp neighbors policy 1048
11.1.0.124 show ip bgp neighbors {received-routes | routes | rejected-routes} 1049
11.1.0.125 show ip bgp route-reflection 1050
11.1.0.126 show ip bgp statistics 1051
11.1.0.127 show ip bgp summary 1052
11.1.0.128 show ip bgp template 1053
11.1.0.129 show ip bgp traffic 1054
11.1.0.130 show ip bgp update-group 1054
11.1.0.131 show ip bgp vpnv4 1057
11.1.0.132 show bgp l2vpn evpn summary 1059
11.1.0.133 show bgp l2vpn evpn 1060
11.1.0.134 show bgp l2vpn evpn update-group 1063
11.1.0.135 show bgp l2vpn evpn statistics 1064
11.1.0.136 show bgp l2vpn evpn route-reflection 1064
11.1.0.137 show bgp ipv6 1064
11.1.0.138 show bgp ipv6 aggregate-address 1065
11.1.0.139 show bgp ipv6 community 1066
11.1.0.140 show bgp ipv6 community-list 1066
11.1.0.141 show bgp ipv6 listen range 1066
11.1.0.142 show bgp ipv6 neighbors advertised-routes 1067
11.1.0.143 show bgp ipv6 neighbors routes 1067
11.1.0.144 show bgp ipv6 neighbors policy 1067
11.1.0.145 show bgp ipv6 route-reflection 1068
11.1.0.146 show bgp ipv6 neighbors 1068
11.1.0.147 show bgp ipv6 statistics 1069
11.1.0.148 show bgp ipv6 summary 1070
11.1.0.149 show bgp ipv6 update-group 1070
11.1.0.150 snapshot bgp 1070
11.2 BGP Routing Policy Commands 1071
11.2.0.1 ip as-path access-list 1071
11.2.0.2 ip bgp-community new-format 1072
11.2.0.3 ip community-list 1073
11.2.0.4 ip prefix-list 1073

11.2.0.5 ip prefix-list description 1075
11.2.0.6 ipv6 prefix-list 1075
11.2.0.7 match as-path 1076
11.2.0.8 match community 1077
11.2.0.9 match ip address 1077
11.2.0.10 set as-path 1078
11.2.0.11 set comm-list delete 1079
11.2.0.12 set community 1079
11.2.0.13 set local-preference 1080
11.2.0.14 set metric (BGP) 1080
11.2.0.15 set ipv6 next-hop (BGP) 1081
11.2.0.16 show ip as-path-access-list 1081
11.2.0.17 show ip community-list 1082
11.2.0.18 clear ip community-list 1082
11.2.0.19 show ip prefix-list 1082
11.2.0.20 clear ip prefix-list 1083
11.2.0.21 show ipv6 prefix-list 1084
11.2.0.22 clear ipv6 prefix-list 1085

Chapter 12: Quality of Service Commands 1086

12.1 Class of Service Commands 1086
12.1.0.1 classofservice dot1p-mapping 1086
12.1.0.2 classofservice ip-dscp-mapping 1086
12.1.0.3 classofservice trust 1087
12.1.0.4 cos-queue min-bandwidth 1087
12.1.0.5 cos-queue random-detect 1088
12.1.0.6 cos-queue strict 1088
12.1.0.7 random-detect 1089
12.1.0.8 random-detect exponential weighting-constant 1089
12.1.0.9 random-detect queue-parms 1089
12.1.0.10 traffic-shape 1093
12.1.0.11 show classofservice dot1p-mapping 1094
12.1.0.12 show classofservice ip-precedence-mapping 1094
12.1.0.13 show classofservice ip-dscp-mapping 1094
12.1.0.14 show classofservice trust 1095
12.1.0.15 show interfaces cos-queue 1095
12.1.0.16 show interfaces random-detect 1096
12.2 Differentiated Services Commands 1098
12.2.0.1 diffserv 1098
12.3 DiffServ Class Commands 1100
12.3.0.1 class-map 1100

12.3.0.2 class-map rename 1101
12.3.0.3 match access-group 1101
12.3.0.4 match access-group name 1102
12.3.0.5 match any 1102
12.3.0.6 match class-map 1102
12.3.0.7 match cos 1103
12.3.0.8 match secondary-cos 1103
12.3.0.9 match destination-address mac 1103
12.3.0.10 match dstip 1104
12.3.0.11 match dstip6 1104
12.3.0.12 match dstl4port 1104
12.3.0.13 match ethertype 1104
12.3.0.14 match exp 1104
12.3.0.15 match ip dscp 1105
12.3.0.16 match ip precedence 1105
12.3.0.17 match ip tos 1105
12.3.0.18 match ip6flowlbl 1106
12.3.0.19 match protocol 1106
12.3.0.20 match protocol 1106
12.3.0.21 match source-address mac 1107
12.3.0.22 match srcip 1107
12.3.0.23 match srcip6 1107
12.3.0.24 match srcl4port 1107
12.3.0.25 match src port 1108
12.3.0.26 match vlan 1108
12.3.0.27 match secondary-vlan 1108
12.4 DiffServ Policy Commands 1109
12.4.0.1 assign-queue 1109
12.4.0.2 drop 1109
12.4.0.3 mirror 1109
12.4.0.4 redirect 1110
12.4.0.5 conform-color 1110
12.4.0.6 class 1110
12.4.0.7 mark cos 1110
12.4.0.8 mark secondary-cos 1111
12.4.0.9 mark cos-as-sec-cos 1111
12.4.0.10 mark exp 1111
12.4.0.11 mark ip-dscp 1111
12.4.0.12 mark ip-precedence 1112
12.4.0.13 police-simple 1112

12.4.0.14 police-single-rate 1113
12.4.0.15 police-two-rate 1113
12.4.0.16 policy-map 1113
12.4.0.17 policy-map rename 1114
12.5 DiffServ Service Commands 1115
12.5.0.1 service-policy 1115
12.6 DiffServ Show Commands 1116
12.6.0.1 show class-map 1116
12.6.0.2 show diffserv 1116
12.6.0.3 show policy-map 1117
12.6.0.4 show diffserv service 1119
12.6.0.5 show diffserv service brief 1119
12.6.0.6 show policy-map interface 1120
12.6.0.7 show service-policy 1120
12.7 MAC Access Control List Commands 1122
12.7.0.1 mac access-list extended 1122
12.7.0.2 mac access-list extended rename 1122
12.7.0.3 mac access-list resequence 1123
12.7.0.4 {deny | permit} (MAC ACL) 1123
12.7.0.5 mac access-group 1125
12.7.0.6 remark 1126
12.7.0.7 show mac access-lists 1127
12.8 IP Access Control List Commands 1129
12.8.0.1 access-list 1129
12.8.0.2 access-list counters enable 1132
12.8.0.3 ip access-list 1133
12.8.0.4 ip access-list rename 1133
12.8.0.5 ip access-list resequence 1134
12.8.0.6 {deny | permit} (IP ACL) 1134
12.8.0.7 ip access-group 1137
12.8.0.8 acl-trapflags 1138
12.8.0.9 show ip access-lists 1139
12.8.0.10 show access-lists 1141
12.8.0.11 show access-lists vlan 1141
12.9 IPv6 Access Control List Commands 1142
12.9.0.1 ipv6 access-list 1142
12.9.0.2 ipv6 access-list rename 1142
12.9.0.3 ipv6 access-list resequence 1142
12.9.0.4 {deny | permit} (IPv6) 1143
12.9.0.5 ipv6 traffic-filter 1147

12.9.0.6 show ipv6 access-lists 1148
12.10 Management Access Control and Administration List 1151
12.10.0.1 management access-list 1151
12.10.0.2 {deny | permit} (Management ACAL) 1151
12.10.0.3 management access-class 1152
12.10.0.4 show management access-list 1152
12.10.0.5 show management access-class 1153
12.11 Time Range Commands for Time-Based ACLs 1154
12.11.0.1 time-range 1154
12.11.0.2 absolute 1154
12.11.0.3 periodic 1155
12.11.0.4 show time-range 1155
Chapter 13: EFOS Log Messages 1157
13.1 Core 1157
13.2 Utilities 1159
13.3 Management 1162
13.4 Switching 1164
13.5 QoS 1168
13.6 Routing/IPv6 Routing 1169
13.7 Multicast 1171
13.8 Technologies 1175
13.9 O/S Support 1177
Appendix A: Related Documents 1178
Appendix B: Command Index 1179
Revision History 1202
EFOS3.X-SWUM200; November 21, 2018 1202

Chapter 1: Introduction

This document describes the command-line interface (CLI) commands used to view and configure EFOS software. You can access the CLI by using a direct connection to the serial port or by using telnet or SSH over a remote network connection.

This document is for system administrators who configure and operate systems using EFOS software. It provides an understanding of the configuration options of the EFOS software.

Software engineers who integrate EFOS software into their hardware platform can also benefit from a description of the configuration options.

This document assumes that the reader has an understanding of the EFOS software base and has read the appropriate specification for the relevant networking device platform. It also assumes that the reader has a basic knowledge of Ethernet and networking concepts.

Refer to the release notes for the EFOS application-level code. The release notes detail the platform-specific functionality of the Switching, Routing, SNMP, Configuration, Management, and other packages. The suite of features the EFOS packages support is not available on all the platforms to which EFOS software has been ported.

1.1 About Ethernet Fabric Operating System Software

Ethernet Fabric Operating System (EFOS) switch software is designed for the data storage market. The EFOS product is customized for IP storage customers. The EFOS product is designed to run on ODM hardware platforms, is targeted towards binary customers, and is accompanied with EFOS documentation. The release numbers follow the EFOS numbering scheme and the current release is named EFOS 3.4.3. The EFOS 3.4.3 product has an EFOS-specific *Port and Feature Licensing* feature which is based on a *pay as you use* concept, enabling blocks of ports and features based on the downloaded license file. Future releases will introduce multiple EFOS specific features and additional software license would be required to use them.

As of the EFOS 3.4.3 release, EFOS is supported only on the BCM56870-based IX8-B ODM platform. Although the platform has 48 x 25G + 8 x 100G ports, only 16x25G + 2x100G ports are enabled by default. An additional downloadable software license is needed to enable multiples of 8 x 25G + 2 x 100G port blocks and the BroadView™ feature.

Chapter 2: Using the Command-Line Interface

The command-line interface (CLI) is a text-based way to manage and monitor the system. You can access the CLI by using a direct serial connection or by using a remote logical connection with telnet or SSH.

This chapter describes the CLI syntax, conventions, and modes. It contains the following sections:

2.1 Command Syntax

A command is one or more words that might be followed by one or more parameters. Parameters can be required or optional values.

Some commands, such as `show network` or `clear vlan`, do not require parameters. Other commands, such as `network parms`, require that you supply a value after the command. You must type the parameter values in a specific order, and optional parameters follow required parameters. The following example describes the `network parms` command syntax:
`network parms ipaddr netmask [gateway]`

- `network parms` is the command name.
- `ipaddr` and `netmask` are parameters and represent required values that you must enter after you type the command keywords.
- `[gateway]` is an optional parameter, so you are not required to enter a value in place of the parameter.

The *CLI Command Reference* lists each command by the command name and provides a brief description of the command. Each command reference also contains the following information:

- Format shows the command keywords and the required and optional parameters.
- Mode identifies the command mode you must be in to access the command.
- Default shows the default value, if any, of a configurable setting on the device.

The `show` commands also contain a description of the information that the command shows.

2.2 Command Conventions

The parameters for a command might include mandatory values, optional values, or keyword choices. Parameters are order-dependent. Table 1, Parameter Conventions describes the conventions this document uses to distinguish between value types.

Table 1: Parameter Conventions

Symbol	Example	Description
[] square brackets	`[value]`	Indicates an optional parameter.
`italic font in a parameter.`	*`value or [value]`*	Indicates a variable value. You must replace the italicized text and brackets with an appropriate value, which might be a name or number.
`{}` curly braces	`{choice1 | choice2}`	Indicates that you must select a parameter from the list of choices.
| Vertical bars	`choice1 | choice2`	Separates the mutually exclusive choices.
[{}] Braces within square brackets	`[{choice1 | choice2}]`	Indicates a choice within an optional element.

2.3 Common Parameter Values

Parameter values might be names (strings) or numbers. To use spaces as part of a name parameter, enclose the name value in double quotes. For example, the expression “System Name with Spaces” forces the system to accept the spaces. Empty strings (“”) are not valid user-defined strings. Table 2, Parameter Descriptions describes common parameter values and value formatting.

Table 2: Parameter Descriptions

Parameter	Description

ipaddr	This parameter is a valid IP address. You can enter the IP address in the following formats:
	`a (32 bits)`
	`a.b (8.24 bits)`
	`a.b.c (8.8.16 bits)`
	`a.b.c.d (8.8.8.8)`
	In addition to these formats, the CLI accepts decimal, hexadecimal and octal formats through the following input formats (where *n* is any valid hexadecimal, octal or decimal number):
	`0xn (CLI assumes hexadecimal format.)`
	`0n (CLI assumes octal format with leading zeros.)`
	`n (CLI assumes decimal format.)`

Interface or `slot/port`	Valid slot and port number separated by a forward slash. For example, 0/1 represents slot number 0 and port number 1.
Logical Interface	Represents a logical slot and port number. This is applicable in the case of a port-channel (LAG). You can use the logical `slot/port` to configure the port-channel.
Character strings	Use double quotation marks to identify character strings, for example, “System Name with Spaces”. An empty string (“”) is not valid.

2.4 Slot/Port Naming Convention

The EFOS software references physical entities such as cards and ports by using a `slot/port` naming convention. The EFOS software also uses this convention to identify certain logical entities, such as Port-Channel interfaces.

The slot number has two uses. In the case of physical ports, it identifies the card containing the ports. In the case of logical and CPU ports it also identifies the type of interface or port.

Table 3: Type of Slots

Slot Type	Description
Physical slot numbers	Physical slot numbers begin with zero, and are allocated up to the maximum number of physical slots.
Logical slot numbers	Logical slots immediately follow physical slots and identify port-channel (LAG) or router interfaces. The value of logical slot numbers depend on the type of logical interface and can vary from platform to platform.
CPU slot numbers	The CPU slots immediately follow the logical slots.

The port identifies the specific physical port or logical interface being managed on a given slot.

Table 4: Type of Ports

Port Type	Description
Physical Ports	The physical ports for each slot are numbered sequentially starting from zero.

Table 4: Type of Ports (Continued)

Port Type	Description
Logical Interfaces	Port-channel or Link Aggregation Group (LAG) interfaces are logical interfaces that are only used for bridging functions. VLAN routing interfaces are only used for routing functions. Loopback interfaces are logical interfaces that are always up. Tunnel interfaces are logical point-to-point links that carry encapsulated packets.
CPU ports	CPU ports are handled by the driver as one or more physical entities located on physical slots.

NOTE: In the CLI, loopback interfaces do not use the `slot/port` format. To specify a loopback interface, you use the loopback ID.

2.5 Using the No Form of a Command

The `no` keyword is a specific form of an existing command and does not represent a new or distinct command. Almost every configuration command has a `no` form. In general, use the `no` form to reverse the action of a command or reset a value back to the default. For example, the `no shutdown` configuration command reverses the shutdown of an interface. Use the command without the keyword `no` to re-enable a disabled feature or to enable a feature that is disabled by default. Only the configuration commands are available in the `no` form.

2.6 Executing Show Commands

All show commands can now be issued from any configuration mode (Global Config, Interface Config, VLAN Database, etc.). The show commands provide information about system and feature-specific configuration, status, and statistics. In previous releases, show commands could be issued only in User EXEC or Privileged EXEC modes.

2.7 CLI Output Filtering

Many CLI show commands include considerable content to display to the user. This can make output confusing and cumbersome to parse through to find important information. The CLI Output Filtering feature allows the user, when executing CLI show display commands, to optionally specify arguments to filter the CLI output to display only desired information. The result is to simplify the display and make it easier for the user to find the information the user is interested in.

The main functions of the CLI Output Filtering feature are:

- Pagination Control
  - Supports enabling/disabling paginated output for all **show** CLI commands. When disabled, output is displayed in its entirety. When enabled, output is displayed page-by-page such that content does not scroll off the terminal screen until the user presses a key to continue. --More-- or (q)uit is displayed at the end of each page.
  - When pagination is enabled, press the return key to advance a single line, press q or Q to stop pagination, or press any other key to advance a whole page. These keys are not configurable.

NOTE: Although some EFOS **show** commands already support pagination, the implementation is unique per command and not generic to all commands.

- Output Filtering
  - “Grep”-like control for modifying the displayed output to only show the user-desired content.
    - Filter displayed output to only include lines containing a specified string match.
    - Filter displayed output to exclude lines containing a specified string match.

- Filter displayed output to only include lines including and following a specified string match.
- Filter displayed output to only include a specified section of the content (e.g., “interface 0/1”) with a configurable end-of-section delimiter.
- String matching should be case insensitive.
- Pagination, when enabled, also applies to filtered output.

Example: The following shows an example of the extensions made to the CLI show commands for the Output Filtering feature.

```
show running-config ?
<cr>      Press enter to execute the command.
all       Show all the running configuration on the switch.
|         Output filter options

show running-config | ?
include {keyword}
exclude {keyword}
section {begin end}
```

For commands for the feature, see Section 4.3, CLI Output Filtering Commands.

2.8 EFOS Modules

EFOS software consists of flexible modules that can be applied in various combinations to develop advanced Layer 2/3/4+ products. The commands and command modes available on your switch depend on the installed modules. Additionally, for some `show` commands, the output fields might change based on the modules included in the EFOS software.

The EFOS software suite includes the following modules:

- Switching (Layer 2)
- Data Center
- Routing (Layer 3)
- IPv6 Routing (Layer 3)
- Multicast
- BGP-4
- Quality of Service
- Management (CLI and SNMP)

Not all modules are available for all platforms or software releases.

2.9 Command Modes

The CLI groups commands into modes according to the command function. Each of the command modes supports specific EFOS software commands. The commands in one mode are not available until you switch to that particular mode, with the exception of the User EXEC mode commands. You can execute the User EXEC mode commands in the Privileged EXEC mode.

The command prompt changes in each command mode to help you identify the current mode. Table 5, CLI Command Modes describes the command modes and the prompts visible in that mode.

NOTE: The command modes available on your switch depend on the software modules that are installed. For example, a switch that does not support BGPv4 does not have the BGPv4 Router Command Mode.

Table 5: CLI Command Modes

Command Mode	Prompt	Mode Description
User EXEC	`Switch>`	Contains a limited set of commands to view basic system information.
Privileged EXEC	`Switch#`	Allows you to issue any `EXEC` command, enter the VLAN mode, or enter the Global Configuration mode.
Global Config	`Switch (Config)#`	Groups general setup commands and permits you to make modifications to the running configuration.
VLAN Database	`Switch (Vlan)#`	Groups all the VLAN commands.

Interface Config	`Switch (Interface slot/port)#`
	`Switch (Interface vlan vlan-id)#`
	`Switch (Interface lag vlan-id)#`
	`Switch (Interface Loopback id)#`
	`Switch (Interface tunnel id)#`
	`Switch (Interface slot/port (startrange)-slot/port(endrange)#`
		Manages the operation of an interface and provides access to the router interface configuration commands.
		Use this mode to set up a physical port for a specific logical connection operation.
		You can also use this mode to manage the operation of a range of interfaces. For example for the range of interfaces from ports 0/2 to 0/4, the prompt displays as follows:
		`(Routing) (Interface 0/2-0/4)#`

Line Console	`Switch (config-line)#`	Contains commands to configure outbound telnet settings and console interface settings, as well as to configure console login/enable authentication.
Line SSH	`Switch (config-ssh)#`	Contains commands to configure SSH login/enable authentication.
Line Telnet	`Switch (config-telnet)#`	Contains commands to configure telnet login/enable authentication.
AAA IAS User Config	`Switch (Config-IAS-User)#`	Allows password configuration for a user in the IAS database.
Mail Server Config	`Switch (Mail-Server)#`	Allows configuration of the e-mail server.
Data Center Bridging	`Switch (config-if-dcb)#`	Allows DCBX features to be configure on the interface(s) from which it is initiated.
Policy Map Config	`Switch (Config-policy-map)#`	Contains the QoS Policy-Map configuration commands.

Table 5: CLI Command Modes (Continued)

Command Mode	Prompt	Mode Description
Policy Class Config	`Switch (Config-policy-class-map)#`	Consists of class creation, deletion, and matching commands. The class match commands specify Layer 2, Layer 3, and general match criteria.
Class Map Config	`Switch (Config-class-map)#`	Contains the QoS class map configuration commands for IPv4.
Router OSPF Config	`Switch (Config-router)#`	Contains the OSPF configuration commands.
BGP Router Config	`Switch (Config-router)#`	Contains the BGP4 configuration commands.
Route Map Config	`Switch (config-route-map)#`	Contains the route map configuration commands.
IPv6 Address Family Config	`Switch (Config-router-af)#`	Contains the IPv6 address family configuration commands.
Peer Template Config	`Switch (Config-rtr-tmplt)#`	Contains the BGP peer template configuration commands.
Peer Template Address Family Config	`Switch (Config-rtr-tmplt-af)#`	Contains the BGP peer template IPv4 and IPv6 address family configuration commands.
Radius Dynamic Authorization Config	`(Config-radius-da)`	Contains the Radius Dynamic Authorization commands.
MAC Access-list Config	`Switch (Config-mac-access-list)#`	Allows you to create a MAC Access-List and to enter the mode containing MAC Access-List configuration commands.
IPv4 Access-list Config	`Switch (Config-ipv4-acl)#`	Allows you to create an IPv4 named or extended Access-List and to enter the mode containing IPv4 Access-List configuration commands.
IPv6Access-list Config	`Switch (Config-ipv6-acl)#`	Allows you to create an IPv6 Access-List and to enter the mode containing IPv6 Access-List configuration commands.
Management Access-list Config	`Switch (config-macal)#`	Allows you to create a Management Access-List and to enter the mode containing Management Access-List configuration commands.
TACACS Config	`Switch (Tacacs)#`	Contains commands to configure properties for the TACACS servers.
ARP Access-List Config Mode	`Switch (Config-arp-access-list)#`	Contains commands to add ARP ACL rules in an ARP Access List.
User-Group Configuration Mode	`Switch (config-usergroup)`	Contains user group commands
Task-Group Configuration Mode	`Switch (config-taskgroup)`	Contains task group commands
VLAN Config	`Switch (vlan vlan-id)#`	Contains commands to configure private VLAN settings on a VLAN, FIP snooping, and to configure the RSPAN mode.
ERSPAN Source Session Configuration Mode	`Switch (config-erspan-src)#`	Configure the source interface for ERSPAN and access ERSPAN Source Session Destination Configuration mode
ERSPAN Source Session Destination Configuration Mode	`Switch (config-erspan-src-dst)#`	Configure the ERSPAN origin and destination IPv4 addresses, session ID, and various characteristics of the packets in the ERSPAN traffic.
ERSPAN Destination Session Configuration Mode	`Switch (config-erspan-src)#`	Configure the destination interface for ERSPAN and access ERSPAN Destination Session Source Configuration mode

Table 5: CLI Command Modes (Continued)

Command Mode	Prompt	Mode Description
ERSPAN Destination Session Source Configuration Mode	`Switch (config-erspan-dst-src)#`	Configure the ERSPAN destination IP address and ERSPAN session ID.
Track Configuration Mode	`Switch (config-track)#`	Configure settings to track the state of an IP Service Level Agreements (SLAs) operation
IP SLA Configuration Mode	`Switch (config-ip-sla)#`	Configure an IP SLA ICMP echo operation
SLA ICMP ECHO Configuration Mode	`Switch (config-ip-sla-echo)#`	Configure IP SLA ICMP parameters.

Table 6, CLI Mode Access and Exit explains how to enter each mode. To exit a mode and return to the previous mode, enter exit. To exit to Privileged EXEC mode, press Ctrl+z.

NOTE: Pressing Ctrl+z from Privileged EXEC mode exits to User EXEC mode. To exit User EXEC mode, enter logout.

Table 6: CLI Mode Access and Exit

Command Mode	Access Method
User EXEC	This is the first level of access.
Privileged EXEC	From the User EXEC mode, enter `enable`.
Global Config	From the Privileged EXEC mode, enter `configure`.
VLAN Database	From the Privileged EXEC mode, enter `vlan database`.

Interface Config	From the Global Config mode, enter one of the following:
	`interface slot/port`
	`interface vlan vlan-id`
	`interface lag lag-number`
	`interface loopback id`
	`interface tunnel id`
	`interface slot/port(startrange)-slot/port(endrange)`

Line Console	From the Global Config mode, enter `line console`.
Line SSH	From the Global Config mode, enter `line ssh`.
Line Telnet	From the Global Config mode, enter `line telnet`.
AAA IAS User Config	From the Global Config mode, enter `aaa ias-user username name`.
Mail Server Config	From the Global Config mode, enter `mail-server address`
Data Center Bridging	From Interface Config mode, enter `datacenter-bridging`
Policy-Map Config	From the Global Config mode, enter `policy-map <policy-name> <direction>`.
Policy-Class-Map Config	From the Policy Map mode enter `class <classname>`. **NOTE:** Classname should be created using the `class-map` command.
Class-Map Config	From the Global Config mode, enter `class-map match-all <class-map-name>`, and specify the optional keyword `ipv4` or ipv6 to specify the Layer 3 protocol for this class. See Section 12.3.0.1, class-map for more information.
Router OSPF Config	From the Global Config mode, enter `router ospf`.
BGP Router Config	From the Global Config mode, enter `router bgp asnumber`.
Route Map Config	From the Global Config mode, enter `route-map map-tag`
IPv6 Address Family Config	From the BGP Router Config mode, enter `address-family ipv6`.

Table 6: CLI Mode Access and Exit (Continued)

Command Mode	Access Method
Peer Template Config	From the BGP Router Config mode, enter `template peer name` to create a BGP peer template and enter Peer Template Configuration mode.
Peer Template Address Family Config	From the Peer Template Config mode, enter `address-family {ipv4 | ipv6}`.
MAC Access-list Config	From the Global Config mode, enter `mac access-list extended name`.
IPv4 Access-list Config	From the Global Config mode, enter `ip access-list name`.
IPv6 Access-list Config	From the Global Config mode, enter `ipv6 access-list name`.
Management Access-list Config	From the Global Config mode, enter `management access-list name`.
TACACS Config	From the Global Config mode, enter `tacacs-server host ip-addr`, where `ip-addr` is the IP address of the TACACS server on your network.
ARP Access-List Config Mode	From the Global Config mode, enter the `arp access-list` command.
User-Group Configuration Mode	From the Global Config mode, enter the `usergroup <usergroup-name>` command.
Task-Group Configuration Mode	From the Global Config mode, enter the `taskgroup <taskgroup-name>` command.
VLAN Config	From the Global Config mode, enter `vlan vlan-id`
ERSPAN Source Session Configuration Mode	From the Global Config mode, enter `monitor session` *`session-id`* `type erspan-source`
ERSPAN Source Session Destination Configuration Mode	From the ERSPAN Source Session Configuration Mode, enter `destination`.
ERSPAN Destination Session Configuration Mode	From the Global Config mode, enter `monitor session` *`session-id`* `type erspan-destination`
ERSPAN Destination Session Source Configuration Mode	From the ERSPAN Destination Session Configuration Mode, enter `source`.
Track Configuration Mode	From Global Config mode, enter `track object-number ip sla operation-number`
IP SLA Configuration Mode	From Global Config mode, enter `ip sla operation-number`
SLA ICMP ECHO Configuration Mode	From IP SLA Config mode, enter `icmp-echo destination-ip-address`

2.10 Command Completion and Abbreviation

Command completion finishes spelling the command when you type enough letters of a command to uniquely identify the command keyword. Once you have entered enough letters, press the SPACEBAR or TAB key to complete the word.

Command abbreviation allows you to execute a command when you have entered there are enough letters to uniquely identify the command. You must enter all of the required keywords and parameters before you enter the command.

2.11 CLI Error Messages

If you enter a command and the system is unable to execute it, an error message appears. Table 7, CLI Error Messages describes the most common CLI error messages.

Table 7: CLI Error Messages

Message Text	Description
`% Invalid input detected at '^' marker.`	Indicates that you entered an incorrect or unavailable command. The carat (^) shows where the invalid text is detected. This message also appears if any of the parameters or values are not recognized.

Table 7: CLI Error Messages (Continued)

Message Text	Description
`Command not found / Incomplete command. Use ? to list commands.`	Indicates that you did not enter the required keywords or values.
`Ambiguous command`	Indicates that you did not enter enough letters to uniquely identify the command.

2.12 CLI Line-Editing Conventions

Table 8, CLI Editing Conventions describes the key combinations you can use to edit commands or increase the speed of command entry. You can access this list from the CLI by entering `help` from the User or Privileged EXEC modes.

Table 8: CLI Editing Conventions

Key Sequence	Description
DEL or Backspace	Delete previous character.
Ctrl-A	Go to beginning of line.
Ctrl-E	Go to end of line.
Ctrl-F	Go forward one character.
Ctrl-B	Go backward one character.
Ctrl-D	Delete current character.
Ctrl-U, X	Delete to beginning of line.
Ctrl-K	Delete to end of line.
Ctrl-W	Delete previous word.
Ctrl-T	Transpose previous character.
Ctrl-P	Go to previous line in history buffer.
Ctrl-R	Rewrites or pastes the line.
Ctrl-N	Go to next line in history buffer.
Ctrl-Y	Prints last deleted character.
Ctrl-Q	Enables serial flow.
Ctrl-S	Disables serial flow.
Ctrl-Z	Return to root command prompt.
Tab, <SPACE>	Command-line completion.
Exit	Go to next lower command prompt.
?	List available commands, keywords, or parameters.

2.13 Using CLI Help

Enter a question mark (?) at the command prompt to display the commands available in the current mode.

```
(Routing)>?

enable                    Enter into user privilege mode.
help                      Display help for various special keys.
logout                    Exit this session. Any unsaved changes are lost.
ping                      Send ICMP echo packets to a specified IP address.
quit                      Exit this session. Any unsaved changes are lost.
show                      Display Switch Options and Settings.
telnet                    Telnet to a remote host.
```

Enter a question mark (?) after each word you enter to display available command keywords or parameters.

```
(Routing) #network ?

mgmt_vlan                 Configure the Management VLAN ID of the switch.
parms                     Configure Network Parameters of the router.
protocol                  Select DHCP, BootP, or None as the network config
                          protocol.
```

If the help output shows a parameter in angle brackets, you must replace the parameter with a value.

```
(Routing) #network parms ?

<ipaddr>                  Enter the IP address.
```

If there are no additional command keywords or parameters, or if additional parameters are optional, the following message appears in the output:

```
<cr>                      Press Enter to execute the command
```

You can also enter a question mark (?) after typing one or more characters of a word to list the available command or parameters that begin with the letters, as shown in the following example:

```
(Routing) #show m?

mac-addr-table            mac-address-table         monitor
```

2.14 Accessing the CLI

You can access the CLI by using a direct console connection or by using a telnet or SSH connection from a remote management host.

For the initial connection, you must use a direct connection to the console port. You cannot access the system remotely until the system has an IP address, subnet mask, and default gateway. You can set the network configuration information manually, or you can configure the system to accept these settings from a BOOTP or DHCP server on your network. For more information, see Section 3.1, Network Interface Commands.

Chapter 3: Management Commands

This section describes the management commands available in the EFOS CLI.

NOTE: The commands in this section are in one of three functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Clear commands clear some or all of the settings to factory defaults.

3.1 Network Interface Commands

This section describes the commands you use to configure a logical interface for management access. To configure the management VLAN, see Section 5.3.0.2, network mgmt_vlan.

3.1.0.1 enable (Privileged EXEC access)

This command gives you access to the Privileged EXEC mode. From the Privileged EXEC mode, you can configure the network interface.

Format `enable`

Mode User EXEC

3.1.0.2 do (Privileged EXEC commands)

This command executes Privileged EXEC mode commands from any of the configuration modes.

Format `do` *`Priv Exec Mode Command`*

Mode
- Global Config
- Interface Config
- VLAN Database
- Routing Config

Example: The following is an example of the `do` command that executes the Privileged EXEC command `script list` in Global Config Mode.

```
(Routing) #configure

(Routing)(config)#do script list

Configuration Script Name        Size(Bytes)
-------------------------------- -----------
backup-config                           2105
running-config                          4483
startup-config                           445

3 configuration script(s) found.
2041 Kbytes free.
```

```
Routing(config)#
```

3.1.0.3 serviceport ip

This command sets the IP address, the netmask and the gateway of the network management port. You can specify the `none` option to clear the IPv4 address and mask and the default gateway (i.e., reset each of these values to 0.0.0.0).

Format `serviceport ip {`*`ipaddr netmask`* `[`*`gateway`*`] | none}`
Mode Privileged EXEC

3.1.0.4 serviceport protocol

This command specifies the network management port configuration protocol. If you modify this value, the change is effective immediately. If you use the `bootp` parameter, the switch periodically sends requests to a BootP server until a response is received. If you use the `dhcp` parameter, the switch periodically sends requests to a DHCP server until a response is received. If you use the `none` parameter, you must configure the network information for the switch manually.

Default dhcp
Format `serviceport protocol {none | bootp | dhcp}`
Mode Privileged EXEC

3.1.0.5 serviceport protocol dhcp

This command enables the DHCPv4 client on a Service port and sends DHCP client messages with the client identifier option (DHCP Option 61).

Format `serviceport protocol dhcp [client-id]`
Mode Privileged EXEC

There is no support for the **no** form of the command **serviceport protocol dhcp client-id**. To remove the `client-id` option from the DHCP client messages, issue the command **serviceport protocol dhcp** without the `client-id` option. The command **serviceport protocol none** can be used to disable the DHCP client and client-id option on the interface.

Example: The following shows an example of the command.

```
(Routing) # serviceport protocol dhcp client-id
```

3.1.0.6 network parms

This command sets the IP address, subnet mask and gateway of the device. The IP address and the gateway must be on the same subnet. You can specify the none option to clear the IPv4 address and mask and the default gateway (i.e., to reset each of these values to the default value on the switch).

Format `network parms {`*`ipaddr netmask`* `[`*`gateway`*`]| none}`
Mode Privileged EXEC

3.1.0.7 network protocol

This command specifies the network configuration protocol to be used. If you modify this value, change is effective immediately. If you use the `bootp` parameter, the switch periodically sends requests to a BootP server until a response is received. If you use the `dhcp` parameter, the switch periodically sends requests to a DHCP server until a response is received. If you use the `none` parameter, you must configure the network information for the switch manually.

Default dhcp

Format `network protocol {none | bootp | dhcp}`

Mode Privileged EXEC

3.1.0.8 network protocol dhcp

This command enables the DHCPv4 client on a Network port and sends DHCP client messages with the client identifier option (DHCP Option 61).

Format `network protocol dhcp [client-id]`

Mode Global Config

There is no support for the **no** form of the command `network protocol dhcp client-id`. To remove the `client-id` option from the DHCP client messages, issue the command `network protocol dhcp` without the `client-id` option. The command `network protocol none` can be used to disable the DHCP client and client-id option on the interface.

Example: The following shows an example of the command.

```
(Routing) # network protocol dhcp client-id
```

3.1.0.9 network mac-address

This command sets locally administered MAC addresses. The following rules apply:

- Bit 6 of byte 0 (called the U/L bit) indicates whether the address is universally administered (b'0') or locally administered (b'1').
- Bit 7 of byte 0 (called the I/G bit) indicates whether the destination address is an individual address (b'0') or a group address (b'1').
- The second character of the twelve character `macaddr` must be 2, 6, A or E.

A locally administered address must have bit 6 On (b'1') and bit 7 Off (b'0').

Format `network mac-address` *`macaddr`*

Mode Privileged EXEC

3.1.0.10 network mac-type

This command specifies whether the switch uses the burned in MAC address or the locally-administered MAC address.

Default burnedin

Format `network mac-type {local | burnedin}`

Mode Privileged EXEC

3.1.0.10.1 no network mac-type

This command resets the value of MAC address to its default.

Format `no network mac-type`
Mode Privileged EXEC

3.1.0.11 show network

This command displays configuration settings associated with the switch's network interface. The network interface is the logical interface used for in-band connectivity with the switch via any of the switch's front panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed. The network interface is always considered to be up, whether or not any member ports are up; therefore, the `show network` command will always show **Interface Status** as `Up`.

Format `show network`
Modes
- Privileged EXEC
- User EXEC

Term	Definition
Interface Status	The network interface status; it is always considered to be “up”.
IP Address	The IP address of the interface. The factory default value is 0.0.0.0.
Subnet Mask	The IP subnet mask for this interface. The factory default value is 0.0.0.0.
Default Gateway	The default gateway for this IP interface. The factory default value is 0.0.0.0.
IPv6 Administrative Mode	Whether enabled or disabled.
IPv6 Address/Length	The IPv6 address and length.
IPv6 Default Router	The IPv6 default router address.
Burned In MAC Address	The burned in MAC address used for in-band connectivity.
Locally Administered MAC Address	If desired, a locally administered MAC address can be configured for in-band connectivity. To take effect, 'MAC Address Type' must be set to 'Locally Administered'. Enter the address as twelve hexadecimal digits (6 bytes) with a colon between each byte. Bit 1 of byte 0 must be set to a 1 and bit 0 to a 0, i.e. byte 0 should have the following mask 'xxxx xx10'. The MAC address used by this bridge when it must be referred to in a unique fashion. It is recommended that this be the numerically smallest MAC address of all ports that belong to this bridge. However it is only required to be unique. When concatenated with dot1dStpPriority a unique Bridge Identifier is formed which is used in the Spanning Tree Protocol.
MAC Address Type	The MAC address which should be used for in-band connectivity. The choices are the burned in or the Locally Administered address. The factory default is to use the burned in MAC address.
Configured IPv4 Protocol	The IPv4 network protocol being used. The options are bootp | dhcp | none.
Configured IPv6 Protocol	The IPv6 network protocol being used. The options are dhcp | none.
DHCPv6 Client DUID	The DHCPv6 client’s unique client identifier. This row is displayed only when the configured IPv6 protocol is dhcp.
IPv6 Autoconfig Mode	Whether IPv6 Stateless address autoconfiguration is enabled or disabled.
DHCP Client Identifier	The client identifier is displayed in the output of the command only if DHCP is enabled with the **client-id** option on the network port. See Section 3.1.0.8, network protocol dhcp.

Example: The following shows example CLI display output for the network port.

```
(Switching) #show network
```

```
Interface Status.............................. Up
IP Address.................................... 10.250.3.1
Subnet Mask................................... 255.255.255.0
Default Gateway............................... 10.250.3.3
IPv6 Administrative Mode...................... Enabled
IPv6 Prefix is ............................... fe80::210:18ff:fe82:64c/64
IPv6 Prefix is ............................... 2003::1/128
IPv6 Default Router is ....................... fe80::204:76ff:fe73:423a
Burned In MAC Address......................... 00:10:18:82:06:4C
Locally Administered MAC address.............. 00:00:00:00:00:00
MAC Address Type.............................. Burned In
Configured IPv4 Protocol ..................... None
Configured IPv6 Protocol ..................... DHCP
DHCPv6 Client DUID ........................... 00:03:00:06:00:10:18:82:06:4C
IPv6 Autoconfig Mode.......................... Disabled
Management VLAN ID............................ 1
DHCP Client Identifier........................ 0efos-0010.1882.160B-vl1
```

3.1.0.12 show serviceport

This command displays service port configuration information.

Format `show serviceport`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Interface Status	The network interface status. It is always considered to be up.
IP Address	The IP address of the interface. The factory default value is 0.0.0.0.
Subnet Mask	The IP subnet mask for this interface. The factory default value is 0.0.0.0.
Default Gateway	The default gateway for this IP interface. The factory default value is 0.0.0.0.
IPv6 Administrative Mode	Whether enabled or disabled. Default value is enabled.
IPv6 Address/Length	The IPv6 address and length. Default is Link Local format.
IPv6 Default Router	TheIPv6 default router address on the service port. The factory default value is an unspecified address.
Configured IPv4 Protocol	The IPv4 network protocol being used. The options are bootp | dhcp | none.
Configured IPv6 Protocol	The IPv6 network protocol being used. The options are dhcp | none.
DHCPv6 Client DUID	The DHCPv6 client's unique client identifier. This row is displayed only when the configured IPv6 protocol is dhcp.
IPv6 Autoconfig Mode	Whether IPv6 Stateless address autoconfiguration is enabled or disabled.
Burned in MAC Address	The burned in MAC address used for in-band connectivity.
DHCP Client Identifier	The client identifier is displayed in the output of the command only if DHCP is enabled with the **client-id** option on the service port. See Section 3.1.0.4, serviceport protocol.

Example: The following shows example CLI display output for the service port.

```
(Switching) #show serviceport

Interface Status.............................. Up
IP Address.................................... 10.230.3.51
Subnet Mask................................... 255.255.255.0
```

```
Default Gateway.............................. 10.230.3.1
IPv6 Administrative Mode..................... Enabled
IPv6 Prefix is .............................. fe80::210:18ff:fe82:640/64
IPv6 Prefix is .............................. 2005::21/128
IPv6 Default Router is ...................... fe80::204:76ff:fe73:423a
Configured IPv4 Protocol .................... DHCP
Configured IPv6 Protocol .................... DHCP
DHCPv6 Client DUID .......................... 00:03:00:06:00:10:18:82:06:4C
IPv6 Autoconfig Mode......................... Disabled
Burned In MAC Address........................ 00:10:18:82:06:4D
DHCP Client Identifier....................... 0efos-0010.1882.160C
```

3.2 IPv6 Management Commands

IPv6 Management commands allow a device to be managed via an IPv6 address in a switch or IPv4 routing (i.e., independent from the IPv6 Routing package). For Routing/IPv6 builds of EFOS dual IPv4/IPv6 operation over the service port is enabled. EFOS has capabilities such as:

- Static assignment of IPv6 addresses and gateways for the service/network ports.
- The ability to ping an IPv6 link-local address over the service/network port.
- Using IPv6 Management commands, you can send SNMP traps and queries via the service/network port.
- The user can manage a device via the network port (in addition to a Routing Interface or the Service port).

3.2.0.1 serviceport ipv6 enable

Use this command to enable IPv6 operation on the service port. By default, IPv6 operation is enabled on the service port.

Default enabled

Format `serviceport ipv6 enable`

Mode Privileged EXEC

3.2.0.1.1 no serviceport ipv6 enable

Use this command to disable IPv6 operation on the service port.

Format `no serviceport ipv6 enable`

Mode Privileged EXEC

3.2.0.2 network ipv6 enable

Use this command to enable IPv6 operation on the network port. By default, IPv6 operation is enabled on the network port.

Default enabled

Format `network ipv6 enable`

Mode Privileged EXEC

3.2.0.2.1 no network ipv6 enable

Use this command to disable IPv6 operation on the network port.

Format `no network ipv6 enable`
Mode Privileged EXEC

3.2.0.3 serviceport ipv6 address

Use the options of this command to manually configure IPv6 global address, enable/disable stateless global address auto-configuration and to enable/disable dhcpv6 client protocol information on the service port.

NOTE: Multiple IPv6 prefixes can be configured on the service port.

Format `serviceport ipv6 address {`*`address/prefix-length`* `[eui64]|autoconfig|dhcp}`
Mode Privileged EXEC

Parameter	Description
address	IPv6 prefix in IPv6 global address format.
prefix-length	IPv6 prefix length value.
eui64	Formulate IPv6 address in eui64 address format.
autoconfig	Configure stateless global address autoconfiguration capability.
dhcp	Configure dhcpv6 client protocol.

3.2.0.3.1 no serviceport ipv6 address

Use the command `no serviceport ipv6 address` to remove all configured IPv6 prefixes on the service port interface. Use the command with the address option to remove the manually configured IPv6 global address on the network port interface. Use the command with the autoconfig option to disable the stateless global address auto-configuration on the service port. Use the command with the dhcp option to disable the dhcpv6 client protocol on the service port.

Format `no serviceport ipv6 address {`*`address/prefix-length`* `[eui64] | autoconfig | dhcp}`
Mode Privileged EXEC

3.2.0.4 serviceport ipv6 gateway

Use this command to configure IPv6 gateway (i.e. Default routers) information for the service port.

NOTE: Only a single IPv6 gateway address can be configured for the service port. There may be a combination of IPv6 prefixes and gateways that are explicitly configured and those that are set through auto-address configuration with a connected IPv6 router on their service port interface.

Format `serviceport ipv6 gateway` *`gateway-address`*
Mode Privileged EXEC

Parameter	Description
gateway-address	Gateway address in IPv6 global or link-local address format.

3.2.0.4.1 no serviceport ipv6 gateway

Use this command to remove IPv6 gateways on the service port interface.

Format `no serviceport ipv6 gateway`
Mode Privileged EXEC

3.2.0.5 serviceport ipv6 neighbor

Use this command to manually add IPv6 neighbors to the IPv6 neighbor table for the service port. If an IPv6 neighbor already exists in the neighbor table, the entry is automatically converted to a static entry. Static entries are not modified by the neighbor discovery process. They are, however, treated the same for IPv6 forwarding. Static IPv6 neighbor entries are applied to the kernel stack and to the hardware when the corresponding interface is operationally active.

Format `serviceport ipv6 neighbor` *`ipv6-address macaddr`*
Mode Privileged EXEC

Parameter	Description
ipv6-address	The IPv6 address of the neighbor or interface.
macaddr	The link-layer address.

3.2.0.5.1 no serviceport ipv6 neighbor

Use this command to remove IPv6 neighbors from the IPv6 neighbor table for the service port.

Format `no serviceport ipv6 neighbor` *`ipv6-address macaddr`*
Mode Privileged EXEC

3.2.0.6 network ipv6 neighbor

Use this command to manually add IPv6 neighbors to the IPv6 neighbor table for this network port. If an IPv6 neighbor already exists in the neighbor table, the entry is automatically converted to a static entry. Static entries are not modified by the neighbor discovery process. They are, however, treated the same for IPv6 forwarding. Static IPv6 neighbor entries are applied to the kernel stack and to the hardware when the corresponding interface is operationally active.

Format `network ipv6 neighbor` *`ipv6-address macaddr`*
Mode Privileged EXEC

Parameter	Description
ipv6-address	The IPv6 address of the neighbor or interface.
macaddr	The link-layer address.

3.2.0.6.1 no network ipv6 neighbor

Use this command to remove IPv6 neighbors from the neighbor table.

Format `no network ipv6 neighbor` *`ipv6-address macaddr`*
Mode Privileged EXEC

3.2.0.7 network ipv6 address

Use the options of this command to manually configure IPv6 global address, enable/disable stateless global address auto-configuration and to enable/disable dhcpv6 client protocol information for the network port. Multiple IPv6 addresses can be configured on the network port.

Format `network ipv6 address {`*`address/prefix-length`* `[eui64] | autoconfig | dhcp}`
Mode Privileged EXEC

Parameter	Description
address	IPv6 prefix in IPv6 global address format.
prefix-length	IPv6 prefix length value.
eui64	Formulate IPv6 address in eui64 format.
autoconfig	Configure stateless global address autoconfiguration capability.
dhcp	Configure dhcpv6 client protocol.

3.2.0.7.1 no network ipv6 address

The command `no network ipv6 address` removes all configured IPv6 prefixes.

Use this command with the *`address`* option to remove the manually configured IPv6 global address on the network port interface. Use this command with the `autoconfig` option to disable the stateless global address auto-configuration on the network port. Use this command with the `dhcp` option to disable the DHCPv6 client protocol on the network port.

Format `no network ipv6 address {`*`address/prefix-length`* `[eui64] | autoconfig | dhcp}`
Mode Privileged EXEC

3.2.0.8 network ipv6 gateway

Use this command to configure IPv6 gateway (i.e. default routers) information for the network port.

Format `network ipv6 gateway` *`gateway-address`*
Mode Privileged EXEC

Parameter	Description
gateway-address	Gateway address in IPv6 global or link-local address format.

3.2.0.8.1 no network ipv6 gateway

Use this command to remove IPv6 gateways on the network port interface.

Format `no network ipv6 gateway`

Mode Privileged EXEC

3.2.0.9 show network ipv6 neighbors

Use this command to display the information about the IPv6 neighbor entries cached on the network port. The information is updated to show the type of the entry.

Default None

Format `show network ipv6 neighbors`

Mode
- Privileged EXEC

Field	Description
IPv6 Address	The IPv6 address of the neighbor.
MAC Address	The MAC Address of the neighbor.
isRtr	Shows if the neighbor is a router. If TRUE, the neighbor is a router; FALSE it is not a router.
Neighbor State	The state of the neighbor cache entry. Possible values are: Incomplete, Reachable, Stale, Delay, Probe, and Unknown
Age	The time in seconds that has elapsed since an entry was added to the cache.
Last Updated	The time in seconds that has elapsed since an entry was added to the cache.
Type	The type of neighbor entry. The type is Static if the entry is manually configured and Dynamic if dynamically resolved.

Example: The following is an example of the command.

```
(Routing) #show network ipv6 neighbors
                                                  Neighbor  Age
IPv6 Address             MAC Address       isRtr State    (Secs)      Type
------------------------ ----------------- ----- --------- ------     ------
FE80::5E26:AFF:FEBD:852C 5c:26:0a:bd:85:2c FALSE Reachable 0          Static
```

3.2.0.10 show serviceport ipv6 neighbors

Use this command to displays information about the IPv6 neighbor entries cached on the service port. The information is updated to show the type of the entry.

Default None

Format `show serviceport ipv6 neighbors`

Mode Privileged EXEC

Field	Description
IPv6 Address	The IPv6 address of the neighbor.
MAC Address	The MAC Address of the neighbor.
isRtr	Shows if the neighbor is a router. If TRUE, the neighbor is a router; if FALSE, it is not a router.
Neighbor State	The state of the neighbor cache entry. The possible values are: Incomplete, Reachable, Stale, Delay, Probe, and Unknown.
Age	The time in seconds that has elapsed since an entry was added to the cache.

Field	Description
Type	The type of neighbor entry. The type is Static if the entry is manually configured and Dynamic if dynamically resolved.

Example: The following is an example of the command.

```
(Routing) #show serviceport ipv6 neighbors

                                                          Neighbor  Age
IPv6 Address                          MAC Address       isRtr State    (Secs)   Type
------------------------------------- ----------------- ----- --------- ------  --------
FE80::5E26:AFF:FEBD:852C              5c:26:0a:bd:85:2c FALSE Reachable 0       Dynamic
```

3.2.0.11 show network ipv6 dhcp statistics

This command displays the statistics of the DHCPv6 client running on the network management interface.

Format `show network ipv6 dhcp statistics`

Mode
- Privileged EXEC
- User EXEC

Field	Description
DHCPv6 Advertisement Packets Received	The number of DHCPv6 Advertisement packets received on the network interface.
DHCPv6 Reply Packets Received	The number of DHCPv6 Reply packets received on the network interface.
Received DHCPv6 Advertisement Packets Discarded	The number of DHCPv6 Advertisement packets discarded on the network interface.
Received DHCPv6 Reply Packets Discarded	The number of DHCPv6 Reply packets discarded on the network interface.
DHCPv6 Malformed Packets Received	The number of DHCPv6 packets that are received malformed on the network interface.
Total DHCPv6 Packets Received	The total number of DHCPv6 packets received on the network interface.
DHCPv6 Solicit Packets Transmitted	The number of DHCPv6 Solicit packets transmitted on the network interface.
DHCPv6 Request Packets Transmitted	The number of DHCPv6 Request packets transmitted on the network interface.
DHCPv6 Renew Packets Transmitted	The number of DHCPv6 Renew packets transmitted on the network interface.
DHCPv6 Rebind Packets Transmitted	The number of DHCPv6 Rebind packets transmitted on the network interface.
DHCPv6 Release Packets Transmitted	The number of DHCPv6 Release packets transmitted on the network interface.
Total DHCPv6 Packets Transmitted	The total number of DHCPv6 packets transmitted on the network interface.

Example: The following shows example CLI display output for the command.

```
(Switching)#show network ipv6 dhcp statistics
DHCPv6 Client Statistics
------------------------

DHCPv6 Advertisement Packets Received.................. 0
DHCPv6 Reply Packets Received.......................... 0
Received DHCPv6 Advertisement Packets Discarded....... 0
Received DHCPv6 Reply Packets Discarded................ 0
DHCPv6 Malformed Packets Received...................... 0
Total DHCPv6 Packets Received.......................... 0
```

```
DHCPv6 Solicit Packets Transmitted..................... 0
DHCPv6 Request Packets Transmitted..................... 0
DHCPv6 Renew Packets Transmitted....................... 0
DHCPv6 Rebind Packets Transmitted...................... 0
DHCPv6 Release Packets Transmitted..................... 0
Total DHCPv6 Packets Transmitted....................... 0
```

3.2.0.12 show serviceport ipv6 dhcp statistics

This command displays the statistics of the DHCPv6 client running on the serviceport management interface.

Format `show serviceport ipv6 dhcp statistics`

Mode
- Privileged EXEC
- User EXEC

Field	Description
DHCPv6 Advertisement Packets Received	The number of DHCPv6 Advertisement packets received on the service port interface.
DHCPv6 Reply Packets Received	The number of DHCPv6 Reply packets received on the service port interface.
Received DHCPv6 Advertisement Packets Discarded	The number of DHCPv6 Advertisement packets discarded on the service port interface.
Received DHCPv6 Reply Packets Discarded	The number of DHCPv6 Reply packets discarded on the service port interface.
DHCPv6 Malformed Packets Received	The number of DHCPv6 packets that are received malformed on the service port interface.
Total DHCPv6 Packets Received	The total number of DHCPv6 packets received on the service port interface.
DHCPv6 Solicit Packets Transmitted	The number of DHCPv6 Solicit packets transmitted on the service port interface.
DHCPv6 Request Packets Transmitted	The number of DHCPv6 Request packets transmitted on the service port interface.
DHCPv6 Renew Packets Transmitted	The number of DHCPv6 Renew packets transmitted on the service port interface.
DHCPv6 Rebind Packets Transmitted	The number of DHCPv6 Rebind packets transmitted on the service port interface.
DHCPv6 Release Packets Transmitted	The number of DHCPv6 Release packets transmitted on the service port interface.
Total DHCPv6 Packets Transmitted	The total number of DHCPv6 packets transmitted on the service port interface.

Example: The following shows example CLI display output for the command.

```
(Switching)#show serviceport ipv6 dhcp statistics
DHCPv6 Client Statistics
------------------------

DHCPv6 Advertisement Packets Received.................. 0
DHCPv6 Reply Packets Received.......................... 0
Received DHCPv6 Advertisement Packets Discarded....... 0
Received DHCPv6 Reply Packets Discarded................ 0
DHCPv6 Malformed Packets Received...................... 0
Total DHCPv6 Packets Received.......................... 0

DHCPv6 Solicit Packets Transmitted..................... 0
DHCPv6 Request Packets Transmitted..................... 0
DHCPv6 Renew Packets Transmitted....................... 0
DHCPv6 Rebind Packets Transmitted...................... 0
DHCPv6 Release Packets Transmitted..................... 0
Total DHCPv6 Packets Transmitted....................... 0
```

3.2.0.13 clear network ipv6 dhcp statistics

Use this command to clear the DHCPv6 statistics *on the network management* interface.

Format `clear network ipv6 dhcp statistics`

Mode
- Privileged EXEC

3.2.0.14 clear serviceport ipv6 dhcp statistics

Use this command to clear the DHCPv6 client statistics *on the service port* interface.

Format `clear serviceport ipv6 dhcp statistics`

Mode
- Privileged EXEC

3.2.0.15 ping ipv6

Use this command to determine whether another computer is on the network. Ping provides a synchronous response when initiated from the CLI interface. To use the command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station. Use the `ipv6-address|hostname` parameter to ping an interface by using the global IPv6 address of the interface. Use the optional `size` keyword to specify the size of the ping packet. Use the `outgoing-interface` option to specify the outgoing interface for a multicast IP/IPv6 ping.

You can utilize the ping or trace route facilities over the service/network ports when using an IPv6 global address `ipv6-global-address|hostname`. Any IPv6 global address or gateway assignments to these interfaces will cause IPv6 routes to be installed within the IP stack such that the ping or trace route request is routed out the service/network port properly. When referencing an IPv6 link-local address, you must also specify the service or network port interface by using the `serviceport` or `network` parameter.

Default
- The default count is 1.
- The default interval is 3 seconds.
- The default size is 0 bytes.

Format `ping ipv6 {`*`ipv6-global-address`*`|`*`hostname`* `| {interface {`*`slot/port`* `| vlan` *`vlan-id`* `| serviceport | loopback | tunnel | network}` *`link-local-address`*`} [size` *`datagram-size]`* `[outgoing-interface {`*`slot/port`* `| vlan 1-4093 | serviceport | network}]}`

Mode
- Privileged EXEC
- User EXEC

3.2.0.16 ping ipv6 interface

Use this command to determine whether another computer is on the network. To use the command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to

the target station. Use the `interface` keyword to ping an interface by using the link-local address or the global IPv6 address of the interface. You can use a loopback, network port, serviceport, tunnel, or physical interface as the source. Use the optional `size` keyword to specify the size of the ping packet. The `ipv6-address` is the link local IPv6 address of the device you want to query. Use the `outgoing-interface` option to specify the outgoing interface for a multicast IP/IPv6 ping.

Format `ping ipv6 interface {slot/port | loopback loopback-id |network |serviceport |tunnel tunnel-id} {link-local-address link-local-address | ipv6-address} [size datagram-size] [outgoing-interface {slot/port | vlan 1-4093 | serviceport | network}]`

Modes
- Privileged EXEC
- User EXEC

3.2.0.17 traceroute

Use the `traceroute` command to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis. Traceroute continues to provide a synchronous response when initiated from the CLI.

The user may specify the source IP address or the virtual router of the traceroute probes. Recall that traceroute works by sending packets that are expected not to reach their final destination, but instead trigger ICMP error messages back to the source address from each hop along the forward path to the destination. By specifying the source address, the user can determine where along the forward path there is no route back to the source address. Note that this is only useful if the route from source to destination and destination to source is symmetric.) It would be common, for example, to send a traceroute from an edge router to a target higher in the network using a source address from a host subnet on the edge router. This would test reachability from within the network back to hosts attached to the edge router. Alternatively, one might send a traceroute with an address on a loopback interface as a source to test reachability back to the loopback interface address.

In the CLI, the user may specify the source either as an IPv4 address, a virtual router, or as a routing interface. When the source is specified as a routing interface, the traceroute is sent using the primary IPv4 address on the source interface. With SNMP, the source must be specified as an address.

EFOS will not accept an incoming packet, such as a traceroute response, that arrives on a routing interface if the packet's destination address is on one of the out-of-band management interfaces (service port or network port). Similarly, EFOS will not accept a packet that arrives on a management interface if the packet's destination is an address on a routing interface. Thus, it would be futile to send a traceroute on a management interface using a routing interface address as source, or to send a traceroute on a routing interface using a management interface as source. When sending a traceroute on a routing interface, the source must be that routing interface or another routing interface. When sending a traceroute on a management interface, the source must be on that management interface. For this reason, the user cannot specify the source as a management interface or management interface address. When sending a traceroute on a management interface, the user should not specify a source address, but instead let the system select the source address from the outgoing interface.

Default
- count: 3 probes
- interval: 3 seconds
- size: 0 bytes
- port: 33434
- maxTtl: 30 hops
- maxFail: 5 probes
- initTtl: 1 hop

Format `traceroute [vrf vrf-name] {ip-address | [ipv6] {ipv6-address | hostname}} [initTtl initTtl] [maxTtl maxTtl] [maxFail maxFail] [interval interval] [count count] [port port][size size] [source {ip-address | | ipv6-address | unit/slot/port}]`

Mode Privileged EXEC

Using the options described below, you can specify the initial and maximum time-to-live (TTL) in probe packets, the maximum number of failures before termination, the number of probes sent for each TTL, and the size of each probe.

Parameter	Description
vrf-name	(Optional) The name of the VRF instance from which to initiate traceroute. Only hosts reachable from within the VRF instance can be tracerouted. If a source parameter is specified in conjunction with a vrf parameter, it must be a member of the VRF. The ipv6 parameter cannot be used in conjunction with the vrf parameter.
ipaddress	The *ipaddress* value should be a valid IP address.
ipv6-address	The *ipv6-address* value should be a valid IPv6 address.
hostname	The *hostname* value should be a valid hostname.
ipv6	The optional *ipv6* keyword can be used before *ipv6-address* or *hostname*. Giving the *ipv6* keyword before the *hostname* tries it to resolve to an IPv6 address.
initTtl	Use `initTtl` to specify the initial time-to-live (TTL), the maximum number of router hops between the local and remote system. Range is 0 to 255.
maxTtl	Use `maxTtle` to specify the maximum TTL. Range is 1 to 255.
maxFail	Use `maxFail` to terminate the traceroute after failing to receive a response for this number of consecutive probes. Range is 0 to 255.
interval	Use the optional `interval` parameter to specify the time between probes, in seconds. If a response is not received within this interval, then traceroute considers that probe a failure (printing *) and sends the next probe. If traceroute does receive a response to a probe within this interval, then it sends the next probe immediately. Range is 1 to 60 seconds.
count	Use the optional `count` parameter to specify the number of probes to send for each TTL value. Range is 1 to 10 probes.
port	Use the optional `port` parameter to specify destination UDP port of the probe. This should be an unused port on the remote destination system. Range is 1 to 65535.
size	Use the optional `size` parameter to specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to 65507 bytes.
source	Use the optional *source* parameter to specify the source IP address or interface for the traceroute.

The following are examples of the CLI command.

Example: traceroute Success:

```
(Routing) # traceroute 10.240.10.115 initTtl 1 maxTtl 4 maxFail 0 interval 1 count 3 port 33434 size 43
 Traceroute to 10.240.10.115 ,4 hops max 43 byte packets:
1 10.240.4.1   708 msec     41 msec     11 msec
2 10.240.10.115   0 msec     0 msec     0 msec

Hop Count = 1 Last TTL = 2 Test attempt = 6 Test Success = 6
```

Example: traceroute ipv6 Success

```
(Routing) # traceroute 2001::2 initTtl 1 maxTtl 4 maxFail 0 interval 1 count 3 port 33434 size 43

Traceroute to 2001::2 hops max 43 byte packets:
1   2001::2   708 msec     41 msec     11 msec

The above command can also be execute with the optional ipv6 parameter as follows:

(Routing) # traceroute ipv6 2001::2 initTtl 1 maxTtl 4 maxFail 0 interval 1 count 3 port 33434 size 43
```

Example: traceroute Failure:

```
(Routing) # traceroute 10.40.1.1 initTtl 1 maxFail 0 interval 1 count 3
port 33434 size 43
Traceroute to 10.40.1.1 ,30 hops max 43 byte packets:
1 10.240.4.1   19 msec     18 msec     9 msec
2 10.240.1.252   0 msec     0 msec     1 msec
3 172.31.0.9   277 msec     276 msec     277 msec
4 10.254.1.1   289 msec     327 msec     282 msec
5 10.254.21.2   287 msec     293 msec     296 msec
6 192.168.76.2   290 msec     291 msec     289 msec
7 0.0.0.0   0 msec *
Hop Count = 6 Last TTL = 7 Test attempt = 19 Test Success = 18
```

Example: traceroute ipv6 Failure

```
(Routing) # traceroute 2001::2 initTtl 1 maxFail 0 interval 1 count 3 port 33434 size 43

Traceroute to 2001::2 hops max 43 byte packets:
1   3001::1   708 msec     41 msec     11 msec
2   4001::2   250 msec     200 msec    193 msec
3   5001::3   289 msec     313 msec    278 msec
4   6001::4   651 msec     41 msec     270 msec
5          0             0 msec *
Hop Count = 4 Last TTL = 5 Test attempt = 1 Test Success = 0
```

3.2.0.18 traceroute ipv6

Use this command to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis. The `ipv6-address` parameter must be a valid IPv6 address. The optional `port` parameter is the UDP port used as the destination of packets sent as part of the traceroute. This port should be an unused port on the destination system. The range for `port` is 0 (zero) to 65535.The default value is 33434.

Format `traceroute ipv6 ipv6-address | hostname [port]}`

Mode Privileged EXEC

3.2.0.19 ipv6 dhcp relay

Use this command to configure an interface for DHCPv6 relay functionality on an interface or range of interfaces. Use the *destination* keyword to set the relay server IPv6 address. The *relay-address* parameter is an IPv6 address of a DHCPv6 relay server. Use the *interface* keyword to set the relay server interface. The *relay-interface* parameter is an interface (`slot/port`) to reach a relay server. The optional *remote-id* is the Relay Agent Information Option “remote ID” suboption to be added to relayed messages.This can either be the special keyword *duid-ifid*, which causes the “remote ID” to be derived from the DHCPv6 server DUID and the relay interface number, or it can be specified as a user-defined string.

NOTE: If *relay-address* is an IPv6 global address, then *relay-interface* is not required. If *relay-address* is a link-local or multicast address, then *relay-interface* is required. Finally, if you do not specify a value for *relay-address*, then you must specify a value for *relay-interface* and the DHCPV6-ALL-AGENTS multicast address (i.e. `FF02::1:2`) is used to relay DHCPv6 messages to the relay server.

Format `ipv6 dhcp relay {destination [relay-address] interface [relay-interface]| interface [relay-interface]} [remote-id (duid-ifid | user-defined-string)]`

Mode Interface Config

3.3 Console Port Access Commands

This section describes the commands you use to configure the console port. You can use a serial cable to connect a management host directly to the console port of the switch.

3.3.0.1 configuration

This command gives you access to the Global Config mode. From the Global Config mode, you can configure a variety of system settings, including user accounts. From the Global Config mode, you can enter other command modes, including Line Config mode.

Format `configuration`
Mode Privileged EXEC

3.3.0.2 line

This command gives you access to the Line Console mode, which allows you to configure various Telnet settings and the console port, as well as to configure console login/enable authentication.

Format `line {console | telnet | ssh}`
Mode Global Config

Parameter	Definition
console	Console terminal line.
telnet	Virtual terminal for remote console access (Telnet).
ssh	Virtual terminal for secured remote console access (SSH).

Example: The following shows an example of the CLI command.

```
(Routing)(config)#line telnet
(Routing)(config-telnet)#
```

3.3.0.3 serial baudrate

This command specifies the communication rate of the terminal interface. The supported rates are 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200.

Default 9600
Format `serial baudrate {1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200}`
Mode Line Config

3.3.0.3.1 no serial baudrate

This command sets the communication rate of the terminal interface.

Format `no serial baudrate`
Mode Line Config

3.3.0.4 serial timeout

This command specifies the maximum connect time (in minutes) without console activity. A value of 0 indicates that a console can be connected indefinitely. The time range is 0 to 160.

Default 5

Format `serial timeout` *`0-160`*

Mode Line Config

3.3.0.4.1 no serial timeout

This command sets the maximum connect time (in minutes) without console activity.

Format `no serial timeout`

Mode Line Config

3.3.0.5 show serial

This command displays serial communication settings for the switch.

Format `show serial`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Serial Port Login Timeout (minutes)	The time, in minutes, of inactivity on a serial port connection, after which the switch will close the connection. A value of 0 disables the timeout.
Baud Rate (bps)	The default baud rate at which the serial port will try to connect.
Character Size (bits)	The number of bits in a character. The number of bits is always 8.
Flow Control	Whether Hardware Flow-Control is enabled or disabled. Hardware Flow Control is always disabled.
Stop Bits	The number of Stop bits per character. The number of Stop bits is always 1.
Parity	The parity method used on the Serial Port. The Parity Method is always None.

3.4 Telnet Commands

This section describes the commands you use to configure and view Telnet settings. You can use Telnet to manage the device from a remote management host.

3.4.0.1 ip telnet server enable

Use this command to enable Telnet connections to the system and to enable the Telnet Server Admin Mode. This command opens the Telnet listening port.

Default enabled

Format `ip telnet server enable`

Mode Privileged EXEC

3.4.0.1.1 no ip telnet server enable

Use this command to disable Telnet access to the system and to disable the Telnet Server Admin Mode. This command closes the Telnet listening port and disconnects all open Telnet sessions.

Format `no ip telnet server enable`

Mode Privileged EXEC

3.4.0.2 ip telnet port

This command configures the TCP port number on which the Telnet server listens for requests.

Default 23

Format `ip telnet port` *`1-65535`*

Mode Privileged EXEC

3.4.0.2.1 no ip telnet port

This command restores the Telnet server listen port to its factory default value.

Format `no ip telnet port`

Mode Privileged EXEC

3.4.0.3 telnet

This command establishes a new outbound Telnet connection to a remote host. The *host* value must be a valid IP address or host name. Valid values for *port* should be a valid decimal integer in the range of 0 to 65535, where the default value is 23. If `[debug]` is used, the current Telnet options enabled is displayed. The optional *line* parameter sets the outbound Telnet operational mode as linemode where, by default, the operational mode is character mode. The *localecho* option enables local echo.

Format `telnet` *`ip-address|hostname port`* `[debug] [line] [localecho]`

Modes
- Privileged EXEC
- User EXEC

3.4.0.4 transport input telnet

This command regulates new Telnet sessions. If enabled, new Telnet sessions can be established until there are no more sessions available. An established session remains active until the session is ended or an abnormal network error ends the session.

NOTE: If the Telnet Server Admin Mode is disabled, Telnet sessions cannot be established. Use the `ip telnet server enable` command to enable Telnet Server Admin Mode.

Default enabled
Format `transport input telnet`
Mode Line Config

3.4.0.4.1 no transport input telnet

Use this command to prevent new Telnet sessions from being established.

Format `no transport input telnet`
Mode Line Config

3.4.0.5 transport output telnet

This command regulates new outbound Telnet connections. If enabled, new outbound Telnet sessions can be established until the system reaches the maximum number of simultaneous outbound Telnet sessions allowed. An established session remains active until the session is ended or an abnormal network error ends it.

Default enabled
Format `transport output telnet`
Mode Line Config

3.4.0.5.1 no transport output telnet

Use this command to prevent new outbound Telnet connection from being established.

Format `no transport output telnet`
Mode Line Config

3.4.0.6 session-limit

This command specifies the maximum number of simultaneous outbound Telnet sessions. A value of 0 indicates that no outbound Telnet session can be established.

Default 5
Format `session-limit` *`0-5`*
Mode Line Config

3.4.0.6.1 no session-limit

This command sets the maximum number of simultaneous outbound Telnet sessions to the default value.

Format `no session-limit`

Mode Line Config

3.4.0.7 session-timeout

This command sets the Telnet session timeout value.The timeout value unit of time is minutes.

Default 5

Format `session-timeout` *`1-160`*

Mode Line Config

3.4.0.7.1 no session-timeout

This command sets the Telnet session timeout value to the default. The timeout value unit of time is minutes.

Format `no session-timeout`

Mode Line Config

3.4.0.8 telnetcon maxsessions

This command specifies the maximum number of Telnet connection sessions that can be established. A value of 0 indicates that no Telnet connection can be established. The range is 0-5.

Default 5

Format `telnetcon maxsessions` *`0-5`*

Mode Privileged EXEC

3.4.0.8.1 no telnetcon maxsessions

This command sets the maximum number of Telnet connection sessions that can be established to the default value.

Format `no telnetcon maxsessions`

Mode Privileged EXEC

3.4.0.9 telnetcon timeout

This command sets the Telnet connection session timeout value, in minutes. A session is active as long as the session has not been idle for the value set. The time is a decimal value from 1 to 160.

NOTE: When you change the timeout value, the new value is applied to all active and inactive sessions immediately. Any sessions that have been idle longer than the new timeout value are disconnected immediately.

Default 5

Format `telnetcon timeout` *`1-160`*

Mode Privileged EXEC

3.4.0.9.1 no telnetcon timeout

This command sets the Telnet connection session timeout value to the default.

NOTE: Changing the timeout value for active sessions does not become effective until the session is accessed again. Also, any keystroke activates the new timeout duration.

Format `no telnetcon timeout`

Mode Privileged EXEC

3.4.0.10 show telnet

This command displays the current outbound Telnet settings. In other words, these settings apply to Telnet connections initiated from the switch to a remote system.

Format `show telnet`

Modes
- Privileged EXEC
- User EXEC

Parameter	Definition
Outbound Telnet Login Timeout	The number of minutes an outbound Telnet session is allowed to remain inactive before being logged off.
Maximum Number of Outbound Telnet Sessions	The number of simultaneous outbound Telnet connections allowed.
Allow New Outbound Telnet Sessions	Indicates whether outbound Telnet sessions will be allowed.

3.4.0.11 show telnetcon

This command displays the current inbound Telnet settings. In other words, these settings apply to Telnet connections initiated from a remote system to the switch.

Format `show telnetcon`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Remote Connection Login Timeout (minutes)	This object indicates the number of minutes a remote connection session is allowed to remain inactive before being logged off. May be specified as a number from 1 to 160. The factory default is 5.
Maximum Number of Remote Connection Sessions	This object indicates the number of simultaneous remote connection sessions allowed. The factory default is 5.
Allow New Telnet Sessions	New Telnet sessions will not be allowed when this field is set to no. The factory default value is yes.
Telnet Server Admin Mode	If Telnet Admin mode is enabled or disabled.
Telnet Server Port	The configured TCP port number on which the Telnet server listens for requests. (The default is 23.)

3.5 Secure Shell Commands

This section describes the commands you use to configure Secure Shell (SSH) access to the switch. Use SSH to access the switch from a remote management host.

NOTE: The system allows a maximum of five SSH sessions.

3.5.0.1 ip ssh

Use this command to enable SSH access to the system. (This command is the short form of the `ip ssh server enable` command.)

Default	disabled
Format	`ip ssh`
Mode	Privileged EXEC

3.5.0.2 ip ssh port

Use this command to configure the TCP port number on which the SSH server listens for requests. Valid port numbers are from 1–65535.

Default	22
Format	`ip ssh port` *`1-65535`*
Mode	Privileged EXEC

3.5.0.2.1 no ip ssh port

Use this command to restore the SSH server listen port to its factory default value.

Format	`no ip ssh port`
Mode	Privileged EXEC

3.5.0.3 ip ssh server enable

This command enables the IP secure shell server. No new SSH connections are allowed, but the existing SSH connections continue to work until timed-out or logged-out.

Default	disabled
Format	`ip ssh server enable`
Mode	Privileged EXEC

3.5.0.3.1 no ip ssh server enable

This command disables the IP secure shell server.

Format	`no ip ssh server enable`
Mode	Privileged EXEC

3.5.0.4 sshcon maxsessions

This command specifies the maximum number of SSH connection sessions that can be established. A value of 0 indicates that no ssh connection can be established. The range is 0 to 5.

Default 5
Format `sshcon maxsessions` *`0-5`*
Mode Privileged EXEC

3.5.0.4.1 no sshcon maxsessions

This command sets the maximum number of allowed SSH connection sessions to the default value.

Format `no sshcon maxsessions`
Mode Privileged EXEC

3.5.0.5 sshcon timeout

This command sets the SSH connection session timeout value, in minutes. A session is active as long as the session has been idle for the value set. The time is a decimal value from 1 to 160.

Changing the timeout value for active sessions does not become effective until the session is re accessed. Also, any keystroke activates the new timeout duration.

Default 5
Format `sshcon timeout` *`1-160`*
Mode Privileged EXEC

3.5.0.5.1 no sshcon timeout

This command sets the SSH connection session timeout value, in minutes, to the default.

Changing the timeout value for active sessions does not become effective until the session is re accessed. Also, any keystroke activates the new timeout duration.

Format `no sshcon timeout`
Mode Privileged EXEC

3.5.0.6 show ip ssh

This command displays the SSH settings, including the SCP server status on the switch.

Format `show ip ssh`
Mode Privileged EXEC

Parameter	Definition
Administrative Mode	This field indicates whether the administrative mode of SSH is enabled or disabled.
SSH Port	The SSH port.
Protocol Level	The protocol level, which is SSH version 2.
SSH Sessions Currently Active	The number of SSH sessions currently active.
Max SSH Sessions Allowed	The maximum number of SSH sessions allowed.
SSH Timeout	The SSH timeout value in minutes.
Keys Present	Indicates whether the SSH RSA and DSA key files are present on the device.
Key Generation in Progress	Indicates whether RSA or DSA key files generation is currently in progress.
SCP Server Administrative Mode	Indicates whether the SCP server is enabled on the switch. To allow file transfers from a host system to the switch using SCP push operations, the SCP server must be enabled.

3.6 Management Security Commands

This section describes commands you use to generate keys and certificates, which you can do in addition to loading them as before.

3.6.0.1 crypto key generate rsa

Use this command to generate an RSA key pair for SSH. The new key files will overwrite any existing generated or downloaded RSA key files.

Format `crypto key generate rsa`

Mode Global Config

3.6.0.1.1 no crypto key generate rsa

Use this command to delete the RSA key files from the device.

Format `no crypto key generate rsa`

Mode Global Config

3.6.0.2 crypto key generate dsa

Use this command to generate a DSA key pair for SSH. The new key files will overwrite any existing generated or downloaded DSA key files.

Format `crypto key generate dsa`

Mode Global Config

3.6.0.2.1 no crypto key generate dsa

Use this command to delete the DSA key files from the device.

Format `no crypto key generate dsa`

Mode Global Config

3.7 Access Commands

Use the commands in this section to close remote connections or to view information about connections to the system.

3.7.0.1 disconnect

Use the `disconnect` command to close Telnet or SSH sessions. Use `all` to close all active sessions, or use `session-id` to specify the session ID to close. To view the possible values for `session-id`, use the `show loginsession` command.

Format `disconnect {`*`session_id`* `| all}`
Mode Privileged EXEC

3.7.0.2 efos-show

Use this command to open a connection and execute the given show command. To start the application, EFOS should be running. If EFOS is not running, the command retries for 60 seconds for EFOS to be ready to accept the efos-show connection. After 60 seconds, an error message is displayed.

The efos-show command can execute all the show commands in Privileged EXEC and User Exec mode. The output of the show command is displayed and the application terminates. If the command does not start with a show, show is added automatically before the command internally. The user can terminate the application by pressing ^c at any point of time. The efos-show command cannot handle auto-fill or tab (to auto-fill) like CLI. User is advised to enter complete command. However, partial unambiguous commands are executed like complete commands and the result is displayed normally. Partial ambiguous commands are terminated with error message. The user can use “?” to know the existing show command options.

Format `efos-show [show]` *`show option`*
Mode Privileged EXEC

3.7.0.3 linuxsh

Use the `linuxsh` command to access the Linux shell. Use the `exit` command to exit the Linux shell and return to the EFOS CLI. The shell session will timeout after five minutes of inactivity. The inactivity timeout value can be changed using the command Section 3.4.0.7, session-timeout in Line Console mode.

Default ip-port:2324
Format `linuxsh [`*`ip-port`*`]`
Mode Privileged EXEC

Parameter	Description
ip-port	The IP port number on which the telnet daemon listens for connections. ip-port is an integer from 1 to 65535. The default value is 2324.

3.7.0.4 show loginsession

This command displays current Telnet, SSH and serial port connections to the switch. This command displays truncated user names. Use the `show loginsession long` command to display the complete usernames.

Format `show loginsession`
Mode Privileged EXEC

Parameter	Definition
ID	Login Session ID.
User Name	The name the user entered to log on to the system.
Connection From	IP address of the remote client machine or EIA-232 for the serial port connection.
Idle Time	Time this session has been idle.
Session Time	Total time this session has been connected.
Session Type	Shows the type of session, which can be telnet, serial, or SSH.

3.7.0.5 show loginsession long

This command displays the complete user names of the users currently logged in to the switch.

Format `show loginsession long`
Mode Privileged EXEC

Example: The following shows an example of the command.

```
(Routing) #show loginsession long
User Name
------------
admin
test1111test1111test1111test1111test1111test1111test1111test1111
```

3.8 AAA Commands

This section describes the commands you use to add, manage, and delete system users. EFOS software has two default users: admin and guest. The admin user can view and configure system settings, and the guest user can view settings.

NOTE: You cannot delete the admin user. There is only one user allowed with read/write privileges. You can configure up to five read-only users on the system.

3.8.0.1 aaa authentication login

Use this command to set authentication at login. The default and optional list names created with the command are used with the `aaa authentication login` command. Create a list by entering the `aaa authentication login list-name method` command, where `list-name` is any character string used to name this list. The `method` argument identifies the list of methods that the authentication algorithm tries, in the given sequence.

The additional methods of authentication are used only if the previous method returns an error, not if there is an authentication failure. To ensure that the authentication succeeds even if all methods return an error, specify `none` as the final method in the command line. For example, if `none` is specified as an authentication method after `radius`, no authentication is used if the RADIUS server is down.

Default
- `defaultList`. Used by the console and only contains the method none.
- `networkList`. Used by telnet and SSH and only contains the method local.

Format `aaa authentication login {default | list-name} method1 [method2...]`

Mode Global Config

Parameter	Definition
default	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
list-name	Character string of up to 15 characters used to name the list of authentication methods activated when a user logs in.
method1... *[***method2...***]*	At least one from the following: ■ enable. Uses the enable password for authentication. ■ ldap. Uses the list of all LDAP servers for authentication. ■ line. Uses the line password for authentication. ■ local. Uses the local username database for authentication. ■ none. Uses no authentication. ■ radius. Uses the list of all RADIUS servers for authentication. ■ tacacs. Uses the list of all TACACS servers for authentication.

Example: The following shows an example of the command.

```
(switch)(config)# aaa authentication login default radius local enable none
```

3.8.0.1.1 no aaa authentication login

This command returns to the default.

Format `aaa authentication login {default | list-name}`

Mode Global Config

3.8.0.2 aaa authentication enable

Use this command to set authentication for accessing higher privilege levels. The default enable list is `enableList`. It is used by console, and contains the method as `enable followed by none`.

A separate default enable list, `enableNetList, is used for Telnet` and SSH users instead of `enableList. This list is applied by default for Telnet and SSH, and contains enable followed by deny` methods. In EFOS, by default, the enable password is not configured. That means that, by default, Telnet and SSH users will not get access to Privileged EXEC mode. On the other hand, with default conditions, a console user always enter the Privileged EXEC mode without entering the `enable` password.

The default and optional list names created with the `aaa authentication enable` command are used with the `enable authentication` command. Create a list by entering the `aaa authentication enable list-name method` command where `list-name` is any character string used to name this list. The `method` argument identifies the list of methods that the authentication algorithm tries in the given sequence.

The user manager returns ERROR (not PASS or FAIL) for enable and line methods if no password is configured, and moves to the next configured method in the authentication list. The method `none` reflects that there is no authentication needed.

The user will only be prompted for an enable password if one is required. The following authentication methods do not require passwords:

1. none
2. deny
3. enable (if no enable password is configured)
4. line (if no line password is configured)

   Example: See the examples below.

   a. `aaa authentication enable default enable none`

   b. `aaa authentication enable default line none`

   c. `aaa authentication enable default enable radius none`

   d. `aaa authentication enable default line tacacs none`

Examples **a** and **b** do not prompt for a password, however because examples **c** and **d** contain the radius and tacacsmethods, the password prompt is displayed.

If the login methods include only enable, and there is no enable password configured, then EFOS does not prompt for a username. In such cases, EFOS only prompts for a password. EFOS supports configuring methods after the local method in authentication and authorization lists. If the user is not present in the local database, then the next configured method is tried.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify `none` as the final method in the command line.

NOTE: Requests sent by the switch to a RADIUS server include the username `$enabx$`, where `x` is the requested privilege level. For enable to be authenticated on Radius servers, add `$enabx$` users to them. The login user ID is now sent to TACACS+ servers for enable authentication.

Default default

Format `aaa authentication enable {default | list-name} method1 [method2...]`

Mode Global Config

Parameter	Description
default	Uses the listed authentication methods that follow this argument as the default list of methods, when using higher privilege levels.
list-name	Character string used to name the list of authentication methods activated, when using access higher privilege levels. Range: 1-15 characters.
method1 *[***method2...***]*	Specify at least one from the following: ■ `deny`. Used to deny access. ■ `enable`. Uses the enable password for authentication. ■ `ldap`. Uses the list of all LDAP servers for authentication. ■ `line`. Uses the line password for authentication. ■ `none`. Uses no authentication. ■ `radius`. Uses the list of all RADIUS servers for authentication. ■ `tacacs`. Uses the list of all TACACS+ servers for authentication.

Example: The following example sets authentication when accessing higher privilege levels.

```
(switch)(config)# aaa authentication enable default enable
```

3.8.0.2.1 no aaa authentication enable

Use this command to return to the default configuration.

Format `no aaa authentication enable {default | list-name}`

Mode Global Config

3.8.0.3 aaa authorization commands

Use this command to configure command authorization method lists. This list is identified by `default` or a user-specified `list-name`. If `tacacs` is specified as the authorization method, authorization commands are notified to a TACACS server. If `none` is specified as the authorization method, command authorization is not applicable. A maximum of five authorization method lists can be created for the `commands` type.

NOTE: Local method is not supported for command authorization. Command authorization with RADIUS will work if, and only if, the applied authentication method is also radius.

3.8.0.3.1 Per-Command Authorization

When authorization is configured for a line mode, the user manager sends information about an entered command to the AAA server. The AAA server validates the received command, and responds with either a PASS or FAIL response. If approved, the command is executed. Otherwise, the command is denied and an error message is shown to the user. The various utility commands like tftp, and ping, and outbound telnet should also pass command authorization. Applying the script is treated as a single command apply script, which also goes through authorization. Startup-config commands applied on device boot-up are not an object of the authorization process.

The per-command authorization usage scenario is this:

1. Configure Authorization Method List
   `aaa authorization commands listname tacacs radius none`
2. Apply AML to an Access Line Mode (console, telnet, SSH)

`authorization commands` *`listname`*

3. Commands entered by the user will go through command authorization via TACACS+ or RADIUS server and will be accepted or denied.

Format *`aaa authorization commands {default|list-name} method1`*
Mode Global Config

Parameter	Description
default	The default list of methods for authorization services.
list-name	Alphanumeric character string used to name the list of authorization methods.
method	`TACACS+`,`RADIUS` and `none` are supported.

Example: The following shows an example of the command.

```
(Routing) #
(Routing) #configure
(Routing) (Config)#aaa authorization commands default none
```

3.8.0.3.2 no aaa authorization

This command deletes the authorization method list.

Format *`no aaa authorization commands {default|list-name} method1`*
Mode Global Config

3.8.0.4 authorization commands

This command applies a command authorization method list to an access method (console, telnet, ssh). For usage scenarios on per command authorization, see Section 3.8.0.3, aaa authorization commands.

Format *`authorization commands [default|list-name]`*
Mode Line console, Line telnet, Line SSH

Parameter	Description
commands	This causes command authorization for each command execution attempt.

3.8.0.4.1 no authorization commands

This command removes command authorization from a line config mode.

Format *`no authorization {commands|exec}`*
Mode Line console, Line telnet, Line SSH

Example: The following shows an example of the command.

```
(Switching) (Config)#line console
(Switching) (Config-line)#authorization commands list2
```

```
(Switching) (Config-line)#
(Switching) (Config-line)#exit

(Switching) (Config)#
```

3.8.0.5 enable authentication

Use this command to specify the authentication method list when accessing a higher privilege level from a remote telnet or console.

Format *enable authentication* {default | *list-name*}

Mode Line Config

Parameter	Description
default	Uses the default list created with the `aaa authentication enable` command.
list-name	Uses the indicated list created with the `aaa authentication enable` command.

Example: The following example specifies the default authentication method when accessing a higher privilege level console.

```
(Routing) (Config)# line console
(Routing) (config-line)# enable authentication default
```

3.8.0.5.1 no enable authentication

Use this command to return to the default specified by the `enable authentication` command.

Format *no enable authentication*

Mode Line Config

3.8.0.6 aaa ias-user username

The Internal Authentication Server (IAS) database is a dedicated internal database used for local authentication of users for network access through the IEEE 802.1X feature.

Use the `aaa ias-user username` command in Global Config mode to add the specified user to the internal user database. This command also changes the mode to AAA User Config mode.

Format `aaa ias-user username` *user*

Mode Global Config

3.8.0.6.1 no aaa ias-user username

Use this command to remove the specified user from the internal user database.

Format `no aaa ias-user username` *user*

Mode Global Config

Example: The following shows an example of the command.

```
(Routing) #
(Routing) #configure
```

```
(Routing) (Config)#aaa ias-user username client-1
(Routing) (Config-aaa-ias-User)#exit
(Routing) (Config)#no aaa ias-user username client-1
(Routing) (Config)#
```

3.8.0.7 aaa session-id

Use this command in Global Config mode to specify if the same session-id is used for Authentication, Authorization and Accounting service type within a session.

Default `common`

Format `aaa session-id [common | unique]`

Mode Global Config

Parameter	Description
common	Use the same session-id for all AAA Service types.
unique	Use a unique session-id for all AAA Service types.

3.8.0.7.1 no aaa session-id

Use this command in Global Config mode to reset the aaa session-id behavior to the default.

Format `no aaa session-id [unique]`

Mode Global Config

3.8.0.8 aaa accounting

Use this command in Global Config mode to create an accounting method list for user EXEC sessions, user-executed commands, or DOT1X. This list is identified by **default** or a user-specified **list_name**. Accounting records, when enabled for a line-mode, can be sent at both the beginning and at the end (**start-stop**) or only at the end (**stop-only**). If **none** is specified, then accounting is disabled for the specified list. If **tacacs** is specified as the accounting method, accounting records are notified to a TACACS+ server.If **radius** is the specified accounting method, accounting records are notified to a RADIUS server.

NOTE: Note the following:

- A maximum of five Accounting Method lists can be created for each exec and commands type.
- Only the default Accounting Method list can be created for DOT1X. There is no provision to create more.
- The same list-name can be used for both exec and commands accounting type
- AAA Accounting for commands with RADIUS as the accounting method is not supported.
- Start-stop or None are the only supported record types for DOT1X accounting. Start-stop enables accounting and None disables accounting.
- RADIUS is the only accounting method type supported for DOT1X accounting.

Format `aaa accounting {exec | commands | dot1x} {default | list_name} {start-stop | stop-only |none} method1 [method2…]`

Mode Global Config

Parameter	Description
exec	Provides accounting for a user EXEC terminal sessions.
commands	Provides accounting for all user executed commands.
dot1x	Provides accounting for DOT1X user commands.
default	The default list of methods for accounting services.
list-name	Character string used to name the list of accounting methods.
start-stop	Sends a start accounting notice at the beginning of a process and a stop accounting notice at the beginning of a process and a stop accounting notice at the end of a process.
stop-only	Sends a stop accounting notice at the end of the requested user process.
none	Disables accounting services on this line.
method	Use either TACACS or the radius server for accounting purposes.

Example: The following shows an example of the command.

```
(Routing) #
(Routing) #configure
(Routing) #aaa accounting commands default stop-only tacacs
(Routing) #aaa accounting exec default start-stop radius
(Routing) #aaa accounting dot1x default start-stop radius
(Routing) #aaa accounting dot1x default none
(Routing) #exit
```

For the same set of accounting type and list name, the administrator can change the record type, or the methods list, without having to first delete the previous configuration.

```
(Routing) #
(Routing) #configure
(Routing) #aaa accounting exec ExecList stop-only tacacs
(Routing) #aaa accounting exec ExecList start-stop tacacs
(Routing) #aaa accounting exec ExecList start-stop tacacs radius
```

The first **aaa** command creates a method list for exec sessions with the name *ExecList*, with **record-type** as *stop-only* and the **method** as *TACACS+*. The second command changes the **record type** to *start-stop* from *stop-only* for the same method list. The third command, for the same list changes the **methods list** to {*tacacs,radius*} from {*tacacs*}.

3.8.0.8.1 no aaa accounting

This command deletes the accounting method list.

Format `no aaa accounting {exec | commands |dot1x} {default | list_name default}`

Mode Global Config

Example: The following shows an example of the command.

```
(Routing) #
(Routing) #configure
(Routing) (Config)#aaa accounting commands userCmdAudit stop-only tacacs radius
(Routing) (Config)#no aaa accounting commands userCmdAudit
(Routing) (Config)#exit
```

3.8.0.9 aaa accounting update

Use this command to configure interim accounting records.

Default newinfo: Disabled
Periodic: 5 minutes

Format `aaa accounting update [newinfo [periodic 1-200] | periodic 1-200]`

Mode Global Config

Parameter	Definition
newinfo	Indicates that updates should be sent to the RADIUS server whenever there is a new information available, such as “Re-authentication of the client.”
periodic	The interval at which interim accounting records are sent, in minutes

3.8.0.9.1 no aaa accounting update

This command resets sending the interim accounting records.

Format `no aaa accounting update`

Mode Global Config

Example: The following shows an example of the command.

```
(Routing) #configure
(Routing) (Config)#aaa accounting update newinfo periodic 20
```

3.8.0.10 password (AAA IAS User Configuration)

Use this command to specify a password for a user in the IAS database. An optional parameter **encrypted** is provided to indicate that the password given to the command is already pre-encrypted.

Format `password` *`password`* `[encrypted]`

Mode AAA IAS User Config

Parameter	Definition
password	Password for this level. Range: 8-64 characters
encrypted	Encrypted password to be entered, copied from another switch configuration.

3.8.0.10.1 no password (AAA IAS User Configuration)

Use this command to clear the password of a user.

Format `no password`

Mode AAA IAS User Config

Example: The following shows an example of the command.

```
(Routing) #
(Routing) #configure
(Routing) (Config)#aaa ias-user username client-1
(Routing) (Config-aaa-ias-User)#password client123
```

```
(Routing) (Config-aaa-ias-User)#no password
```

Example: The following is an example of adding a MAB Client to the Internal user database.

```
(Routing) #
(Routing) #configure
(Routing) (Config)#aaa ias-user username 1f3ccb1157
(Routing) (Config-aaa-ias-User)#password 1f3ccb1157
(Routing) (Config-aaa-ias-User)#exit
(Routing) (Config)#
```

3.8.0.11 clear aaa ias-users

Use this command to remove all users from the IAS database.

Format `clear aaa ias-users`

Mode Privileged EXEC

Parameter	Definition
password	Password for this level. Range: 8-64 characters
encrypted	Encrypted password to be entered, copied from another switch configuration.

Example: The following is an example of the command.

```
(Routing) #
(Routing) #clear aaa ias-users
(Routing) #
```

3.8.0.12 show aaa ias-users

Use this command to display configured IAS users and their attributes. Passwords configured are not shown in the show command output.

Format `show aaa ias-users [username]`

Mode Privileged EXEC

Example: The following is an example of the command.

```
(Routing) #
(Routing) #show aaa ias-users

UserName
------------------
Client-1
Client-2
```

Example: Following are the IAS configuration commands shown in the output of **show running-config** command. Passwords shown in the command output are always encrypted.

```
aaa ias-user username client-1
password a45c74fdf50a558a2b5cf05573cd633bac2c6c598d54497ad4c46104918f2c encrypted
exit
```

3.8.0.13 accounting

Use this command in Line Configuration mode to apply the accounting method list to a line config (console/telnet/ssh).

Format `accounting {exec | commands } {default | listname}`

Mode Line Configuration

Parameter	Description
exec	Causes accounting for an EXEC session.
commands	This causes accounting for each command execution attempt. If a user is enabling accounting for exec mode for the current line-configuration type, the user will be logged out.
default	The default Accounting List
listname	Enter a string of not more than 15 characters.

Example: The following is a example of the command.

```
(Routing) #
(Routing) #configure
(Routing) (Config)#line telnet
(Routing) (Config-telnet)#accounting exec default
(Routing) (Config-telnet)#exit
```

3.8.0.13.1 no accounting

Use this command to remove accounting from a Line Configuration mode.

Format `no accounting {exec|commands]`

Mode Line Configuration

3.8.0.14 show accounting

Use this command to display ordered methods for accounting lists.

Format `show accounting`

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) #show accounting
Number of Accounting Notifications sent at beginning of an EXEC session:     0
Errors when sending Accounting Notifications beginning of an EXEC session:          0
Number of Accounting Notifications at end of an EXEC session:                 0
Errors when sending Accounting Notifications at end of an EXEC session:             0
Number of Accounting Notifications sent at beginning of a command execution:       0
Errors when sending Accounting Notifications at beginning of a command execution:   0
Number of Accounting Notifications sent at end of a command execution:             0
Errors when sending Accounting Notifications at end of a command execution:         0
```

3.8.0.15 show accounting methods

Use this command to display configured accounting method lists.

Format `show accounting methods`

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) #
(Routing) #show accounting methods

Acct Type      Method Name     Record Type    Method Type
----------    ------------    ------------   ------------
Exec          dfltExecList    start-stop    TACACS
Commands      dfltCmdsList    stop-only      TACACS
Commands      UserCmdAudit    start-stop     TACACS
DOT1X         dfltDot1xList    start-stop    radius

Line      EXEC Method List    Command Method List
-------  ---------------------------------------
Console  dfltExecList          dfltCmdsList
Telnet   dfltExecList          dfltCmdsList
SSH      dfltExecList          UserCmdAudit
```

3.8.0.16 show accounting update

Use this command to display configured accounting interim update information.

Format `show accounting update`

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) #
(Routing) #show accounting update

aaa accounting  update newinfo  : Enabled
aaa accounting  update periodic : 10 minutes
```

3.8.0.17 show authorization methods

This command displays the configured authorization method lists.

Format *`show authorization methods`*

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) #show authorization methods

Command Authorization List     Method
------------------------- -------------------------------------
dfltCmdAuthList               tacacs         none
list2                         none           undefined
list4                         tacacs         undefined

Line          Command Method List
------------ ------------------------------
Console       dfltCmdAuthList
Telnet        dfltCmdAuthList
SSH           dfltCmdAuthList

Exec Authorization List     Method
```

```
----------------------   ---------------------------------------
dfltExecAuthList          tacacs         none
list2                     none           undefined
list4                     tacacs         undefined

Line          Exec Method List
------------ ------------------------------
Console      dfltExecAuthList
Telnet       dfltExecAuthList
SSH          dfltExecAuthList
```

3.8.0.18 login authentication

Use this command to specify the login authentication method list for a line (console, telnet, or SSH). The default configuration uses the default set with the command `aaa authentication login`.

Format `login authentication {default | list-name}`

Mode Line Configuration

Parameter	Description
default	Uses the default list created with the `aaa authentication login` command.
list-name	Uses the indicated list created with the `aaa authentication login` command.

Example: The following example specifies the default authentication method for a console.

```
(Routing) (config)# line console
(Routing) (config-line)# login authentication default
```

3.8.0.18.1 no login authentication

Use this command to return to the default specified by the `authentication login` command.

3.9 User Account and Password Commands

3.9.0.1 username (Global Config)

Use the `username` command in Global Config mode to add a new user to the local user database. The default privilege level is 1. Using the `encrypted` keyword allows the administrator to transfer local user passwords between devices without having to know the passwords. When the `password` parameter is used along with `encrypted` parameter, the password must be exactly 128 hexadecimal characters in length. If the password strength feature is enabled, this command checks for password strength and returns an appropriate error if it fails to meet the password strength criteria. Giving the optional parameter `override-complexity-check` disables the validation of the password strength.

Format `username` *`name`* `{password` *`password`* `[encrypted [override-complexity-check] | level` *`level`* `[encrypted [override-complexity-check]] | override-complexity-check]} | {level` *`level`* `[override-complexity-check] password}`

Mode Global Config

Parameter	Description
name	The name of the user. Range: 1-64 characters.
password	The authentication password for the user. Range 8-64 characters. This value can be zero if the `no passwords min-length` command has been executed. The special characters allowed in the password include! # $ % & ' ( ) * + , - / ; < = > @ [\ ] ^ _ ` { | } ~.
level	The user level. Level 0 can be assigned by a level 15 user to another user to suspend that user's access. Range 0-15. Enter access level 1 for non-privileged (switch> prompt) or 15 for highest privilege (switch# prompt). If not specified where it is optional, the privilege level is 1.
encrypted	Encrypted password entered, copied from another switch configuration.
override-complexity-check	Disables the validation of the password strength.

Example: The following example configures user `bob` with password `xxxyyymmmm` and user level 15.

```
(Routing) (config)# username bob password xxxyyymmmm level 15
```

Example: The following example configures user test with password testPassword and assigns a user level of 1. The password strength will not be validated.

```
(Routing) (config)# username test password testPassword level 1 override-complexity-check
```

Example: A third example.

```
(Routing) (Config)#username test password testtest
```

Example: A fourth example.

```
(Routing) (Config)# username test password
e8d63677741431114f9e39a853a15e8fd35ad059e2e1b49816c243d7e08152b052eafbf23b528d348cdba1b1b7ab91be8422
78e5e970dbfc62d16dcd13c0b864 level 1 encrypted override-complexity-check

(Routing) (Config)#  username test level 15 password

Enter new password:********

Confirm new password:********
```

Example: A fifth example.

```
(Routing) (Config)# username test level 15 override-complexity-check  password

Enter new password:********

Confirm new password:********
```

3.9.0.1.1 no username

Use this command to remove a user name.

Format `no username name`
Mode Global Config

3.9.0.2 username *name nopassword*

Use this command to remove an existing user's password (NULL password).

Format `username name nopassword [level level]`
Mode Global Config

Parameter	Description
name	The name of the user. Range: 1-32 characters.
password	The authentication password for the user. Range 8-64 characters.
level	The user level. Level 0 can be assigned by a level 15 user to another user to suspend that user's access. Range 0-15.

3.9.0.3 username unlock

Use this command to allows a locked user account to be unlocked. Only a user with Level 1 access can reactivate a locked user account.

Format `username name unlock`
Mode Global Config

3.9.0.4 show users

This command displays the configured user names and their settings. The `show users` command displays truncated user names. Use the `show users long` command to display the complete user names. The `show users` command is only available for users with Level 15 privileges. The SNMPv3 fields will only be displayed if SNMP is available on the system.

Format `show users`
Mode Privileged EXEC

Parameter	Definition
User Name	The name the user enters to login using the serial port or Telnet.

Parameter	Definition
User Access Mode	Shows whether the user is able to change parameters on the switch (Level 15) or is only able to view them (Level 1). As a factory default, the “admin” user has Level 15 access and the “guest” has Level 1 access.

3.9.0.5 show users long

This command displays the complete usernames of the configured users on the switch.

Format `show users long`
Mode Privileged EXEC

Example: The following shows an example of the command.

```
(Routing) #show users long
User Name
------------
admin
guest
test1111test1111test1111test1111
```

3.9.0.6 show users accounts

This command displays the local user status with respect to user account lockout and password aging.This command displays truncated user names. Use the `show users long` command to display the complete usernames.

Format `show users accounts [detail]`
Mode Privileged EXEC

Parameter	Definition
User Name	The local user account’s user name.
Access Level	The user’s access level (1 for non-privilege (switch> prompt) or 15 for highest privilege (switch# prompt)).
Password Aging	Number of days, since the password was configured, until the password expires.
Password Expiry Date	The current password expiration date in date format.
Lockout	Indicates whether the user account is locked out (true or false).

If the detail keyword is included, the following additional fields display.

Parameter	Definition
Password Override Complexity Check	Displays the user's Password override complexity check status. By default it is disabled.
Password Strength	Displays the user password's strength (Strong or Weak). This field is displayed only if the Password Strength feature is enabled.

Example: The following example displays information about the local user database.

```
(Routing) #show users accounts
```

```
UserName            Privilege Password Password     Lockout
                              Aging    Expiry date
------------------- --------- -------- ------------ -------
admin               15        ---      ---          False
guest               1         ---      ---          False

(Routing) #show users accounts detail

UserName..................................... admin
Privilege.................................... 15
Password Aging............................... ---
Password Expiry.............................. ---
Lockout...................................... False
Override Complexity Check.................... Disable
Password Strength............................ ---
```

3.9.0.7 show users login-history

Use this command to display information about the login history of users.

Format `show users login-history [name] [long]`

Mode Privileged EXEC

Parameter	Description
name	Name of the user. Range: 1-20 characters.

Example: The following example shows user login history outputs.

```
(Routing) #show users login-history

Login Time           Username  Protocol  Location
-------------------  --------- --------- ---------------
Jan 19 2005 08:23:48  Bob       Serial
Jan 19 2005 08:42:31  John      SSH       172.16.0.1
Jan 19 2005 08:49:52  Betty     Telnet    172.16.1.7
```

3.9.0.8 password

This command allows the currently logged in user to change his or her password without having Level 15 privileges.

Format `password cr`

Mode User EXEC

3.9.0.9 password (Line Configuration)

Use the `password` command in Line Configuration mode to specify a password on a line. The default configuration is no password is specified.

Format `password [password [encrypted]]`

Mode Line Config

Parameter	Definition
password	Password for this level. Range: 8-64 characters
encrypted	Encrypted password to be entered, copied from another switch configuration. The encrypted password should be 128 characters long because the assumption is that this password is already encrypted with AES.

Example: The following example specifies a password `mcmxxyyy` on a line.

```
(Routing)(config-line)# password mcmxxyyy
```

Example: The following is another example of the command.

```
(Routing)(Config-line)# password testtest

(Routing) (Config-line)# password
e8d63677741431114f9e39a853a15e8fd35ad059e2e1b49816c243d7e08152b052eafbf23b528d348cdba1b1b7ab91be8422
78e5e970dbfc62d16dcd13c0b864 encrypted

(Routing) (Config-line)# password

Enter new password:********

Confirm new password:********
```

3.9.0.9.1 no password (Line Configuration)

Use this command to remove the password on a line.

Format `no password`
Mode Line Config

3.9.0.10 password (User EXEC)

Use this command to allow a user to change the password for only that user. This command should be used after the password has aged. The user is prompted to enter the old password and the new password.

Format `password`
Mode User EXEC

Example: The following example shows the prompt sequence for executing the password command.

```
(Routing) >password
Enter old password:********
Enter new password:********
Confirm new password:********
```

3.9.0.11 enable password

Use the `enable password` configuration command to set a local password to control access to the privileged EXEC mode.

Format `enable password [`*`password`* `[encrypted]]`
Mode Privileged EXEC

Parameter	Description
password	Password string. Range: 8-64 characters.
encrypted	Encrypted password you entered, copied from another switch configuration. The encrypted password should be 128 characters long because the assumption is that this password is already encrypted with AES.

Example: The following shows an example of the command.

```
(Routing) #enable password testtest

(Routing) #enable password
e8d63677741431114f9e39a853a15e8fd35ad059e2e1b49816c243d7e08152b052eafbf23b528d348cdba1b1b7ab91be8422
78e5e970dbfc62d16dcd13c0b864 encrypted

(Routing) #enable password
Enter old password:********
Enter new password:********
Confirm new password:********
```

3.9.0.11.1 no enable password

Use the `no enable password` command to remove the password requirement.

Format `no enable password`
Mode Privileged EXEC

3.9.0.12 passwords min-length

Use this command to enforce a minimum password length for local users. The value also applies to the enable password. The valid range is 0-64.

Default 8
Format `passwords min-length` *`0-64`*
Mode Global Config

3.9.0.12.1 no passwords min-length

Use this command to set the minimum password length to the default value.

Format `no passwords min-length`
Mode Global Config

3.9.0.13 passwords history

Use this command to set the number of previous passwords that shall be stored for each user account. When a local user changes his or her password, the user will not be able to reuse any password stored in password history. This ensures that users don’t reuse their passwords often. The valid range is 0-10.

Default 0
Format `passwords history` *`0-10`*
Mode Global Config

3.9.0.13.1 no passwords history

Use this command to set the password history to the default value.

Format `no passwords history`

Mode Global Config

3.9.0.14 passwords aging

Use this command to implement aging on passwords for local users. When a user's password expires, the user will be prompted to change it before logging in again. The valid range is 1-365. The default is 0, or no aging.

Default 0

Format `passwords aging` *`1-365`*

Mode Global Config

3.9.0.14.1 no passwords aging

Use this command to set the password aging to the default value.

Format `no passwords aging`

Mode Global Config

3.9.0.15 passwords lock-out

Use this command to strengthen the security of the switch by locking user accounts that have failed login due to wrong passwords. When a lockout count is configured, a user that is logged in must enter the correct password within that count. Otherwise the user will be locked out from further switch access. Only a user with Level 15 access can reactivate a locked user account. Password lockout does not apply to log ins from the serial console. The valid range is 1-5. The default is 0, or no lockout count enforced.

Default 0

Format `passwords lock-out` *`1-5`*

Mode Global Config

3.9.0.15.1 no passwords lock-out

Use this command to set the password lock-out count to the default value.

Format `no passwords lock-out`

Mode Global Config

3.9.0.16 passwords strength-check

Use this command to enable the password strength feature. It is used to verify the strength of a password during configuration.

Default Disable

Format `passwords strength-check`

Mode Global Config

3.9.0.16.1 no passwords strength-check

Use this command to set the password strength checking to the default value.

Format `no passwords strength-check`

Mode Global Config

3.9.0.17 passwords strength maximum consecutive-characters

Use this command to set the maximum number of consecutive characters to be used in password strength. The valid range is 0-15. The default is 0. Minimum of 0 means no restriction on that set of characters.

Default 0

Format `passwords strength maximum consecutive-characters` *`0-15`*

Mode Global Config

3.9.0.18 passwords strength maximum repeated-characters

Use this command to set the maximum number of repeated characters to be used in password strength. The valid range is 0-15. The default is 0. Minimum of 0 means no restriction on that set of characters.

Default 0

Format `passwords strength maximum consecutive-characters` *`0-15`*

Mode Global Config

3.9.0.19 passwords strength minimum uppercase-letters

Use this command to enforce a minimum number of uppercase letters that a password should contain. The valid range is 0-16. The default is 2. Minimum of 0 means no restriction on that set of characters.

Default 2

Format `passwords strength minimum uppercase-letters`

Mode Global Config

3.9.0.19.1 no passwords strength minimum uppercase-letters

Use this command to reset the minimum uppercase letters required in a password to the default value.

Format `no passwords minimum uppercase-letter`

Mode Global Config

3.9.0.20 passwords strength minimum lowercase-letters

Use this command to enforce a minimum number of lowercase letters that a password should contain. The valid range is 0-16. The default is 2. Minimum of 0 means no restriction on that set of characters.

Default 2

Format `passwords strength minimum lowercase-letters`

Mode Global Config

3.9.0.20.1 no passwords strength minimum lowercase-letters

Use this command to reset the minimum lower letters required in a password to the default value.

Format `no passwords minimum lowercase-letter`

Mode Global Config

3.9.0.21 passwords strength minimum numeric-characters

Use this command to enforce a minimum number of numeric characters that a password should contain. The valid range is 0-16. The default is 2. Minimum of 0 means no restriction on that set of characters.

Default 2

Format `passwords strength minimum numeric-characters`

Mode Global Config

3.9.0.21.1 no passwords strength minimum numeric-characters

Use this command to reset the minimum numeric characters required in a password to the default value.

Format `no passwords minimum numeric-characters`

Mode Global Config

3.9.0.22 passwords strength minimum special-characters

Use this command to enforce a minimum number of special characters that a password should contain. The valid range is 0-16. The default is 2. Minimum of 0 means no restriction on that set of characters.

Default 2

Format `passwords strength minimum special-characters`

Mode Global Config

3.9.0.22.1 no passwords strength minimum special-characters

Use this command to reset the minimum special characters required in a password to the default value.

Format `no passwords minimum special-characters`

Mode Global Config

3.9.0.23 passwords strength minimum character-classes

Use this command to enforce a minimum number of characters classes that a password should contain. Character classes are uppercase letters, lowercase letters, numeric characters and special characters. The valid range is 0-4. The default is 4.

Default 4

Format `passwords strength minimum character-classes`

Mode Global Config

3.9.0.23.1 no passwords strength minimum character-classes

Use this command to reset the minimum number of character classes required in a password to the default value.

Format `no passwords minimum character-classes`

Mode Global Config

3.9.0.24 passwords strength exclude-keyword

Use this command to exclude the specified keyword while configuring the password. The password does not accept the keyword in any form (in between the string, case in-sensitive and reverse) as a substring. User can configure up to a maximum of 3 keywords.

Format `passwords strength exclude-keyword` *`keyword`*

Mode Global Config

3.9.0.24.1 no passwords strength exclude-keyword

Use this command to reset the restriction for the specified keyword or all the keywords configured.

Format `no passwords exclude-keyword` *`[keyword]`*

Mode Global Config

3.9.0.25 show passwords configuration

Use this command to display the configured password management settings.

Format `show passwords configuration`

Mode Privileged EXEC

Parameter	Definition
Minimum Password Length	Minimum number of characters required when changing passwords.
Password History	Number of passwords to store for reuse prevention.
Password Aging	Length in days that a password is valid.
Lockout Attempts	Number of failed password login attempts before lockout.
Minimum Password Uppercase Letters	Minimum number of uppercase characters required when configuring passwords.
Minimum Password Lowercase Letters	Minimum number of lowercase characters required when configuring passwords.
Minimum Password Numeric Characters	Minimum number of numeric characters required when configuring passwords.
Maximum Password Consecutive Characters	Maximum number of consecutive characters required that the password should contain when configuring passwords.
Maximum Password Repeated Characters	Maximum number of repetition of characters that the password should contain when configuring passwords.
Minimum Password Character Classes	Minimum number of character classes (uppercase, lowercase, numeric and special) required when configuring passwords.
Password Exclude-Keywords	The set of keywords to be excluded from the configured password when strength checking is enabled.

3.9.0.26 show passwords result

Use this command to display the last password set result information.

Format `show passwords result`

Mode Privileged EXEC

Parameter	Definition
Last User Whose Password Is Set	Shows the name of the user with the most recently set password.
Password Strength Check	Shows whether password strength checking is enabled.
Last Password Set Result	Shows whether the attempt to set a password was successful. If the attempt failed, the reason for the failure is included.

3.10 SNMP Commands

This section describes the commands you use to configure Simple Network Management Protocol (SNMP) on the switch. You can configure the switch to act as an SNMP agent so that it can communicate with SNMP managers on your network.

3.10.0.1 snmp-server

This command sets the name and the physical location of the switch, and the organization responsible for the network. The parameters `name`, `loc` and `con` can be up to 255 characters in length.

Default none

Format `snmp-server {sysname` ***name*** `| location` ***loc*** `| contact` ***con*****`}`**

Mode Global Config

NOTE: To clear the snmp-server, enter an empty string in quotes. For example, snmp-server {sysname " "} clears the system name.

3.10.0.2 snmp-server community

This command adds (and names) a new SNMP community, and optionally sets the access mode, allowed IP address, and create a view for the community.

NOTE: Note the following:

- No SNMP communities exist by default. Prior to EFOS 8.2, two SNMPv2 communities (*public* and *private*) were created by default.
- Community names in the SNMP Community Table must be unique. When making multiple entries using the same community name, the first entry is kept and processed and all duplicate entries are ignored.

Default None

Format `snmp-server community` ***community-string*** `[{ro | rw |su }] [ipaddress` ***ip-address*** `[ipmask` ***ip-mask***`]]` ***[view view-name]***

Mode Global Config

Parameter	Description
community-string	A name associated with the switch and with a set of SNMP managers that manage it with a specified privileged level. The length of `community-string` can be up to 20 case-sensitive characters.
ro | rw | su	The access mode of the SNMP community, which can be read-only (ro), read-write (rw), or super user (su).

Parameter	Description
ip-address	The associated community SNMP packet sending address. It is used along with an optional IP mask value to denote an individual client or range of IP addresses from which SNMP clients may access the device using the specified community-string. If unspecified, access from any host is permitted.
ip-mask	The optional IP mask. This value is AND'ed with the IP address to determine the range of permitted client IP addresses.
view-name	The name of the view to create or update.

3.10.0.2.1 no snmp-server community

This command removes this community name from the table. The `name` is the community name to be deleted.

Format `no snmp-server community` ***community-name***
Mode Global Config

3.10.0.3 snmp-server community-group

This command configures a community access string to permit access via the SNMPv1 and SNMPv2c protocols.

Format `snmp-server community-group` ***community-string group-name*** `[ipaddress` ***ipaddress***`]`
Mode Global Config

Parameter	Description
community-string	The community which is created and then associated with the group. The range is 1 to 20 characters.
group-name	The name of the group that the community is associated with. The range is 1 to 30 characters.
ipaddress	Optionally, the IPv4 address that the community may be accessed from.

3.10.0.4 snmp-server enable traps violation

The Port MAC locking component interprets this command and configures violation action to send an SNMP trap with default trap frequency of 30 seconds. The Global command configures the trap violation mode across all interfaces valid for port-security. There is no global trap mode as such.

NOTE: For other port security commands, see Section 5.28, IGMP Snooping Configuration Commands.

Default disabled
Format `snmp-server enable traps violation`
Mode
- Global Config
- Interface Config

3.10.0.4.1 no snmp-server enable traps violation

This command disables the sending of new violation traps.
Format `no snmp-server enable traps violation`
Mode Interface Config

3.10.0.5 snmp-server enable traps

This command enables the Authentication Flag.

Default enabled

Format `snmp-server enable traps`

Mode Global Config

3.10.0.5.1 no snmp-server enable traps

This command disables the Authentication Flag.

Format `no snmp-server enable traps`

Mode Global Config

3.10.0.6 snmp-server enable traps bgp

The **bgp** option on the Section 3.10.0.5, snmp-server enable traps command above enables the two traps defined in the standard BGP MIB, RFC 4273. A trap is sent when an adjacency reaches the ESTABLISHED state and when a backward adjacency state transition occurs.

Default enabled

Format `snmp-server enable traps bgp state-changes limited`

Mode Global Config

Parameter	Description
state-changes limited	Enabled standard traps defined in RFC 4273.

3.10.0.7 snmp-server enable traps linkmode

NOTE: This command may not be available on all platforms.

This command enables Link Up/Down traps for the entire switch. When enabled, link traps are sent only if the Link Trap flag setting associated with the port is enabled.

Default enabled

Format `snmp-server enable traps linkmode`

Mode Global Config

3.10.0.7.1 no snmp-server enable traps linkmode

This command disables Link Up/Down traps for the entire switch.

Format `no snmp-server enable traps linkmode`

Mode Global Config

3.10.0.8 snmp-server enable traps multiusers

This command enables Multiple User traps. When the traps are enabled, a Multiple User Trap is sent when a user logs in to the terminal interface (EIA 232 or Telnet) and there is an existing terminal interface session.

Default enabled
Format `snmp-server enable traps multiusers`
Mode Global Config

3.10.0.8.1 no snmp-server enable traps multiusers

This command disables Multiple User traps.

Format `no snmp-server enable traps multiusers`
Mode Global Config

3.10.0.9 snmp-server enable traps stpmode

This command enables the sending of new root traps and topology change notification traps.

Default enabled
Format `snmp-server enable traps stpmode`
Mode Global Config

3.10.0.9.1 no snmp-server enable traps stpmode

This command disables the sending of new root traps and topology change notification traps.

Format `no snmp-server enable traps stpmode`
Mode Global Config

3.10.0.10 snmp-server engineID local

This command configures the SNMP engine ID on the local device.

Default The engineID is configured automatically, based on the device MAC address.
Format `snmp-server engineID local {`*`engine-id`*`|default}`
Mode Global Config

Parameter	Description
engine-id	A hexadecimal string identifying the engine-id. Engine-id must be an even length in the range of 6 to 32 hexadecimal characters.
default	Sets the engine-id to the default string, based on the device MAC address.

CAUTION! Changing the engineID will invalidate all SNMP configuration that exists on the box.

3.10.0.10.1 no snmp-server engineID local

This command removes the specified engine ID.

Default The engineID is configured automatically, based on the device MAC address.

Format `no snmp-server engineID local`

Mode Global Config

3.10.0.11 snmp-server filter

This command creates a filter entry for use in limiting which traps will be sent to a host.

Default No filters are created by default.

Format `snmp-server filter` ***`filtername oid-tree`*** `{included|excluded}`

Mode Global Config

Parameter	Description
filtername	The label for the filter being created. The range is 1 to 30 characters.
oid-tree	The OID subtree to include or exclude from the filter. Subtrees may be specified by numerical (1.3.6.2.4) or keywords (system), and asterisks may be used to specify a subtree family (1.3.*.4).
included	The tree is included in the filter.
excluded	The tree is excluded from the filter.

3.10.0.11.1 no snmp-server filter

This command removes the specified filter.

Default No filters are created by default.

Format `snmp-server filter` ***`filtername`*** `[`***`oid-tree`***`]`

Mode Global Config

3.10.0.12 snmp-server group

This command creates an SNMP access group.

Default Generic groups are created for all versions and privileges using the default views.

Format `snmp-server group` ***`group-name`*** `{v1 | v2c | v3 {noauth | auth | priv}} [context` ***`context-name`***`] [read` ***`read-view`***`] [write` ***`write-view`***`] [notify` ***`notify-view`***`]`

Mode Global Config

Parameter	Description
group-name	The group name to be used when configuring communities or users. The range is 1 to 30 characters.
v1	This group can only access via SNMPv1.
v2	This group can only access via SNMPv2c.
v3	This group can only access via SNMPv3.

Parameter	Description
noauth	This group can be accessed only when not using Authentication or Encryption. Applicable only if SNMPv3 is selected.
auth	This group can be accessed only when using Authentication but not Encryption. Applicable only if SNMPv3 is selected.
priv	This group can be accessed only when using both Authentication and Encryption. Applicable only if SNMPv3 is selected.
context-name	The SNMPv3 context used during access. Applicable only if SNMPv3 is selected.
read-view	The view this group will use during GET requests. The range is 1 to 30 characters.
write-view	The view this group will use during SET requests. The range is 1 to 30 characters.
notify-view	The view this group will use when sending out traps. The range is 1 to 30 characters.

3.10.0.12.1 no snmp-server group

This command removes the specified group.

Format `no snmp-server group` *`group-name`* `{v1|v2c| 3 {noauth|auth|priv}} [context context-name]`

Mode Global Config

3.10.0.13 snmp-server host

This command configures traps to be sent to the specified host.

Default No default hosts are configured.

Format `snmp-server host` *`host-addr community-string`* `[informs [timeout` *`seconds`*`] [retries` *`retries`*`]] [version {1 | 2c }] [udp-port` *`port`*`] [filter` *`filter-name`*`]`

Mode Global Config

Parameter	Description
host-addr	The IPv4 or IPv6 address of the host to send the trap or inform to.
community-string	Community string sent as part of the notification. The range is 1 to 20 characters.
traps	Send SNMP traps to the host. This option is selected by default.
version 1	Sends SNMPv1 traps. This option is not available if informs is selected.
version 2c	Sends SNMPv2c traps. This option is not available if informs is selected. This option is selected by default.
informs	Send SNMPv2 informs to the host.
seconds	The number of seconds to wait for an acknowledgement before resending the Inform. The default is 15 seconds. The range is 1 to 300 seconds.
retries	The number of times to resend an Inform. The default is 3 attempts. The range is 0 to 255 retries.
port	The SNMP Trap receiver port. The default is port 162.
filter-name	The filter name to associate with this host. Filters can be used to specify which traps are sent to this host. The range is 1 to 30 characters.

3.10.0.13.1 no snmp-server host

This command removes the specified host entry.

Format `no snmp-server host` *`host-addr`* `{traps|informs} version (1 | 2}`
Mode Global Config

3.10.0.14 snmp-server port

This command configures the UDP port number on which the SNMP server listens for requests.

Default 161
Format `snmp-server port` *`1025-65535`*
Mode Privileged EXEC

3.10.0.14.1 no snmp-server port

This command restores the SNMP server listen port to its factory default value.

Format `no snmp-server port`
Mode Privileged EXEC

3.10.0.15 snmp-server proxy

Use this command to enable EFOS to enter SNMP proxy mode, so that it can be managed with the Net-SNMP server. Once enabled, the current EFOS SNMP configuration is ignored, but preserved.

Format `snmp-server proxy`
Mode Global Config

3.10.0.15.1 no snmp-server proxy

Use this command to disable Net-SNMP proxy.

Format `no snmp-server proxy`
Mode Global Config

3.10.0.16 snmp-server trapsend

Use this command to set the UDP port to which traps are sent by the SNMP server.

Default 50505
Format `snmp-server trapsend` *`portid`*
Mode Global Config

3.10.0.16.1 no snmp-server trapsend

Use this command to send traps to the default UDP port.

Format `no snmp-server trapsend` *`portid`*
Mode Global Config

3.10.0.17 snmp-server user

This command creates an SNMPv3 user for access to the system.

Default No default users are created.

Format `snmp-server user` *`username groupname`* `[remote` *`engineid-string`*`] [ {auth-md5` *`password`* `| auth-sha` *`password`* `| auth-md5-key` *`md5-key`* `| auth-sha-key` *`sha-key`*`} [priv-des` *`password`* `| priv-des-key` *`des-key`*`]`

Mode Global Config

Parameter	Description
username	The username the SNMPv3 user will connect to the switch as. The range is 1 to 30 characters.
group-name	The name of the group the user belongs to. The range is 1 to 30 characters.
engineid-string	The engine-id of the remote management station that this user will be connecting from. The range is 5 to 32 characters.
password	The password the user will use for the authentication or encryption mechanism. The range is 1 to 32 characters.
md5-key	A pregenerated MD5 authentication key. The length is 32 characters.
sha-key	A pregenerated SHA authentication key. The length is 48 characters.
des-key	A pregenerated DES encryption key. The length is 32 characters if MD5 is selected, 48 characters if SHA is selected.

3.10.0.17.1 no snmp-server user

This command removes the specified SNMPv3 user.

Format `no snmp-server user` *`username`*

Mode Global Config

3.10.0.18 snmp-server view

This command creates or modifies an existing view entry that is used by groups to determine which objects can be accessed by a community or user.

Default Views are created by default to provide access to the default groups.

Format `snmp-server` *`viewname oid-tree`* `{included|excluded}`

Mode Global Config

Parameter	Description
viewname	The label for the view being created. The range is 1 to 30 characters.
oid-tree	The OID subtree to include or exclude from the view. Subtrees may be specified by numerical (1.3.6.2.4) or keywords (system), and asterisks may be used to specify a subtree family (1.3.*.4).
included	The tree is included in the view.
excluded	The tree is excluded from the view.

3.10.0.18.1 no snmp-server view

This command removes the specified view.

Format `no snmp-server view viewname [oid-tree]`

Mode Global Config

3.10.0.19 snmp-server v3-host

This command configures traps to be sent to the specified host.

Default No default hosts are configured.

Format `snmp-server v3-host host-addr username [traps | informs [timeout seconds] [retries retries]] [auth | noauth | priv] [udpport port] [filter filtername]`

Mode Global Config

Parameter	Description
host-addr	The IPv4 or IPv6 address of the host to send the trap or inform to.
user-name	User used to send a Trap or Inform message. This user must be associated with a group that supports the version and access method. The range is 1 to 30 characters.
traps	Send SNMP traps to the host. This is the default option.
informs	Send SNMP informs to the host.
seconds	Number of seconds to wait for an acknowledgement before resending the Inform. The default is 15 seconds. The range is 1 to 300 seconds.
retries	Number of times to resend an Inform. The default is 3 attempts. The range is 0 to 255 retries.
auth	Enables authentication but not encryption.
noauth	No authentication or encryption. This is the default.
priv	Enables authentication and encryption.
port	The SNMP Trap receiver port. This value defaults to port 162.
filter-name	The filter name to associate with this host. Filters can be used to specify which traps are sent to this host. The range is 1 to 30 characters.

3.10.0.20 snmptrap source-interface

Use this command in Global Configuration mode to configure the global source-interface (Source IP address) for all SNMP communication between the SNMP client and the server.

Format `snmptrap source-interface {slot/port | loopback loopback-id|tunnel tunnel-id|vlan vlan-id}`

Mode Global Config

Parameter	Description
slot/port	Specifies the port to use as the source interface.
loopback-id	Specifies the loopback interface to use as the source interface. The range of the loopback ID is 0 to 7.
tunnel-id	Specifies the tunnel interface to use as the source interface. The range of the tunnel ID is 0 to 7.
vlan-id	Specifies the VLAN to use as the source interface.

3.10.0.20.1 no snmptrap source-interface

Use this command in Global Configuration mode to remove the global source-interface (Source IP selection) for all SNMP communication between the SNMP client and the server.

Format `no snmptrap source-interface`
Mode Global Config

3.10.0.21 show snmp

This command displays the current SNMP configuration.

Format `show snmp`
Mode Privileged EXEC

Term		Definition
Community Table:	**Community-String**	The community string for the entry. This is used by SNMPv1 and SNMPv2 protocols to access the switch.
	Community-Access	The type of access the community has: ■ Read only ■ Read write ■ su
	View Name	The view this community has access to.
	IP Address	Access to this community is limited to this IP address.
Community Group Table:	**Community-String**	The community this mapping configures
	Group Name	The group this community is assigned to.
	IP Address	The IP address this community is limited to.
Host Table:	**Target Address**	The address of the host that traps will be sent to.
	Type	The type of message that will be sent, either traps or informs.
	Community	The community traps will be sent to.
	Version	The version of SNMP the trap will be sent as.
	UDP Port	The UDP port the trap or inform will be sent to.
	Filter name	The filter the traps will be limited by for this host.
	TO Sec	The number of seconds before informs will time out when sending to this host.
	Retries	The number of times informs will be sent after timing out.

3.10.0.22 show snmp engineID

This command displays the currently configured SNMP engineID.

Format `show snmp engineID`
Mode Privileged EXEC

Parameter	Description
Local SNMP EngineID	The current configuration of the displayed SNMP engineID.

3.10.0.23 show snmp filters

This command displays the configured filters used when sending traps.

Format `show snmp filters [filtername]`
Mode Privileged EXEC

Parameter	Description
Name	The filter name for this entry.
OID Tree	The OID tree this entry will include or exclude.
Type	Indicates if this entry includes or excludes the OID Tree.

3.10.0.24 show snmp group

This command displays the configured groups.

Format `show snmp group [groupname]`
Mode Privileged EXEC

Parameter	Description
Name	The name of the group.
Security Model	Indicates which protocol can access the system via this group.
Security Level	Indicates the security level allowed for this group.
Read View	The view this group provides read access to.
Write View	The view this group provides write access to.
Notify View	The view this group provides trap access to.

3.10.0.25 show snmp-server

This command displays the current SNMP server user configuration.

Format `show snmp-server`
Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing)#show snmp-server

SNMP Server Port.............................. 161
SNMP Trap Send Port........................... 162
Net-SNMP Proxy Mode........................... Enable
```

3.10.0.26 show snmp user

This command displays the currently configured SNMPv3 users.

Format `show snmp user [username]`
Mode Privileged EXEC

Term	Definition
Name	The name of the user.
Group Name	The group that defines the SNMPv3 access parameters.
Auth Method	The authentication algorithm configured for this user.
Privilege Method	The encryption algorithm configured for this user.
Remote Engine ID	The engineID for the user defined on the client machine.

3.10.0.27 show snmp views

This command displays the currently configured views.

Format `show snmp views [viewname]`
Mode Privileged EXEC

Parameter	Description
Name	The view name for this entry.
OID Tree	The OID tree that this entry will include or exclude.
Type	Indicates if this entry includes or excludes the OID tree.

3.10.0.28 show trapflags

This command displays trap conditions. The command's display shows all the enabled OSPFv2 trapflags. Configure which traps the switch should generate by enabling or disabling the trap condition. If a trap condition is enabled and the condition is detected, the SNMP agent on the switch sends the trap to all enabled trap receivers. You do not have to reset the switch to implement the changes. Cold and warm start traps are always generated and cannot be disabled.

Format `show trapflags`
Mode Privileged EXEC

Parameter	Definition
Authentication Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether authentication failure traps will be sent.
Link Up/Down Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether link status traps will be sent.
Multiple Users Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether a trap will be sent when the same user ID is logged into the switch more than once at the same time (either through Telnet or the serial port).
Spanning Tree Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether spanning tree traps are sent.
ACL Traps	May be enabled or disabled. The factory default is disabled. Indicates whether ACL traps are sent.
BGP4 Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether BGP4 traps are sent. (This field appears only on systems with the BGPv4 software package installed.)

Parameter	Definition
OSPFv2 Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether OSPF traps are sent. If any of the OSPF trap flags are not enabled, then the command displays `disabled`. Otherwise, the command shows all the enabled OSPF traps' information.

3.10.0.29 show snmptrap source-interface

Use the `show tacacs source-interface` command in Global Config mode to display the configured global source interface details used for an SNMP client. The IP address of the selected interface is used as source IP for all communications with the server.

Format `show snmptrap source-interface`

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Config)# show snmptrap source-interface

SNMP Client Source Interface     : 0/2
SNMP Client Source IPv4 Address  : 192.168.2.20 [UP]
```

3.11 RADIUS Commands

This section describes the commands you use to configure the switch to use a Remote Authentication Dial-In User Service (RADIUS) server on your network for authentication and accounting.

3.11.0.1 aaa server radius dynamic-author

This command enables CoA functionality and enters dynamic authorization local server configuration mode.

Default None

Format `aaa server radius dynamic-author`

Mode Global Config

Example:

```
(Routing) #configure
(Routing) (Config)#aaa server radius dynamic-author
(Routing) (Config- radius-da)#
```

3.11.0.1.1 no aaa server radius dynamic-author

This command disables CoA functionality.

Default None

Format `no aaa server radius dynamic-author`

Mode Global Config

Example:

```
(Routing) #configure
(Routing) (Config)#no aaa server radius dynamic-author
```

3.11.0.2 authentication command bounce-port ignore

This command configures the device to ignore a RADIUS server `bounce-host-port` command. The `bounce-host-port` command causes a host to flap the link on an authentication port. The link flap causes DHCP renegotiation from one or more hosts connected to this port.

Default FALSE (Bounce-Port messages will be processed)
Format `authentication command bounce-port ignore`
Mode Global Config

Example:

```
(Routing) #configure
(Routing) (Config)#authentication command bounce-port ignore
```

3.11.0.2.1 no authentication command bounce-port ignore

This command resets the device to the default value so that RADIUS server bounce-host-port commands are processed.

Format `no authentication command bounce-port ignore`
Mode Global Config

Example:

```
(Routing) #configure
(Routing) (Config)#no authentication command bounce-port ignore
```

3.11.0.3 auth-type

Use this command to specify the type of authorization that the device uses for RADIUS clients. The client must match the configured attributes for authorization.

Default All
Format `auth-type { any | all | session-key }`
Mode Dynamic Authorization

Example:

```
(Routing) (Config- radius-da)#auth-type all
```

3.11.0.3.1 no auth-type

Use this command to reset the type of authorization that the device must use for RADIUS clients.

Default None
Format `no auth-type`
Mode Dynamic Authorization

Example:

```
(Routing) (Config- radius-da)#no auth-type
```

3.11.0.4 authorization network radius

Use this command to enable the switch to accept VLAN assignment by the radius server.

Default	disable
Format	`authorization network radius`
Mode	Global Config

3.11.0.4.1 no authorization network radius

Use this command to disable the switch to accept VLAN assignment by the radius server.

Format	`no authorization network radius`
Mode	Global Config

3.11.0.5 clear radius dynamic-author statistics

This command clears radius dynamic authorization counters.

Default	None
Format	`clear radius dynamic-author statistics`
Mode	Privileged EXEC

Example:

```
(Routing) #clear radius dynamic-author statistics

Are you sure you want to clear statistics? (y/n) y

Statistics cleared.
```

3.11.0.6 client

Use this command to configure the IP address or hostname of the AAA server client. Use the optional server-key keyword and string argument to configure the server key at the client level.

Default	None
Format	`client { ip-address | hostname } [server-key [0|7] key-string]`
Mode	Dynamic Authorization

Example:

```
(Routing) (Config- radius-da)#client 10.0.0.1 server-key 7  device1
```

3.11.0.6.1 no client

Use this command to remove the configured Dynamic Authorization client and the key associated with that client in the device.

Default	None
Format	`no client { ip-address | hostname }`

Mode Dynamic Authorization

Example:

```
(Routing) (Config- radius-da)#no client 10.0.0.1
```

3.11.0.7 debug aaa coa

Use this command to display Dynamic Authorization Server processing debug information.

Default None
Format `debug aaa coa`
Mode Dynamic Authorization

3.11.0.8 debug aaa pod

Use this command to display Disconnect Message packets.

Default None
Format `debug aaa pod`
Mode Dynamic Authorization

3.11.0.9 ignore server-key

Use this optional command to configure the device to ignore the server key.

Default Disable
Format `ignore server-key`
Mode Dynamic Authorization

Example:

```
(Routing) (Config- radius-da)#ignore server-key
```

3.11.0.9.1 no ignore server-key

Use this optional command to configure the device not to ignore the server key (that is, it resets the ignore server key property on the device).

Default Disable
Format `no ignore server-key`
Mode Dynamic Authorization

Example:

```
(Routing) (Config- radius-da)#no ignore server-key
```

3.11.0.10 ignore session-key

Use this optional command to configure the device to ignore the session key.

Default	Disable
Format	`ignore session-key`
Mode	Dynamic Authorization

Example:

```
(Routing) (Config- radius-da)#ignore session-key
```

3.11.0.10.1 no ignore session-key

Use this optional command to configure the device to not ignore the session key (that is, it resets the ignore session key property on the device).

Default	Disable
Format	`no ignore session-key`
Mode	Dynamic Authorization

Example:

```
(Routing) (Config- radius-da)#no ignore session-key
```

3.11.0.11 port (Dynamic Authorization Mode)

Use this command to specify the UDP port on which a device listens for RADIUS requests from configured Dynamic Authorization clients. The supported range for the port-number is 1025 to 65535.

Default	3799
Format	`port` *`port-number`*
Mode	Dynamic Authorization

Example:

```
(Routing) (Config- radius-da)#port 1700
```

3.11.0.11.1 no port

Use this command to reset the configured UDP port on which a device listens for RADIUS requests from configured Dynamic Authorization clients.

Default	3799
Format	`no port`
Mode	Dynamic Authorization

Example:

```
(Routing) (Config- radius-da)#no port
```

3.11.0.12 radius accounting mode

This command is used to enable the RADIUS accounting function.

Default disabled

Format `radius accounting mode`

Mode Global Config

3.11.0.12.1 no radius accounting mode

This command is used to set the RADIUS accounting function to the default value - i.e. the RADIUS accounting function is disabled.

Format `no radius accounting mode`

Mode Global Config

3.11.0.13 radius server attribute

This command specifies the RADIUS client to use the specified RADIUS attribute in the RADIUS requests. The supported attributes are as follows:

- 4: Include the NAS-IP Address attribute. If the specific IP address is configured while enabling this attribute, the RADIUS client uses that IP address while sending NAS-IP-Address attribute in RADIUS communication.
- 95: Include the NAS-IPV6-Address attribute. If the specific IPv6 address is configured while enabling this attribute, the RADIUS client uses that IPv6 address while sending NAS-IPV6-Address attribute in RADIUS communication.
- 30: This command configures the format in which the MAC address is sent to the RADIUS server in attribute 30.
- 31: This command configures the format in which the MAC address is sent to the RADIUS server in attribute 31 (Calling-Station-ID).
- 32: This command configures the format in which the MAC address is sent to the RADIUS server in attribute 32 (NAS-Identifier).

Default (Attribute 30 and 31 only) MAC address format: legacy lower case

Format `radius server attribute {4 [`*`ipaddr`*`] | 95 [`*`ipv6_addr`*`] | {30 | 31 | 32} mac-format {leagacy `*`lower-case`*` | `*`upper-case`*` | ietf `*`lower-case`*` | `*`upper-case`*` | unformatted `*`lower-case`*` | `*`upper-case`*` }}`

Mode Global Config

Parameter	Definition
4	NAS-IP-Address attribute to be used in RADIUS requests.
ipaddr	The IP address of the server.
ipv6_addr	The IPv6 address of the server.
ietf	**Format the MAC address as xx-xx-xx-xx-xx-xx.**
legacy	**Format the MAC address as xx:xx:xx:xx:xx:xx**
unformatted	**Format the MAC address as aaaabbbbcccc.**

Example: The following shows an example of the command.

```
(Switch) (Config) #radius server attribute 4  192.168.37.60
```

Example: The following shows an example of the command.

```
(Switch) (Config) #(Config)#radius server attribute 95 3ffe:ffff:100:f101::1
```

Example: The following shows an example of the command.

```
(Switch) (Config) #(Config)#radius server attribute 31 mac-format unformatted lower-case
```

3.11.0.13.1 no radius server attribute

The `no` version of this command resets the RADIUS attributes to their default values. For attributes 4 and 95, this command disables the specified attribute global parameter for the RADIUS client. When this parameter is disabled, the RADIUS client does not send the NAS-IP-Address or NAS-IPv6-Address attribute in RADIUS requests.

Format `no radius server attribute {4 [ipaddr] | 95 [ipv6_addr] | {30 | 31 | 32} mac-format}`
Mode Global Config

3.11.0.14 radius server attribute 32 include-in-access-req

When this command is configured with the `32` option, the RADIUS attribute 32 (NAS-Identifier) is sent to the RADIUS server in access-request and accounting-request messages. The `format` option specifies the RADIUS Attribute 32 format. If the format is not configured, a default format (%m) is used.

Default Attribute is not sent
Format `radius server attribute 32 include-in-access-req [format format]`
Mode Global Config

Term	Definition
format	The format value can be 2 to 128 characters or one or more of the following: ■ %m: MAC address ■ %i: IP address ■ %h: Host Name ■ %d: Domain Name.

Example: The following shows an example of the command.

```
(Switch) (Config) #(Config)#radius server attribute 32 include-in-access-req format %i
```

3.11.0.14.1 no radius server attribute 32 include-in-access-req

This command disables sending RADIUS attribute 32.

Format `no radius server attribute 32 include-in-access-req`
Mode Global Config

3.11.0.15 radius server attribute 44 include-in-access-req

When this command is configured with the `44` option, the RADIUS attribute 44 (Accounting-Session-ID) is sent to the RADIUS server in access-request messages. The same accounting session ID is used in the subsequent accounting requests sent to the RADIUS server.

Default Attribute is not sent
Format `radius server attribute 44 include-in-access-req`
Mode Global Config

3.11.0.15.1 no radius server attribute include-in-access-req

This command disables sending RADIUS attribute 44.

Format `no radius server attribute 44 include-in-access-req`
Mode Global Config

3.11.0.16 radius server deadtime

This command configures the dead time (in minutes) for all RADIUS authentication servers. The dead time is the amount of time to skip a RADIUS server that is not responding to authentication requests. The valid deadtime range is 0 to 2000 minutes.

Default 0
Format `radius server deadtime` *`minutes`*
Mode Global Config

3.11.0.16.1 no radius server deadtime

This command resets the deadtime for all RADIUS authentication servers to the default value.

Format `no radius server deadtime`
Mode Global Config

3.11.0.17 radius server dead-criteria

This command configures the condition under which a RADIUS server is considered to be dead. The criteria configured for both the dead time and the number of tries need to be satisfied before a RADIUS server is consider as unavailable.

Default Time: 20 seconds
Tries 4
Format `radius server dead-criteria time` *`seconds`* `tries` *`tries`*
Mode Global Config

Term	Definition
time	Number of seconds during which a RADIUS client need not get a valid response from the RADIUS server. The valid range is 1 to 120 seconds.
tries	Number of times that a RADIUS client attempts to get a valid response before the RADIUS server is considered as unavailable. The valid range is 1 to 100.

Example:

```
(Switch) (Config)# radius server dead-criteria time 40 tries 6
```

3.11.0.17.1 no radius server dead-criteria

This command resets the dead criteria for all RADIUS servers to the default value.

Format `no radius server dead-criteria {time | tries}`

Mode Global Config

3.11.0.18 radius server host

This command configures the IPv4/IPv6 address or DNS name to use for communicating with the RADIUS server of a selected server type. While configuring the IPv4/IPv6 address or DNS name for the authenticating or accounting servers, you can also configure the deadtime, port number, and server name. If the authenticating and accounting servers are configured without a name, the command uses the Default_RADIUS_Auth_Server and Default_RADIUS_Acct_Server as the default names, respectively. The same name can be configured for more than one authenticating servers and the name should be unique for accounting servers. The RADIUS client allows the configuration of a maximum 32 authenticating and accounting servers.

If you use the *auth* parameter, the command configures the IPv4/IPv6 address or hostname to use to connect to a RADIUS authentication server. You can configure up to 3 servers per RADIUS client. If the maximum number of configured servers is reached, the command fails until you remove one of the servers by issuing the “no” form of the command. If you use the optional *port* parameter, the command configures the UDP port number to use when connecting to the configured RADIUS server. The *port* number range is 1 to 65535, with 1812 being the default value. If you use the optional `deadtime` parameter, the command configures the deadtime to use for the configured RADIUS server. The deadtime value is 0 to 2000 (in minutes), with 0 being the default.

NOTE: To reconfigure a RADIUS authentication server to use the default UDP *port*, set the *port* parameter to 1812.

If you use the *acct* token, the command configures the IPv4/IPv6 address or hostname to use for the RADIUS accounting server. You can only configure one accounting server. If an accounting server is currently configured, use the “no” form of the command to remove it from the configuration. The IPv4/IPv6 address or hostname you specify must match that of a previously configured accounting server. If you use the optional *port* parameter, the command configures the UDP port to use when connecting to the RADIUS accounting server. If a *port* is already configured for the accounting server, the new *port* replaces the previously configured *port*. The *port* must be a value in the range 0 to 65535, with 1813 being the default. If you use the optional `deadtime` parameter, the command configures the deadtime to use for the configured RADIUS server. The deadtime value is 0 to 2000 (in minutes), with 0 being the default.

NOTE: To reconfigure a RADIUS accounting server to use the default UDP *port*, set the *port* parameter to 1813.

Format `radius server host {auth | acct} {`***ipaddr*** `|` ***ipv6addr*** `|` ***dnsname***`} [name` ***servername***`] [port` ***0-65535***`] [deadtime` ***0-2000***`]`

Mode Global Config

Field	Description
ipaddr	The IP address of the server.
ipv6addr	The IPv6 address of the server.
dnsname	The DNS name of the server.
0-65535	The port number to use to connect to the specified RADIUS server.
servername	The alias name to identify the server.
deadtime	The amount of time to skip a RADIUS server that is not responding to authentication requests. The valid deadtime range is 0 to 2000 minutes

3.11.0.18.1 no radius server host

The no version of this command deletes the configured server entry from the list of configured RADIUS servers. If the RADIUS authenticating server being removed is the active server in the servers that are identified by the same server name, then the RADIUS client selects another server for making RADIUS transactions. If the 'auth' token is used, the previously configured RADIUS authentication server is removed from the configuration. Similarly, if the 'acct' token is used, the previously configured RADIUS accounting server is removed from the configuration. The *ipaddr | ipv6addr | dnsname* parameter must match the IPv4/IPv6 address or DNS name of the previously configured RADIUS authentication / accounting server.

Format `no radius server host {auth | acct} {`*`ipaddr | ipv6addr | dnsname`*`}`

Mode Global Config

Example: The following shows an example of the command.

```
(Switch) (Config) #radius server host acct 192.168.37.60
(Switch) (Config) #radius server host acct 192.168.37.60 port 1813
(Switch) (Config) #radius server host auth 192.168.37.60 name Network1_RS port 1813
(Switch) (Config) #radius server host acct 192.168.37.60 name Network2_RS
(Switch) (Config) #no radius server host acct 192.168.37.60
```

3.11.0.19 radius server host link-local

This command configures the link-local-address of the RADIUS server and the outgoing interface to be used by the RADIUS client to communicate with the RADIUS server. The outgoing interface can be any physical interface or service port or network port.

Default None

Format `radius server host {auth | acct} link-local` *`link-local-address`* `interface {`*`slot/port`* `| network | serviceport } [name` *`servername`*`] [port` *`port`*`]`

Mode Global Config

Field	Description
link-local-address	The IP address of the server.
interface	The interface for the RADIUS client to use for outgoing RADIUS messages.
servername	The alias name to identify the server.
port	The port number to use to connect to the specified RADIUS server.

Example: The following shows an examples of the command.

```
(Routing) (Config) #radius server host auth link-local fe80::208:a1ff:fe7e:4519 interface network name
auth_server  port 1813

 (Routing) (Config) #radius server host acct link-local fe80::208:a1ff:fe7e:4519 interface serviceport
name acct_server port 1813
```

3.11.0.19.1 no radius server host link-local

This command removes the configured radius server link-local-address.

Default None

Format `radius server host {auth | acct} link-local` *`link-local-address`*

Mode Global Config

Example: The following shows an examples of the command.

```
(Routing) (Config) #no radius server host auth link-local fe80::208:a1ff:fe7e:4519
```

3.11.0.20 radius server host test

This command configures automated tests for configured RADIUS servers. When a test user name is configured for a RADIUS server, the client sends periodic test probes to the server. The RADIUS server responds with a reject message. The receipt of a response is an indication of liveliness of the server. Test probes are sent to server based configured time interval in minutes, idle time.

Default Idle time: 60 minutes

Format `radius server host {auth | acct} {`*`ipaddr`* `|` *`ipv6addr`* `|` *`hostname`*`} test username` *`name`* `[deadtime` *`0-2000`*`] [idle-time` *`1-35791`*`] [name` *`servername`*`] [port` *`1-65535`*`]`

Mode Global Config

Field	Description
ipaddr	The IP address of the server.
ipv6addr	The IPv6 address of the server.
hostname	The host name of the server.
username	RADIUS server test user name.
deadtime	The amount of time to skip a RADIUS server that is not responding to authentication requests. The valid deadtime range is 0 to 2000 minutes.
idle-time	The number of minutes between test probes, which is in the range of 1 to 35792 minutes.
name	Identification name to the server.
port	A Layer 4 port number in the range of 1 to 65535 (the default is 1813).

Example:

```
(Routing)(Config)# radius server acct 10.22.11.33 test username dummy idle-time 2
```

3.11.0.20.1 no radius server host test

This command disables RADIUS server test user name. It can also be used to set server idle-time to default value.

Format `no radius server host {auth | acct} {`*`ipaddr`* `|` *`ipv6addr`* `|` *`hostname`*`} test username`

Mode Global Config

3.11.0.21 radius server key

This command configures the key to be used in RADIUS client communication with the specified server. The key can be configured for all RADIUS servers or, depending on whether the `auth` or `acct` token is used, the shared secret is configured for the particular RADIUS authentication or accounting server. The IP address or IPv6 address or hostname, when provided, must match a previously configured server. When this command is executed, the secret is prompted.

Text-based configuration supports RADIUS server's secrets in encrypted and non-encrypted format. When you save the configuration, these secret keys are stored in encrypted format only. If you want to enter the key in encrypted format, enter the key along with the encrypted keyword. In the Section 4.5.0.24, show running-config command's display, these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

NOTE: The secret must be an alphanumeric value not exceeding 64 characters.

Format `radius server key [auth | acct | encrypted password] {ipaddr | ipv6addr | hostname} encrypted password`

Mode Global Config

Field	Description
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.
password	The password in encrypted format.

Example: The following shows an example of the CLI command.

```
radius server key acct 10.240.4.10 encrypted encrypt-string
```

3.11.0.21.1 no radius server key

This command removes the shared secret used for the RADIUS servers.

Format `no radius server key [{acct | auth} {ipaddr | ipv6address | hostname} ]`

Mode Global Config

3.11.0.22 radius server load-balance

This command configures the load balancing algorithm used by the RADIUS client to manage authentication and accounting requests sent to configured RADIUS servers. Load balancing configuration is configured for a group of RADIUS servers or global default RADIUS server group. A server group is identified as a group of RADIUS servers using the same configured server name.

The supported load balancing method is based on the least number of outstanding requests. In this mode, the RADIUS client selects a configured RADIUS server that has the least number of pending requests. Before selecting a new server, the number of pending requests on the current server in use should be more than configured batch size value.

Default Method: None
Batch size: 25

Format `radius server load-balance {acct | auth} {name servername | radius} method {least-outstanding [batch-size 1-2147483647] | none}`

Mode Global Config

Field	Description
acct	Configure the RADIUS accounting server group.
auth	Configure the RADIUS authentication server group.
name	The RADIUS server group name.

Field	Description
radius	Server using default identification name.
method	Load balance based on the lowest number of outstanding requests.
none	Do not load balance.

Example:

```
(Routing) (Config)# radius server load-balance acct name group1 method least-outstanding batch-size 40
(Routing) (Config)# radius server load-balance auth radius method least-outstanding batch-size 30
```

3.11.0.22.1 no radius server load-balance

The no version of this command disables the load balancing algorithm to be used for the specified RADIUS server.

Format `no radius server load-balance {auth | acct} {radius | name` *`servername`*`} method`
Mode Global Config

3.11.0.23 radius server msgauth

This command enables the message authenticator attribute to be used for the specified RADIUS Authenticating server.

Format `radius server msgauth {`*`ipaddr`* | *`ipv6addr`* | *`dnsname`*`}`
Mode Global Config

Parameter	Description
ip addr	The IP address of the server.
ipv6addr	The IPv6 address of the server.
dnsname	The DNS name of the server.

3.11.0.23.1 no radius server msgauth

The no version of this command disables the message authenticator attribute to be used for the specified RADIUS Authenticating server.

Format `no radius server msgauth {`*`ipaddr`* | *`ipv6addr`* | *`dnsname`*`}`
Mode Global Config

3.11.0.24 radius server primary

This command specifies a configured server that should be the primary server in the group of servers which have the same server name. Multiple primary servers can be configured for each number of servers that have the same name. When the RADIUS client has to perform transactions with an authenticating RADIUS server of specified name, the client uses the primary server that has the specified server name by default. If the RADIUS client fails to communicate with the primary server for any reason, the client uses the backup servers configured with the same server name. These backup servers are identified as the Secondary type.

Format `radius server primary {`*`ipaddr`* | *`ipv6addr`* | *`dnsname`*`}`

Mode Global Config

Parameter	Description
ip addr	The IP address of the RADIUS Authenticating server.
ipv6addr	The IPv6 address of the server.
dnsname	The DNS name of the server.

3.11.0.25 radius server retransmit

This command configures the global parameter for the RADIUS client that specifies the number of transmissions of the messages to be made before attempting the fall back server upon unsuccessful communication with the current RADIUS authenticating server. When the maximum number of retries are exhausted for the RADIUS accounting server and no response is received, the client does not communicate with any other server.

Default 4

Format `radius server retransmit` *`retries`*

Mode Global Config

Parameter	Description
retries	The maximum number of transmission attempts in the range of 1 to 15.

3.11.0.25.1 no radius server retransmit

The no version of this command sets the value of this global parameter to the default value.

Format `no radius server retransmit`

Mode Global Config

3.11.0.26 radius source-interface

Use this command to specify the physical or logical interface to use as the RADIUS client source interface (Source IP address). If configured, the address of source Interface is used for all RADIUS communications between the RADIUS server and the RADIUS client. The selected source-interface IP address is used for filling the IP header of RADIUS management protocol packets. This allows security devices (firewalls) to identify the source packets coming from the specific switch.

If a source-interface is not specified, the primary IP address of the originating (outbound) interface is used as the source address. If the configured interface is down, the RADIUS client falls back to its default behavior.

Format `radius source-interface {`*`slot/port`* `| loopback` *`loopback-id`* `|` *`vlan vlan-id`*`}`

Mode Global Config

Parameter	Description
slot/port	Specifies the port to use as the source interface.
loopback-id	Specifies the loopback interface to use as the source interface. The range of the loopback ID is 0 to 7.

Parameter	Description
vlan-id	Specifies the VLAN to use as the source interface.

3.11.0.26.1 no radius source-interface

Use this command to reset the RADIUS source interface to the default settings.

Format `no radius source-interface`
Mode Global Config

3.11.0.27 radius server timeout

This command configures the global parameter for the RADIUS client that specifies the timeout value (in seconds) after which a request must be retransmitted to the RADIUS server if no response is received. The timeout value is an integer in the range of 1 to 30.

Default 5
Format `radius server timeout` *`seconds`*
Mode Global Config

Parameter	Description
retries	Maximum number of transmission attempts in the range 1–30.

3.11.0.27.1 no radius server timeout

The no version of this command sets the timeout global parameter to the default value.
Format `no radius server timeout`
Mode Global Config

3.11.0.28 server-key

Use this command to configure a global shared secret that is used for all dynamic authorization clients that do not have an individual shared secret key configured.

Default None
Format `server-key [7]` *`key-string`*
Mode Dynamic Authorization

Term	Definition
0	An unencrypted key is to be entered
7	An encrypted key is to be entered
string	The shared secret string. Maximum length is 128 characters for unencrypted key and 256 characters for encrypted key. Overrides the global setting for this client only. Enclose in quotes to use special characters or embedded blanks.

Example:

```
(Routing) (Config-radius-da)# server-key encrypted mydevice
```

3.11.0.28.1 no server-key

Use this command to remove the global shared secret key configuration.

Default None

Format `no server-key`

Mode Dynamic Authorization

Example:

```
(Routing) (Config-radius-da)#no server-key
```

3.11.0.29 radius server vsa send

This command enables the processing of Cisco dynamic ACL vendor-specific attributes sent by the RADIUS server. Use the authentication keyword to allow the processing of attributes for authentication.

Default Disabled

Format `radius server vsa send [authentication]`

Mode Global Config

3.11.0.29.1 no radius vsa send

The no version of this command sets the Cisco dynamic VSA processing to the default value.

Format `no radius server vsa send [authentication]`

Mode Global Config

3.11.0.30 show radius

This command displays the values configured for the global parameters of the RADIUS client.

Format `show radius`

Mode Privileged EXEC

Term	Definition
Number of Configured Authentication Servers	The number of RADIUS Authentication servers that have been configured.
Number of Configured Accounting Servers	The number of RADIUS Accounting servers that have been configured.
Number of Named Authentication Server Groups	The number of configured named RADIUS server groups.
Number of Named Accounting Server Groups	The number of configured named RADIUS server groups.

Term	Definition
Number of Dead RADIUS Authentication Servers	The number of RADIUS authentication servers that are considered to be unresponsive based on the dead-time criteria.
Number of Dead RADIUS Accounting Servers	The number of RADIUS accounting servers that are considered to be unresponsive based on the dead-time criteria.
Number of Retransmits	The configured value of the maximum number of times a request packet is retransmitted.
Dead Time	The amount of time to skip a RADIUS server that is not responding to authentication requests.
Dead Criteria Time	Number of seconds during which a RADIUS client need not get a valid response from the RADIUS server.
Dead Criteria Tries	Number of times that a RADIUS client attempts to get a valid response before the RADIUS server is considered as unavailable.
Timeout Duration	The configured timeout value, in seconds, for request retransmissions.
RADIUS Accounting Mode	A global parameter to indicate whether the accounting mode for all the servers is enabled or not.
RADIUS Attribute 4 Mode	A global parameter to indicate whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.
RADIUS Attribute 4 Value	A global parameter that specifies the IP address to be used in the NAS-IP-Address attribute to be used in RADIUS requests.
RADIUS Attribute 95 Mode	A global parameter to indicate whether the NAS-IPv6-Address attribute has been enabled to use in RADIUS requests.
RADIUS Attribute 95 Value	A global parameter that specifies the IPv6 address to be used in the NAS-IPv6-Address attribute to be used in RADIUS requests.
RADIUS Attribute 30 MAC Format	The format in which the MAC address is sent to the RADIUS server in attribute 30.
RADIUS Attribute 31 MAC Format	The format in which the MAC address is sent to the RADIUS server in attribute 31 (Calling-Station-ID).
RADIUS Attribute 32 MAC Format	The format in which the MAC address is sent to the RADIUS server in attribute 32 (NAS-Identifier).
RADIUS Attribute 32 include in access request	Indicates whether RADIUS attribute 32 is sent to the RADIUS server in access-request and accounting-request messages.
RADIUS Attribute 32 format	The format for RADIUS attribute 32, which is one or more of the following: ■ %m: MAC address ■ %i: IP address ■ %h: Host Name ■ %d: Domain Name.
RADIUS Attribute 44 include in access request	Indicates whether RADIUS attribute 44 is sent to the RADIUS server in access-request and accounting-request messages.

Example: The following shows example CLI display output for the command.

```
(Switch) #show radius

Number of Configured Authentication Servers.... 1
Number of Configured Accounting Servers........ 1
Number of Named Authentication Server Groups... 1
Number of Named Accounting Server Groups....... 1
Number of Dead RADIUS Authentication Servers... 0
Number of Dead RADIUS Accounting Servers....... 0
Number of Retransmits.......................... 4
Dead Time...................................... 0
Dead Criteria Time............................. 20
Dead Criteria Tries............................ 4
```

```
Timeout Duration.............................. 5
RADIUS Accounting Mode........................ Disable
RADIUS Attribute 4 Mode....................... Disable
RADIUS Attribute 4 Value...................... 0.0.0.0
RADIUS Attribute 95 Mode...................... Disable
RADIUS Attribute 95 Value..................... ::
RADIUS Attribute 30 Mac Format................ legacy lower-case
RADIUS Attribute 31 Mac Format................ ietf upper-case
RADIUS Attribute 32 Mac Format................ legacy lower-case
RADIUS Attribute 32 include in access request.. Enable
RADIUS Attribute 32 format.................... %i.%d.%m
RADIUS Attribute 44 include in access request.. Disable
```

3.11.0.31 show radius servers

This command displays the summary and details of RADIUS authenticating servers configured for the RADIUS client.

Format `show radius servers [{`*`ipaddr`* `|` *`ipv6addr`* `|` *`dnsname`*`} | name [`*`servername`*`]}]`

Mode Privileged EXEC

Parameter	Description
Command Variables	
ipaddr	The IP address of the authenticating server.
ipv6addr	The IPv6 address of the server.
dnsname	The DNS name of the authenticating server.
servername	The alias name to identify the server.
Command Output Fields	
Current	The * symbol preceding the server host address specifies that the server is currently active.
Host Address	The IP address of the host.
Server Name	The name of the authenticating server.
Port	The port used for communication with the authenticating server.
Type	Specifies whether this server is a primary or secondary type.
Current Host Address (*)	An asterisk (*) indicates which configured RADIUS host is the currently active authenticating server.
Number of Retransmits	The configured value of the maximum number of times a request packet is retransmitted.
Dead Time	The amount of time to skip a RADIUS server that is not responding to authentication requests.
Timeout Duration	The configured timeout value, in seconds, for request retransmissions.
RADIUS Server VSA Authentication	Indicates whether the system processes Cisco dynamic ACL vendor-specific attributes sent by RADIUS Server.
Server State	The administrative state of the RADIUS server.
Server Immortal State	Indicates whether the server is an *immortal* RADIUS server, which is a dead server that is marked as alive after being determined to be dead because it is the last server known to be alive
Test User	The name of the configured RAIDUS server test user.
Idle Time	The number of minutes between RADIUS server test probes,
RADIUS Accounting Mode	A global parameter to indicate whether the accounting mode for all the servers is enabled or not.
RADIUS Attribute 4 Mode	A global parameter to indicate whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.

Parameter	Description
RADIUS Attribute 4 Value	A global parameter that specifies the IP address to be used in NAS-IP-Address attribute used in RADIUS requests.
RADIUS Attribute 95 Mode	A global parameter to indicate whether the NAS-IPv6-Address attribute has been enabled to use in RADIUS requests.
RADIUS Attribute 95 Value	A global parameter that specifies the IPv6 address to be used in the NAS-IPv6-Address attribute to be used in RADIUS requests.
RADIUS Attribute 30 MAC Format	The format in which the MAC address is sent to the RADIUS server in attribute 30.
RADIUS Attribute 31 MAC Format	The format in which the MAC address is sent to the RADIUS server in attribute 31 (Calling-Station-ID).
RADIUS Attribute 32 MAC Format	The format in which the MAC address is sent to the RADIUS server in attribute 32 (NAS-Identifier).
RADIUS Attribute 32 include in access request	Indicates whether RADIUS attribute 32 is sent to the RADIUS server in access-request and accounting-request messages.
RADIUS Attribute 32 format	The format for RADIUS attribute 32, which is one or more of the following: ■ %m: MAC address ■ %i: IP address ■ %h: Host Name ■ %d: Domain Name.
RADIUS Attribute 44 include in access request	Indicates whether RADIUS attribute 44 is sent to the RADIUS server in access-request and accounting-request messages.
Link local interface	If configured, the link local IPv6 address.
Secret Configured	Yes or No Boolean value that indicates whether this server is configured with a secret.
Message Authenticator	A global parameter to indicate whether the Message Authenticator attribute is enabled or disabled.
CoA Bounce-Host-Port	Indicates whether RADIUS server Bounce-Port messages will be processed (Accept) or ignored.
Number of CoA Requests Received	The number of RADIUS Change of Authorization (CoA) requests messages received from a RADIUS host.
Number of CoA ACK Responses Sent	The number of RADIUS CoA acknowledgments the client has sent.
Number of CoA NAK Responses Sent	The number of RADIUS CoA non-acknowledgments the client has sent.
Number of CoA Requests Ignored	The number of RADIUS CoA requests the client has ignored.
Number of CoA Missing/ Unsupported Attribute R	The number of RADIUS CoA requests the client has received that have a missing or unsupported attribute value.
Number of CoA Session Context Not Found Request	The number of RADIUS CoA requests the client has received in which the session context identified in the CoA-Request or not exist on the NAS.
Number of CoA Invalid Attribute Value Request	The number of RADIUS CoA requests the client has received that have an invalid attribute value.
Number of Administratively Prohibited Request	The number of RADIUS CoA requests the client has received that where the NAS is configured to prohibit honoring of CoA-Request or Disconnect- Request packets for the specified session.
Number of Dead servers in Named Server Group	When the `name servername` options are used, this field shows the number of RADIUS servers in the named server group that are determined to be dead.

Example: The following shows example CLI display output for the command.

```
(Switch) #show radius servers

Cur  Host Address              Server Name                       Port  Type
rent
---- ----------------------- --------------------------------- ----- ----------
     *   192.168.37.200           Network1_RADIUS_Server            1813  Primary
      192.168.37.201           Network2_RADIUS_Server            1813  Secondary
```

```
     192.168.37.202           Network3_RADIUS_Server            1813  Primary
     192.168.37.203           Network4_RADIUS_Server            1813  Secondary

(Switch) #show radius servers name

Current Host Address     Server Name                       Type
------------------------ --------------------------------- ----------192.168.37.200
Network1_RADIUS_Server           Secondary
192.168.37.201           Network2_RADIUS_Server            Primary
192.168.37.202           Network3_RADIUS_Server            Secondary
192.168.37.203           Network4_RADIUS_Server            Primary

(Switch) #show radius servers 2.2.2.2

RADIUS Server Name..............................  Default-RADIUS-Server
Current Server IP Address.......................  2.2.2.2
Number of Retransmits...........................  4
Dead Time.......................................  0
Timeout Duration................................  5
RADIUS Server VSA Authentication................  Enable
Server State....................................  Up
Server Immortal State...........................  False
Load Balance....................................  Disable
Test User.......................................
Idle Time.......................................  60
RADIUS Accounting Mode..........................  Disable
RADIUS Attribute 4 Mode.........................  Disable
RADIUS Attribute 4 Value........................  0.0.0.0
RADIUS Attribute 30 Mac Format..................  legacy lower-case
RADIUS Attribute 31 Mac Format..................  legacy lower-case
RADIUS Attribute 32 Mac Format..................  legacy lower-case
RADIUS Attribute 32 include in access request..  Disable
RADIUS Attribute 32 format......................  %m
RADIUS Attribute 44 include in access request..  Disable
Port............................................  1812
Type............................................  Secondary
Secret Configured...............................  Yes
Message Authenticator...........................  Enable
CoA Bounce-Host-Port............................  Accept
Number of CoA Requests Received.................  0
Number of CoA ACK Responses Sent................  0
Number of CoA NAK Responses Sent................  0
Number of CoA Requests Ignored..................  0
Number of CoA Missing/Unsupported Attribute R..  0
Number of CoA Session Context Not Found Reque..  0
Number of CoA Invalid Attribute Value Request..  0
Number of Administratively Prohibited Request..  0
```

3.11.0.32 show radius accounting

This command displays a summary of configured RADIUS accounting servers.

Format `show radius accounting {name [servername] | ipaddr | ipv6address | hostname}`

Mode Privileged EXEC

Field	Description
servername	An alias name to identify the server.
ipaddr	The IPv4 address of the server.
ipv6address	the IPv6 address of the server.
hostname	The DNS resolvable hostname of the server.

If you use the `name` parameter without the *`servername`* option, then only the accounting mode and the RADIUS accounting server details are displayed.

Parameter	Definition
Server Name	The name of the accounting server.
Host Address	The IP address or configured name of the host.
Port	The port used for communication with the accounting server.
Secret Configured	Yes or No Boolean value indicating whether this server is configured with a secret.

Example: The following shows example CLI display output for the command.

```
(Routing) #show radius accounting name

Server Name                     Host Address             Port   Secret
                                                                Configured
------------------------------- ------------------------ ------ ----------
Default-RADIUS-Server           acctServer               1813   No
backupAcct                      192.168.10.55            1813   No
testServer                      fe80::1                  1813   No
```

If you specify the hostname, IPv4 or IPv6 address of the accounting server, the following RADIUS accounting server details are displayed.

Parameter	Definition
RADIUS Accounting Server IP Address	The IPv4 address, IPv6 address, link local address, or configured hostname of the host.
RADIUS Accounting Server Name	The name of the accounting server.
RADIUS Accounting Mode	The mode of the accounting server.
Link local interface	If configured, the interface associated with the link-local IPv6 address.
Port	The port used for communication with the accounting server.
Secret Configured	Yes or No Boolean value indicating whether this server is configured with a secret.
Server State	The administrative state of the server.
Server Immortal State	Indicates whether the server is an *immortal* RADIUS server, which is a dead server that is marked as alive after being determined to be dead because it is the last server known to be alive
Test User	The name of the configured RAIDUS server test user.
Idle Time	The number of minutes between RADIUS server test probes,
Number of Dead servers in Named Server Group	When the `name servername` options are used, this field shows the number of RADIUS servers in the named server group that are determined to be dead.

Example:

```
(Routing) #show radius accounting acctServer
```

```
RADIUS Accounting Server IP Address..... 192.168.10.55
RADIUS Accounting Server Name.......... backupAcct
RADIUS Accounting Mode................. Disable
Link local interface................... Not Available
Port................................... 1813
Secret Configured...................... No
Server State........................... Up
Server Immortal State.................. False
Test User.............................. testUser
Idle Time.............................. 3233

(Routing) #show radius accounting fe80::1

RADIUS Accounting Server IP Address..... fe80::1
RADIUS Accounting Server Name.......... testServer
RADIUS Accounting Mode................. Disable
Link local interface................... 0/3
Port................................... 1813
Secret Configured...................... No
Server State........................... Up
Server Immortal State.................. False
Test User.............................. testUser
Idle Time.............................. 3233
```

3.11.0.33 show radius accounting servers

This command displays the configured RADIUS accounting servers and its name.

Format `show radius accounting servers`

Mode Privileged EXEC

The command displays the information the following table describes.

Parameter	Definition
Selected Server	If an asteristk (*) appears in the first column, the RADIUS accounting server is the primary server for its group.
Host Address	The IPv4 address, IPv6 address, link local address, or configured hostname of the host.
Server Name	The name of the accounting server.
Port	The port used for communication with the accounting server.

Example: The following shows example CLI display output for the command.

```
(Routing) #show radius accounting servers
*  Host Address              Server Name                      Port
---- ----------------------- -------------------------------- ---
  *  10.25.4.10              group1                             1813
  *  10.25.4.5               Default-RADIUS-Server              1813
     10.25.4.4               group1                             1813

 * currently selected server
```

3.11.0.34 show radius accounting statistics

This command displays a summary of statistics for the configured RADIUS accounting servers.

Format `show radius accounting statistics{`*`ipaddr`* | *`ipv6addr`* | *`dnsname`* | `name` *`servername`*`}`

Mode Privileged EXEC

Parameter	Definition
ipaddr	The IP address of the server.
ipv6addr	The IPv6 address of the server.
dnsname	The DNS name of the server.
servername	The alias name to identify the server.
RADIUS Accounting Server Name	The name of the accounting server.
Server Host Address	The IP address of the host.
Round Trip Time	The time interval, in hundredths of a second, between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
Requests	The number of RADIUS Accounting-Request packets sent to this server. This number does not include retransmissions.
Retransmission	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server.
Responses	The number of RADIUS packets received on the accounting port from this server.
Malformed Responses	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed accounting responses.
Bad Authenticators	The number of RADIUS Accounting-Response packets containing invalid authenticators received from this accounting server.
Pending Requests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response.
Timeouts	The number of accounting timeouts to this server.
Unknown Types	The number of RADIUS packets of unknown types, which were received from this server on the accounting port.
Packets Dropped	The number of RADIUS packets received from this server on the accounting port and dropped for some other reason.

Example: The following shows example CLI display output for the command.

```
(Routing) #show radius accounting statistics 192.168.37.200

RADIUS Accounting Server Name.................. Default_RADIUS_Server
Host Address................................... 192.168.37.200
Round Trip Time................................ 0.00
Requests....................................... 0
Retransmissions................................ 0
Responses...................................... 0
Malformed Responses............................ 0
Bad Authenticators............................. 0
Pending Requests............................... 0
Timeouts....................................... 0
Unknown Types.................................. 0
Packets Dropped................................ 0

(Routing) #show radius accounting statistics name Default_RADIUS_Server
```

```
RADIUS Accounting Server Name.................. Default_RADIUS_Server
Host Address................................... 192.168.37.200
Round Trip Time................................ 0.00
Requests....................................... 0
Retransmissions................................ 0
Responses...................................... 0
Malformed Responses............................ 0
Bad Authenticators............................. 0
Pending Requests............................... 0
Timeouts....................................... 0
Unknown Types.................................. 0
Packets Dropped................................ 0
```

3.11.0.35 show radius source-interface

Use the `show radius source-interface` command in Global Config mode to display the configured global source interface details used for a RADIUS client. The IP address of the selected interface is used as source IP for all communications with the server.

Format `show radius source-interface`

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Router)#show radius source-interface

RADIUS Client Source Interface................. 0/1
RADIUS Client Source IPv4 Address.............. 192.168.0.1            [Up]
RADIUS Client Source IPv6 Address.............. 200:23::12             [Up]
```

3.11.0.36 show radius statistics

This command displays the summary statistics of configured RADIUS Authenticating servers.

Format `show radius statistics {`*`ipaddr`* | *`ipv6addr`* | *`dnsname`* | `name` *`servername`*`}`

Mode Privileged EXEC

Parameter	Definition
ipaddr	The IP address of the server.
ipv6addr	The IPv6 address of the server.
dnsname	The DNS name of the server.
servername	The alias name to identify the server.
RADIUS Server Name	The name of the authenticating server.
Server Host Address	The IP address of the host.
Access Requests	The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.
Access Retransmissions	The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.
Access Accepts	The number of RADIUS Access-Accept packets, including both valid and invalid packets, that were received from this server.
Access Rejects	The number of RADIUS Access-Reject packets, including both valid and invalid packets, that were received from this server.

Parameter	Definition
Access Challenges	The number of RADIUS Access-Challenge packets, including both valid and invalid packets, that were received from this server.
Malformed Access Responses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed access responses.
Bad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.
Pending Requests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.
Timeouts	The number of authentication timeouts to this server.
Unknown Types	The number of packets of unknown type that were received from this server on the authentication port.
Packets Dropped	The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

Example: The following shows example CLI display output for the command.

```
(Routing) #show radius statistics 192.168.37.200

RADIUS Server Name..................................... Default_RADIUS_Server
Server Host Address.................................... 192.168.37.200
Access Requests........................................ 0.00
Access Retransmissions................................. 0
Access Accepts......................................... 0
Access Rejects......................................... 0
Access Challenges...................................... 0
Malformed Access Responses............................. 0
Bad Authenticators..................................... 0
Pending Requests....................................... 0
Timeouts............................................... 0
Unknown Types.......................................... 0
Packets Dropped........................................ 0

(Routing) #show radius statistics name Default_RADIUS_Server

RADIUS Server Name..................................... Default_RADIUS_Server
Server Host Address.................................... 192.168.37.200
Access Requests........................................ 0.00
Access Retransmissions................................. 0
Access Accepts......................................... 0
Access Rejects......................................... 0
Access Challenges...................................... 0
Malformed Access Responses............................. 0
Bad Authenticators..................................... 0
Pending Requests....................................... 0
Timeouts............................................... 0
Unknown Types.......................................... 0
Packets Dropped........................................ 0
```

3.12 TACACS+ Commands

TACACS+ provides access control for networked devices via one or more centralized servers. Similar to RADIUS, this protocol simplifies authentication by making use of a single database that can be shared by many clients on a large network. TACACS+ is based on the TACACS protocol (described in RFC1492) but additionally provides for separate authentication, authorization, and accounting services. The original protocol was UDP based with messages passed in clear text over the network; TACACS+ uses TCP to ensure reliable delivery and a shared key configured on the client and daemon server to encrypt all messages.

3.12.0.1 tacacs-server host

Use the `tacacs-server host` command in Global Configuration mode to configure a TACACS+ server. This command enters into the TACACS+ configuration mode. Use the *`ip-address`*, *`ipv6-address`*, or *`hostname`* parameter to specify the IPv4 address, IPv6 address, or hostname of the TACACS+ server. To specify multiple hosts, multiple `tacacs-server host` commands can be used.

Format `tacacs-server host {`*`ip-address`*`| `*`ipv6-address`*` | `*`hostname}`

Mode Global Config

3.12.0.1.1 no tacacs-server host

Use the `no tacacs-server host` command to delete the specified hostname or IP address. The *`ip-address`*, *`ipv6-address`*, or *`hostname`* parameter is the IPv4 address, IPv6 address, or hostname of the TACACS+ server.

Format `no tacacs-server host {`*`ip-address`*`| `*`ipv6-address`*` | `*`hostname`*`}`

Mode Global Config

3.12.0.2 tacacs-server host link-local

Use this command to configure the link-local-address of the TACACS+ server and the outgoing interface to be used by the TACACS+ client to communicate with the TACACS+ server. The outgoing interface can be any physical interface, the service port, or the network port.

Format `tacacs-server host link-local `*`link-local-address`*` interface {`*`slot/port`*` | network | serviceport}`

Mode Global Config

3.12.0.2.1 no tacacs-server host link-local

Use this command to remove the configured TACACS+ server link-local address.

Format `no tacacs-server host link-local`

Mode Global Config

3.12.0.3 tacacs-server key

Use the `tacacs-server key` command to set the authentication and encryption key for all TACACS+ communications between the switch and the TACACS+ daemon. The `key-string` parameter has a range of 0 - 128 characters and specifies the authentication and encryption key for all TACACS communications between the switch and the TACACS+ server. This key must match the key used on the TACACS+ daemon.

Text-based configuration supports TACACS server's secrets in encrypted and non-encrypted format. When you save the configuration, these secret keys are stored in encrypted format only. If you want to enter the key in encrypted format, enter the key along with the encrypted keyword. In the show running config command's display, these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

Format `tacacs-server key [`*`key-string`* `| encrypted` *`key-string`*`]`

Mode Global Config

3.12.0.3.1 no tacacs-server key

Use the `no tacacs-server key` command to disable the authentication and encryption key for all TACACS+ communications between the switch and the TACACS+ daemon. The `key-string` parameter has a range of 0 - 128 characters This key must match the key used on the TACACS+ daemon.

Format `no tacacs-server key` *`key-string`*

Mode Global Config

3.12.0.4 tacacs-server keystring

Use the `tacacs-server keystring` command to set the global authentication encryption key used for all TACACS+ communications between the TACACS+ server and the client.

Format `tacacs-server keystring`

Mode Global Config

Example: The following shows an example of the CLI command.

(Routing) (Config)#tacacs-server keystring

Enter tacacs key:********

Re-enter tacacs key:********

3.12.0.5 tacacs-server timeout

Use the `tacacs-server timeout` command to set the timeout value for communication with the TACACS+ servers. The `timeout` parameter has a range of 1-30 and is the timeout value in seconds. If you do not specify a timeout value, the command sets the global timeout to the default value. TACACS+ servers that do not use the global timeout will retain their configured timeout values.

Default 5

Format `tacacs-server timeout` *`timeout`*

Mode Global Config

3.12.0.5.1 no tacacs-server timeout

Use the `no tacacs-server timeout` command to restore the default timeout value for all TACACS servers.

Format `no tacacs-server timeout`
Mode Global Config

3.12.0.6 key

Use the `key` command in TACACS Configuration mode to specify the authentication and encryption key for all TACACS communications between the device and the TACACS server. This key must match the key used on the TACACS daemon. The `key-string` parameter specifies the key name. For an empty string use " ". (Range: 0 - 128 characters).

Text-based configuration supports TACACS server's secrets in encrypted and non-encrypted format. When you save the configuration, these secret keys are stored in encrypted format only. If you want to enter the key in encrypted format, enter the key along with the encrypted keyword. In the show running config command's display, these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

Format `key [`*`key-string`* `| encrypted` *`key-string`*`]`
Mode TACACS Config

3.12.0.7 keystring

Use the `keystring` command in TACACS Server Configuration mode to set the TACACS+ server-specific authentication encryption key used for all TACACS+ communications between the TACACS+ server and the client.

Format `keystring`
Mode TACACS Server Config

Example: The following shows an example of the command.

```
(Routing) (Config)#tacacs-server host 1.1.1.1
(Routing) (Tacacs)#keystring

Enter tacacs key:********
Re-enter tacacs key:********
```

3.12.0.8 port (TACACS Config Mode)

Use the `port` command in TACACS Configuration mode to specify a server port number. The server `port-number` range is 0 - 65535.

Default 49
Format `port` *`port-number`*
Mode TACACS Config

3.12.0.9 priority

Use the `priority` command in TACACS Configuration mode to specify the order in which servers are used, where 0 (zero) is the highest priority. The `priority` parameter specifies the priority for servers. The highest priority is 0 (zero), and the range is 0 - 65535.

Default 0

Format `priority` ***priority***

Mode TACACS Config

3.12.0.10 tacacs-server source-interface

Use this command in Global Configuration mode to configure the source interface (Source IP address) for TACACS+ server configuration. The selected source-interface IP address is used for filling the IP header of management protocol packets. This allows security devices (firewalls) to identify the source packets coming from the specific switch.

If a source-interface is not specified, the primary IP address of the originating (outbound) interface is used as the source address.

Format `tacacs-server source-interface {`***slot/port*** `|` `loopback` ***loopback-id***`|vlan` ***vlan-id***`}`

Mode Global Config

Parameter	Description
slot/port	Specifies the port to use as the source interface.
loopback-id	Specifies the loopback interface to use as the source interface. The range of the loopback ID is 0 to 7.
vlan-id	Specifies the VLAN to use as the source interface.

Example: The following shows an example of the command.

```
(Config)#tacacs-server source-interface loopback 0
(Config)#tacacs-server source-interface 0/1
(Config)#no tacacs-server source-interface
```

3.12.0.10.1 no tacacs-server source-interface

Use this command in Global Configuration mode to remove the global source interface (Source IP selection) for all TACACS+ communications between the TACACS+ client and the server.

Format `no tacacs-server source-interface`

Mode Global Config

3.12.0.11 timeout

Use the `timeout` command in TACACS Configuration mode to specify the timeout value in seconds. If no timeout value is specified, the global value is used. The `timeout` parameter has a range of 1-30 and is the timeout value in seconds.

Format `timeout` ***timeout***

Mode TACACS Config

3.12.0.12 show tacacs

Use the `show tacacs` command to display the configuration and statistics of a TACACS+ server.

Format `show tacacs` *`[ip-address | ipv6-address | hostname]`*
Mode Privileged EXEC

Parameter	Definition
Host address	The IP address or hostname of the configured TACACS+ server.
Port	The configured TACACS+ server port number.
TimeOut	The timeout in seconds for establishing a TCP connection.
Priority	The preference order in which TACACS+ servers are contacted. If a server connection fails, the next highest priority server is contacted.

3.12.0.13 show tacacs source-interface

Use the `show tacacs source-interface` command in Global Config mode to display the configured global source interface details used for a TACACS+ client. The IP address of the selected interface is used as source IP for all communications with the server.

Format `show tacacs source-interface`
Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) #show tacacs source-interface

TACACS Client Source Interface.................. 0/2
TACACS Client Source IPv4 Address.............. 192.168.2.20          [Up]
```

3.13 Configuration Scripting Commands

Configuration Scripting allows you to generate text-formatted script files representing the current configuration of a system. You can upload these configuration script files to a PC or UNIX system and edit them. Then, you can download the edited files to the system and apply the new configuration. You can apply configuration scripts to one or more switches with no or minor modifications.

Use the `show running-config` command (see Section 4.5.0.24, show running-config) to capture the running configuration into a script. Use the `copy` command (see Section 4.8.0.17, copy) to transfer the configuration script to or from the switch.

Use the show *{startup-config | backup-config | factory-defaults}* command to view the configuration stored in the startup-config, backup-config, or factory-defaults file (see Section 4.5.0.26, show).

You should use scripts on systems with default configuration; however, you are not prevented from applying scripts on systems with non-default configurations.

Scripts must conform to the following rules:

- The file extension must be ".scr".
- A maximum of ten scripts are allowed on the switch.
- The combined size of all script files on the switch shall not exceed 2048 KB.
- The maximum number of configuration file command lines is 2000.

You can type single-line annotations at the command prompt to use when you write test or configuration scripts to improve script readability. The exclamation point (!) character flags the beginning of a comment. The comment flag character can begin a word anywhere on the command line, and all input following this character is ignored. Any command line that begins with the "!" character is recognized as a comment line and ignored by the parser.

The following lines show an example of a script:

```
! Script file for displaying management access

show telnet !Displays the information about remote connections

! Display information about direct connections

show serial

! End of the script file!
```

NOTE: To specify a blank password for a user in the configuration script, you must specify it as a space within quotes. For example, to change the password for user jane from a blank password to hello, the script entry is as follows:

```
users passwd jane
" "
hello
hello
```

3.13.0.1 script apply

This command applies the commands in the script to the switch. The `scriptname` parameter is the name of the script to apply.

Format	`script apply` *`scriptname`*
Mode	Privileged EXEC

3.13.0.2 script delete

This command deletes a specified script where the `scriptname` parameter is the name of the script to delete. The `all` option deletes all the scripts present on the switch.

Format `script delete {`*`scriptname`* `| all}`
Mode Privileged EXEC

3.13.0.3 script list

This command lists all scripts present on the switch as well as the remaining available space.

Format `script list`
Mode Privileged EXEC

Parameter	Definition
Configuration Script	Name of the script.
Size	Privileged EXEC

3.13.0.4 script show

This command displays the contents of a script file, which is named `scriptname`.

Format `script show` *`scriptname`*
Mode Privileged EXEC

Parameter	Definition
Output Format	`line number: line contents`

3.13.0.5 script validate

This command validates a script file by parsing each line in the script file where `scriptname` is the name of the script to validate.The validate option is intended to be used as a tool for script development. Validation identifies potential problems. It might not identify all problems with a given script on any given device.

Format `script validate` *`scriptname`*
Mode Privileged EXEC

3.14 Pre-login Banner, System Prompt, and Host Name Commands

This section describes the commands you use to configure the pre-login banner and the system prompt. The pre-login banner is the text that displays before you login at the `User:` prompt.

3.14.0.1 copy (pre-login banner)

The `copy` command includes the option to upload or download the CLI Banner to or from the switch. You can specify local URLs by using FTP, TFTP, SFTP, SCP, or Xmodem.

Default none

Format `copy <tftp://<ipaddr>/<filepath>/<filename>> nvram:clibanner`

`copy nvram:clibanner <tftp://<ipaddr>/<filepath>/<filename>>`

Mode Privileged EXEC

3.14.0.2 set prompt

This command changes the name of the prompt. The length of name may be up to 64 alphanumeric characters.

Format `set prompt` *`prompt_string`*

Mode Privileged EXEC

3.14.0.3 set clibanner

Use this command to configure the pre-login CLI banner before displaying the login prompt.

Format `set clibanner` *`line`*

Mode Global Config

Parameter	Description
line	Banner text where “” (double quote) is a delimiting character. The banner message can be up to 2000 characters.

3.14.0.3.1 no set clibanner

Use this command to unconfigure the pre-login CLI banner.

Format `no set clibanner`

Mode Global Config

3.14.0.4 show clibanner

Use this command to display the configured pre-login CLI banner. The pre-login banner is the text that displays before displaying the CLI prompt.

Default No contents to display before displaying the login prompt.

Format `show clibanner`

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) #show clibanner

Banner Message configured :
==========================


--------------------------
         TEST
--------------------------
```

3.14.0.5 hostname

This command sets the system hostname. It also changes the prompt. The length of name may be up to 64 alphanumeric, case-sensitive characters.

Format `hostname` *`hostname`*

Mode Privileged EXEC

3.15 Front Panel TAP Interfaces

Use the commands in this section to enable and monitor FPTI mode.

3.15.0.1 fpti

Use this command to enable FPTI mode either globally (in Global Config mode) or for a specific interface (in Interface Config mode).

Default Enabled

Format `fpti`

Mode
- Global Config
- Interface Config

3.15.0.1.1 no fpti

Use this command to disable FPTI mode.

Format `no fpti`

Mode
- Global Config
- Interface Config

3.15.0.2 show port fpti

Use this command to display the FPTI mode on all interfaces and the global FPTI mode. If an interface is specified, only the FPTI mode for the specified interface is displayed.

Format `show port fpti [slot/port]`

Mode
- Global Config
- Interface Config

Example:

```
(Switching) show port fpti

Global Front Panel Tap Interface Mode.......... Enabled

 Intf     Mode
--------- ---------------
0/1       Enabled
0/2       Enabled
0/3       Enabled
0/4       Enabled
0/5       Enabled
0/6       Enabled
0/7       Enabled
0/8       Enabled
0/9       Enabled
0/10      Enabled
0/11      Enabled
0/12      Enabled
0/13      Enabled
```

```
0/14      Enabled
0/15      Enabled
0/16      Enabled
0/17      Enabled
0/18      Enabled
0/19      Enabled
0/20      Enabled
0/21      Enabled
0/22      Enabled
0/23      Enabled
0/24      Enabled
```

Example:

```
(Switching) show port fpti 0/1

Port.....................................  0/1
Front Panel Tap Interface Mode..... Enabled
```

Chapter 4: Utility Commands

This section describes the utility commands available in the EFOS CLI.

NOTE: The commands in this section are in one of five functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Copy commands transfer or save configuration and informational files to and from the switch.
- Debug commands provide diagnostic information and help troubleshoot network issues.
- Clear commands clear some or all of the settings to factory defaults.

4.1 AutoInstall Commands

The AutoInstall feature enables the automatic update of the image and configuration of the switch. This feature enables touchless or low-touch provisioning to simplify switch configuration and imaging.

AutoInstall includes the following support:

- Downloading an image from TFTP server using DHCP option 125. The image update can result in a downgrade or upgrade of the firmware on the switch.
- Automatically downloading a configuration file from a TFTP server when the switch is booted with no saved configuration file.
- Automatically downloading an image from a TFTP server in the following situations:
  - When the switch is booted with no saved configuration found.
  - When the switch is booted with a saved configuration that has AutoInstall enabled.

When the switch boots and no configuration file is found, it attempts to obtain an IP address from a network DHCP server. The response from the DHCP server includes the IP address of the TFTP server where the image and configuration flies are located.

After acquiring an IP address and the additional relevant information from the DHCP server, the switch downloads the image file or configuration file from the TFTP server. A downloaded image is automatically installed. A downloaded configuration file is saved to non-volatile memory.

NOTE: AutoInstall from a TFTP server can run on any IP interface, including the network port, service port, and in-band routing interfaces (if supported). To support AutoInstall, the DHCP client is enabled operationally on the service port, if it exists, or the network port, if there is no service port.

4.1.0.1 boot autoinstall

Use this command to operationally start or stop the AutoInstall process on the switch. The command is non-persistent and is not saved in the startup or running configuration file.

Default	stopped
Format	`boot autoinstall {start | stop}`
Mode	Privileged EXEC

4.1.0.2 boot host retrycount

Use this command to set the number of attempts to download a configuration file from the TFTP server.

Default 3
Format `boot host retrycount` *`1-3`*
Mode Privileged EXEC

4.1.0.2.1 no boot host retrycount

Use this command to set the number of attempts to download a configuration file to the default value.

Format `no boot host retrycount`
Mode Privileged EXEC

4.1.0.3 boot host dhcp

Use this command to enable AutoInstall on the switch for the next reboot cycle. The command does not change the current behavior of AutoInstall and saves the command to NVRAM.

Default enabled
Format `boot host dhcp`
Mode Privileged EXEC

4.1.0.3.1 no boot host dhcp

Use this command to disable AutoInstall for the next reboot cycle.

Format `no boot host dhcp`
Mode Privileged EXEC

4.1.0.4 boot host autosave

Use this command to automatically save the downloaded configuration file to the startup-config file on the switch. When autosave is disabled, you must explicitly save the downloaded configuration to non-volatile memory by using the `write memory` or `copy system:running-config nvram:startup-config` command. If the switch reboots and the downloaded configuration has not been saved, the AutoInstall process begins, if the feature is enabled.

Default disabled
Format `boot host autosave`
Mode Privileged EXEC

4.1.0.4.1 no boot host autosave

Use this command to disable automatically saving the downloaded configuration on the switch.

Format `no boot host autosave`
Mode Privileged EXEC

4.1.0.5 boot host autoreboot

Use this command to allow the switch to automatically reboot after successfully downloading an image. When auto reboot is enabled, no administrative action is required to activate the image and reload the switch.

Default enabled
Format `boot host autoreboot`
Mode Privileged EXEC

4.1.0.5.1 no boot host autoreboot

Use this command to prevent the switch from automatically rebooting after the image is downloaded by using the AutoInstall feature.

Format `no boot host autoreboot`
Mode Privileged EXEC

4.1.0.6 erase startup-config

Use this command to erase the configuration file `startup-config`, the text-based configuration file stored in non-volatile memory. If the switch boots and no startup-config file is found, the AutoInstall process automatically begins.

Format `erase startup-config`
Mode Privileged EXEC

4.1.0.7 erase factory-defaults

Use this command to erase the text-based factory-defaults file stored in non-volatile memory.

Default Disable
Format `erase factory-defaults`
Mode Privileged EXEC

4.1.0.8 erase application

Use this command to remove the specified file from the switch file system application directory.

Default Disable
Format `erase application` *`filename`*
Mode Privileged EXEC

4.1.0.9 show autoinstall

This command displays the current status of the AutoInstall process.

Format `show autoinstall`
Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) #show autoinstall

AutoInstall Mode.............................. Stopped
AutoInstall Persistent Mode................... Disabled
AutoSave Mode................................. Disabled
AutoReboot Mode............................... Enabled
AutoInstall Retry Count....................... 3
```

4.2 Application Commands

4.2.0.1 application install

This command makes the application started by the designated executable file available for configuration and execution. The parameters of this command determine how the application is run on the switch.

This command can be issued using an already installed application file name to update the parameters. This updates the configuration for the next time the application is started.

This command can be issued for a file that is not currently on the switch. This allows preconfiguration of the execution parameters. The configuration does not take effect until the executable file is present in the switch file system.

Format `application install` ***filename*** `[start-on-boot] [auto-restart] [cpu-sharing` ***0-99***`] [max-megabytes` ***megabytes***`]`

Mode Global Config

Parameter	Description	Default
filename	The name of the file containing the executable or script that is started as a Linux process for the application.	N/A
start-on-boot	Starts the application each time the switch boots up. Takes effect on the first reboot after setting. Omit this keyword from the command to disable starting the application at boot time.	N/A
auto-restart	Automatically restarts the application's process(es) if they stop running. Omit this keyword from the command to disable the automatic restart of the application.	N/A
cpu-sharing	Sets the CPU share allocated to this application, expressed as a percentage between 0 and 99. If 0 is specified, the application process(es) are not limited. If this keyword is not specified, the default value is used.	0
max-megabytes	Sets the maximum memory resource that the application process(es) can consume. Expressed as megabytes between 0 and 200. If 0 is specified, the application process(es) are not limited. If this keyword is not specified, the default value is used.	0

4.2.0.1.1 no application install

This command removes the configuration of an application for execution on the switch. If the application is running, all processes associated with the application are stopped automatically.

Format `no application install` ***filename***

Mode Global Config

4.2.0.2 application start

This command starts the execution of the specified application. The application must be installed before it can be started using this command.

Format `application start` *`filename`*
Mode Privileged EXEC

4.2.0.3 application stop

This command stops the execution of the specified application.

Format `application stop` *`filename`*
Mode Privileged EXEC

4.2.0.4 show application

This command displays the applications installed and their parameters.

Format `show applications`
Mode Privileged EXEC

Parameter	Definition
filename	The name of the application.
start-on-boot	If the application is configured to start on boot up. ■ Yes: The application will start on boot up. ■ No: The application will not start on boot up.
auto-restart	If the application is configured to restart when the application process ends. ■ Yes: The application will restart when the application process ends. ■ No: The application will not restart when the application process ends.
Max-CPU-Util	The configured application CPU utilization limit expressed as a percentage. “None” if unlimited.
Max-memory	The configured application memory limit in megabytes. “None” if unlimited.

4.2.0.5 show application files

This command displays the files in the application directory of the switch’s file system.

Format `show application files`
Mode Privileged EXEC

Parameter	Definition
filename	Name of the file.
File size	Number of bytes the file occupies in the file system.
Directory Size	Number of bytes all the files in the application directory.

4.3 CLI Output Filtering Commands

4.3.0.1 show *xxx*|include "*string*"

The command ***xxx*** is executed and the output is filtered to only show lines containing the "***string***" match. All other non-matching lines in the output are suppressed.

Example: The following shows an example of the CLI command.

```
(Routing) #show running-config | include "spanning-tree"

spanning-tree configuration name "00-02-BC-42-F9-33"
spanning-tree bpduguard
spanning-tree bpdufilter default
```

4.3.0.2 show *xxx*|include "*string*" exclude "*string2*"

The command ***xxx*** is executed and the output is filtered to only show lines containing the "***string***" match and not containing the "***string2***" match. All other non-matching lines in the output are suppressed. If a line of output contains both the include and exclude strings then the line is not displayed.

Example: The following shows example of the CLI command.

```
(Routing) #show running-config | include "spanning-tree" exclude "configuration"

spanning-tree bpduguard
spanning-tree bpdufilter default
```

4.3.0.3 show *xxx*|exclude "*string*"

The command ***xxx*** is executed and the output is filtered to show all lines not containing the "***string***" match. Output lines containing the "***string***" match are suppressed.

Example: The following shows an example of the CLI command.

```
(Routing) #show interface 0/1

Packets Received Without Error..................... 0
Packets Received With Error........................ 0
Broadcast Packets Received......................... 0
Packets Transmitted Without Errors................. 0
Transmit Packet Errors............................. 0
Collision Frames................................... 0
Time Since Counters Last Cleared................... 20 day 21 hr 30 min 9 sec

(Routing) #show interface 0/1 | exclude "Packets"

Transmit Packet Errors............................. 0
Collision Frames................................... 0
Time Since Counters Last Cleared................... 20 day 21 hr 30 min 9 sec
```

4.3.0.4 show *xxx*|begin "*string*"

The command ***xxx*** is executed and the output is filtered to show all lines beginning with and following the first line containing the "***string***" match. All prior lines are suppressed.

Example: The following shows an example of the CLI command.

```
(Routing) #show port all | begin "1/1"
```

```
1/1           Enable                         Down   Disable N/A    N/A
1/2           Enable                         Down   Disable N/A    N/A
1/3           Enable                         Down   Disable N/A    N/A
1/4           Enable                         Down   Disable N/A    N/A
1/5           Enable                         Down   Disable N/A    N/A
1/6           Enable                         Down   Disable N/A    N/A

(Routing) #
```

4.3.0.5 show *xxx*|section “*string*”

The command ***xxx*** is executed and the output is filtered to show only lines included within the section(s) identified by lines containing the “***string***” match and ending with the first line containing the default end-of-section identifier (i.e. “exit”).

Example: The following shows an example of the CLI command.

```
(Routing) #show running-config | section “interface 0/1”

interface 0/1
no spanning-tree port mode
exit
```

4.3.0.6 show *xxx*|section “*string*” “*string2*”

The command ***xxx*** is executed and the output is filtered to only show lines included within the section(s) identified by lines containing the “***string***” match and ending with the first line containing the “***string2***” match. If multiple sessions matching the specified string match criteria are part of the base output, then all instances are displayed.

4.3.0.7 show *xxx*|section “*string*” include “*string2*”

The command ***xxx*** is executed and the output is filtered to only show lines included within the section(s) identified by lines containing the “***string***” match and ending with the first line containing the default end-of-section identifier (i.e. “exit”) and that include the “string2” match. This type of filter command could also include “exclude” or user-defined end-of-section identifier parameters as well.

4.4 Dual Image Commands

NOTE: These commands are only available on selected Linux-based platforms.

EFOS software supports a dual image feature that allows the switch to have two software images in the permanent storage. You can specify which image is the active image to be loaded in subsequent reboots. This feature allows reduced down-time when you upgrade or downgrade the software.

4.4.0.1 delete

This command deletes the backup image file from the permanent storage or the core dump file from the local file system.

Format `delete backup`
`delete core-dump-file` *`file-name`* `| all`

Mode Privileged EXEC

4.4.0.2 boot system

This command activates the specified image. It will be the active-image for subsequent reboots and will be loaded by the boot loader. The current active-image is marked as the backup-image for subsequent reboots. If the specified image doesn't exist on the system, this command returns an error message.

Format `boot system {active | backup}`

Mode Privileged EXEC

4.4.0.3 show bootvar

This command displays the version information and the activation status for the current active and backup images. The command also displays any text description associated with an image. This command displays the switch activation status.

Format `show bootvar`

Mode Privileged EXEC

4.4.0.4 filedescr

This command associates a given text description with an image. Any existing description will be replaced.

Format `filedescr {active | backup}` *`text-description`*

Mode Privileged EXEC

4.4.0.5 update bootcode

This command updates the bootcode (boot loader) on the switch. The bootcode is read from the active-image for subsequent reboots.

The update bootcode is:

- Designed to update the U-Boot image in flash. The U-Boot image is responsible for initializing the lower-level hardware, like the BIOS on an x86 system.
- Not supported on x86 platforms and not available on all embedded platforms. Only some vendors include the ability to update the U-Boot firmware from inside EFOS.

Format `update bootcode`
Mode Privileged EXEC

4.5 System Information and Statistics Commands

This section describes the commands you use to view information about system features, components, and configurations.

4.5.0.1 load-interval

This command changes the length of time for which data is used to compute load statistics. The value is given in seconds, and must be a multiple of 30. The allowable range for `interval` is from 30 to 600 seconds. The smaller the value of the load interval is, the more accurate is the instantaneous rate given by load statistics. Smaller values may affect system performance.

Default 300 seconds
Format `load-interval` *`interval`*
Mode Interface Config

Example:

```
(Routing) (Interface 0/1)#load-interval 30
```

4.5.0.1.1 no load-interval

This command resets the load interval on the interface to the default value.

Format `load-interval` *`interval`*
Mode Interface Config

4.5.0.2 show arp switch

This command displays the contents of the IP stack's Address Resolution Protocol (ARP) table. The IP stack only learns ARP entries associated with the management interfaces - network or service ports. ARP entries associated with routing interfaces are not listed.

Format `show arp switch`
Mode Privileged EXEC

Parameter	Definition
IP Address	IP address of the management interface or another device on the management network.
MAC Address	Hardware MAC address of that device.
Interface	For a service port the output is `Management`. For a network port, the output is the `slot/port` of the physical interface.

4.5.0.3 dir

Use this command to list the files in the directory /mnt/fastpath in flash from the CLI.

Format `dir`
Mode Privileged EXEC

```
(Routing) #dir

    0  drwx                2048 May 09 2002 16:47:30 .
    0  drwx                2048 May 09 2002 16:45:28 ..
    0  -rwx                 592 May 09 2002 14:50:24 slog2.txt
    0  -rwx                  72 May 09 2002 16:45:28 boot.dim
    0  -rwx                   0 May 09 2002 14:46:36 olog2.txt
    0  -rwx            13376020 May 09 2002 14:49:10 image1
    0  -rwx                   0 Apr 06 2001 19:58:28 fsyssize
    0  -rwx                1776 May 09 2002 16:44:38 slog1.txt
    0  -rwx                 356 Jun 17 2001 10:43:18 crashdump.ctl
    0  -rwx                1024 May 09 2002 16:45:44 sslt.rnd
    0  -rwx            14328276 May 09 2002 16:01:06 image2
    0  -rwx                 148 May 09 2002 16:46:06 hpc_broad.cfg
    0  -rwx                   0 May 09 2002 14:51:28 olog1.txt
    0  -rwx                 517 Jul 23 2001 17:24:00 ssh_host_key
    0  -rwx               69040 Jun 17 2001 10:43:04 log_error_crashdump
    0  -rwx                 891 Apr 08 2000 11:14:28 sslt_key1.pem
    0  -rwx                 887 Jul 23 2001 17:24:00 ssh_host_rsa_key
    0  -rwx                 668 Jul 23 2001 17:24:34 ssh_host_dsa_key
    0  -rwx                 156 Apr 26 2001 13:57:46 dh512.pem
    0  -rwx                 245 Apr 26 2001 13:57:46 dh1024.pem
    0  -rwx                   0 May 09 2002 16:45:30 slog0.txt
```

4.5.0.4 show eventlog

This command displays the event log, which contains error messages from the system. The event log is not cleared on a system reset.

Format `show eventlog`
Mode Privileged EXEC

Parameter	Definition
File	The file in which the event originated.
Line	The line number of the event.
Task Id	The task ID of the event.
Code	The event code.
Time	The time this event occurred.

NOTE: Event log information is retained across a switch reset.

4.5.0.5 show hardware

This command displays inventory information for the switch.

NOTE: The `show version` command and the `show hardware` command display the same information. In future releases of the software, the `show hardware` command will not be available. For a description of the command output, see the command Section 4.5.0.10, show version.

Format `show hardware`
Mode Privileged EXEC

4.5.0.6 show slot

This command displays information about all the slots in the system or for a specific slot.

Format `show slot` *`[unit/slot]`*
Mode User EXEC

Term	Definition
Slot	The slot identifier in a *`unit/slot`* format.
Slot Status	The slot is empty, full, or has encountered an error
Admin State	The slot administrative mode is enabled or disabled.
Power State	The slot power mode is enabled or disabled.
Configured Card Model Identifier	The model identifier of the card preconfigured in the slot. Model Identifier is a 32-character field used to identify a card.
Pluggable	Cards are pluggable or non-pluggable in the slot.
Power Down	Indicates whether the slot can be powered down.

If you supply a value for *`unit/slot`*, the following additional information appears:

Term	Definition
Inserted Card Model Identifier	The model identifier of the card inserted in the slot. Model Identifier is a 32-character field used to identify a card. This field is displayed only if the slot is full.
Inserted Card Description	The card description. This field is displayed only if the slot is full.
Configured Card Description	10BASE-T half duplex

4.5.0.7 environment temprange

Use this command to set the allowed temperature range for normal operation.

Format `environment temprange min` *`-100-100`* `max` *`-100-100`*
Mode Global Config

Parameter	Definition
min	Sets the minimum allowed temperature for normal operation. The range is between –100°C and 100°C. The default is 0°C.
max	Sets the maximum allowed temperature for normal operation. The range is between –100°C and 100°C. The default is 0°C.

4.5.0.8 environment trap

Use this command to configure environment status traps.

Format `environment trap {fan|powersupply|temperature}`
Mode Global Config

Parameter	Definition
fan	Enables or disables the sending of traps for fan status events. The default is enable.
powersupply	Enables or disables the sending of traps for power supply status events. The default is enable.
temperature	Enables or disables the sending of traps for temperature status events. The default is enable.

4.5.0.9 show environment

This command displays information about system disk space and usage.

Format `show environment`
Mode Privileged EXEC

Parameter	Definition
Unit	The system unit number.
Total Space	The total amount of disk space on the system, in KB.
Free Space	The amount of available disk space on the system, in KB.
Used Space	The amount of disk space in use on the system, in KB.
Utilization	The amount of disk space in use on the system, as a percentage of total disk space.

Example:

```
Unit   Total space (KB)   Free space (KB)   Used space (KB)   Utilization (%)
----   ----------------   ---------------   ---------------   ---------------
1              126,976            85,976            41,000               32
```

4.5.0.10 show version

This command displays inventory information for the switch.

NOTE: The `show version` command will replace the `show hardware` command in future releases of the software.

Format `show version`
Mode Privileged EXEC

Parameter	Definition
System Description	Text used to identify the product name of this switch.
Machine Type	The machine model as defined by the Vital Product Data.
Machine Model	The machine model as defined by the Vital Product Data
Serial Number	The unique box serial number for this switch.

Parameter	Definition
FRU Number	The field replaceable unit number.
Part Number	Manufacturing part number.
Maintenance Level	Hardware changes that are significant to software.
Manufacturer	Manufacturer descriptor field.
Burned in MAC Address	Universally assigned network address.
Software Version	The release.version.revision number of the code currently running on the switch.
Operating System	The operating system currently running on the switch.
Network Processing Device	The type of the processor microcode.
Additional Packages	The additional packages incorporated into this system.

4.5.0.11 show version bootloader

Use this command to display Uboot version information.

Format `show version bootloader`

Mode Privileged EXEC

Example: The following example shows the output of the command:

```
(Switching) #show version bootloader
Querying Active and Backup Software, please wait ....
Running Version.............................. B1.0.0.5
Active Version............................... B1.0.0.5
Backup Version............................... B1.0.0.2
```

4.5.0.12 show platform vpd

This command displays vital product data for the switch.

Format `show platform vpd`

Mode User Privileged

The following information is displayed.

Term	Definition
Operational Code Image File Name	Build Signature loaded into the switch
Software Version	Release Version Maintenance Level and Build (RVMB) information of the switch.
Timestamp	Timestamp at which the image is built

Example: The following shows example CLI display output for the command.

```
(Routing) #show platform vpd

Operational Code Image File Name.............. FastPath-EFOS-esw-xgs4-gto-BL20R-CS-6IQHr3v7m14b35
Software Version.............................. 3.7.14.35
Timestamp..................................... Thu Mar  7 14:36:14 IST 2013
```

4.5.0.13 show interface

This command displays a summary of statistics for a specific interface or a count of all CPU traffic based upon the argument.

Format `show interface {slot/port | switchport | lag lag-id}`

Mode Privileged EXEC

The display parameters, when the argument is *slot/port*, are as follows:

Parameters	Definition
Packets Received Without Error	The total number of packets (including broadcast packets) received by the processor.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address.
Receive Packets Discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Packets Transmitted Without Error	The total number of packets transmitted out of the interface.
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Transmit Packets Errors	The number of outbound packets that could not be transmitted because of errors.
Collisions Frames	The best estimate of the total number of collisions on this Ethernet segment.
Load Interval	The length of time for which data is used to compute load statistics. The value is given in seconds, and must be a multiple of 30. The allowable range is from 30 to 600 seconds
Bits Per Second Received	Approximate number of bits per second received. This value is an exponentially weighted average and is affected by the configured load-interval.
Bits Per Second Transmitted.	Approximate number of bits per second transmitted. This value is an exponentially weighted average and is affected by the configured load-interval.
Packets Per Second Received	Approximate number of packets per second received. This value is an exponentially weighted average and is affected by the configured load-interval.
Packets Per Second Transmitted	Approximate number of packets per second transmitted. This value is an exponentially weighted average and is affected by the configured load-interval.
Percent Utilization Received	Value of link utilization in percentage representation for the RX line.
Percent Utilization Transmitted	Value of link utilization in percentage representation for the TX line.
Link Flaps	The number of link flaps (link up and down cycle) that have occurred.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

The display parameters, when the argument is “switchport” are as follows:

Parameter	Definition
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Packets Transmitted Without Error	The total number of packets transmitted out of the interface.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested to be transmitted to the Broadcast address, including those that were discarded or not sent.

Parameter	Definition
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Address Entries Currently In Use	The total number of Forwarding Database Address Table entries now active on the switch, including learned and static entries.
VLAN Entries Currently In Use	The number of VLAN entries presently occupying the VLAN table.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.

4.5.0.14 show interfaces status

Use this command to display interface information, including the description, port state, speed and auto-neg capabilities. The command is similar to `show port all` but displays additional fields like interface description and port-capability.

The description of the interface is configurable through the existing command `description <name>` which has a maximum length of 64 characters that is truncated to 28 characters in the output. The long form of the description can be displayed using `show port description`. The interfaces displayed by this command are physical interfaces, LAG interfaces and VLAN routing interfaces.

Format `show interfaces status [{`*`slot/port`* `| vlan` *`id`*`}]`
Mode Privileged EXEC

Field	Description
Port	The interface associated with the rest of the data in the row.
Name	The descriptive user-configured name for the interface.
Link State	Indicates whether the link is up or down.
Physical Mode	The speed and duplex settings on the interface.
Physical Status	Indicates the port speed and duplex mode for physical interfaces. The physical status for LAGs is not reported. When a port is down, the physical status is unknown.
Media Type	The media type of the interface.
Flow Control Status	The 802.3x flow control status.
Flow Control	The configured 802.3x flow control mode.

4.5.0.15 show interfaces traffic

Use this command to display interface traffic information.

Format `show interfaces traffic [`*`slot/port`*`]`
Mode Privileged EXEC

Field	Description
Interface Name	The interface associated with the rest of the data in the row.
Congestion Drops	The number of packets that have been dropped on the interface due to congestion.
TX Queue	The number of bytes in the transmit queue.
RX Queue	The number of bytes in the receive queue.
Color Drops: Green	The number of green packets that were dropped.

Field	Description
Color Drops: Yellow	The number of yellow (conformed) packets that were dropped.
Color Drops: Red	The number of red (exceeded) packets that were dropped.
WRED TX Queue	The number of packets in the WRED transmit queue.
ECN Tx Queue	The number of packets in the ECN transmit queue.

Example: The following shows example CLI display output for the command.

```
(Routing) #show interfaces traffic
Intf    Congestion  Tx Queue Rx Queue Color Drops (Pkts)                WRED Tx       ECN Tx
Name    Drops(Pkts) (KB)       (KB) Green       Yellow     Red        Queue(KB) (Pkts)
------- ----------- -------- -------- ----------- ---------- ---------- ------------- --------
0/1               0        0       NA           0          0          0             0        0
0/2               0        0       NA           0          0          0             0        0
0/3               0        0       NA           0          0          0             0        0
0/4               0        0       NA           0          0          0             0        0
0/5               0        0       NA           0          0          0             0        0
0/6               0        0       NA           0          0          0             0        0
0/7               0        0       NA           0          0          0             0        0
0/8               0        0       NA           0          0          0             0        0
0/9               0        0       NA           0          0          0             0        0
0/10              0        0       NA           0          0          0             0        0
0/11              0        0       NA           0          0          0             0        0
```

The `show interfaces traffic <u/s/p>` command displays per cos queue statistics.

```
(Routing) #show interfaces traffic 0/1

Interface Name.................................. 0/1
Congestion Drops(Pkts).......................... 0
Tx Queue(KB)................................ 0
Rx Queue(KB)................................ NA
Color Drops Green(Pkts)......................... 0
Color Drops Yellow(Pkts)........................ 0
Color Drops Red(Pkts)........................... 0
WRED Tx Queue(KB)............................ 0
ECN Tx(Pkts).................................... 0

CoS Queue statistics
CoS   Total Drops  Total      Peak       Current    Average
      (Pkts)       (KB)   (KB)   (KB)   (KB)
----- ------------ ---------- ---------- ---------- ----------
0               0          0          0          0          0
1               0          0          0          0          0
2               0          0          0          0          0
3               0          0          0          0          0
4               0          0          0          0          0
5               0          0          0          0          0
6               0          0          0          0          0
7               0          8          0          0          0
8              NA         NA         NA         NA    1344550
```

NOTE:

- If `counter` is not supported in hardware, the `show` command displays the counter value as NA.

- The `clear counters` command clears all the new counters except `peak count` as this is a status value not a counter.

4.5.0.16 show interface counters

This command reports key summary statistics for all the ports (physical/CPU/port-channel).

Format `show interface counters`
Mode Privileged EXEC

Parameter	Definition
Port	The physical port, LAG, or CPU interface associated with the rest of the data in the row.
InOctets	The number of inbound octets received by the interface.
InUcastPkts	The number of inbound unicast packets received by the interface.
InMcastPkts	The number of inbound multicast packets received by the interface.
InBcastPkts	The number of inbound broadcast packets received by the interface.
OutOctets	The number of outbound octets transmitted by the interface.
OutUcastPkts	The number of outbound unicast packets transmitted by the interface.
OutMcastPkts	The number of outbound multicast packets transmitted by the interface.
OutBcastPkts	The number of outbound broadcast packets transmitted by the interface.

Example: The following shows example CLI display output for the command.

```
(Routing) #show interface counters

Port               InOctets      InUcastPkts      InMcastPkts      InBcastPkts
--------- ---------------- ---------------- ---------------- ----------------
0/1                0            0            0               0
0/2                0            0            0               0
0/3                15098        0            31               39
0/4                0            0            0               0
0/5                0            0            0               0
...
ch1                0            0            0               0
ch2                0            0            0               0
...
ch64               0            0            0               0
CPU                359533       0            3044            217
Port              OutOctets     OutUcastPkts     OutMcastPkts     OutBcastPkts
--------- ---------------- ---------------- ---------------- ----------------
0/1                0           0               0            0
0/2                0           0               0            0
0/3                131369      0               11           89
0/4                0           0               0            0
0/5                0           0               0            0
...
...
ch1                0           0               0            0
ch2                0           0               0            0
...
ch64               0           0               0            0
CPU                 4025293    0               32910        120
```

4.5.0.17 show interface ethernet

This command displays detailed statistics for a specific interface or for all interfaces or for all CPU traffic based upon the argument.

Format `show interface ethernet {`*`slot/port`* `|` *`all`* `| switchport}`

Mode Privileged EXEC

When you specify a value for *`slot/port`*, the command displays the following information.

Parameter	Definition
Packets Received	■ **Total Packets Received (Octets)** - The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including Frame Check Sequence (FCS) octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. The result of this equation is the value Utilization which is the percent utilization of the Ethernet segment on a scale of 0 to 100 percent. ■ **Packets Received 64 Octets** - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets). ■ **Packets Received 65–127 Octets** - The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets). ■ **Packets Received 128–255 Octets** - The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets). ■ **Packets Received 256–511 Octets** - The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets). ■ **Packets Received 512–1023 Octets** - The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). ■ **Packets Received 1024–1518 Octets** - The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets). ■ **Packets Received > 1518 Octets** - The total number of packets received that were longer than 1522 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. ■ **Packets RX and TX 64 Octets** - The total number of packets (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets). ■ **Packets RX and TX 65–127 Octets** - The total number of packets (including bad packets) received and transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets). ■ **Packets RX and TX 128–255 Octets** - The total number of packets (including bad packets) received and transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets). ■ **Packets RX and TX 256–511 Octets** - The total number of packets (including bad packets) received and transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).

Parameter	Definition
Packets Received (con't)	■ **Packets RX and TX 512–1023 Octets** - The total number of packets (including bad packets) received and transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). ■ **Packets RX and TX 1024–1518 Octets** - The total number of packets (including bad packets) received and transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets). ■ **Packets RX and TX 1519–2047 Octets** - The total number of packets received and transmitted that were between 1519 and 2047 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed. ■ **Packets RX and TX 1523–2047 Octets** - The total number of packets received and transmitted that were between 1523 and 2047 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed. ■ **Packets RX and TX 2048–4095 Octets** - The total number of packets received that were between 2048 and 4095 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed. ■ **Packets RX and TX 4096–9216 Octets** - The total number of packets received that were between 4096 and 9216 octets in length inclusive (excluding framing bits, but including FCS octets) and were otherwise well formed.
Packets Received Successfully	■ **Total Packets Received Without Error** - The total number of packets received that were without errors. ■ **Unicast Packets Received** - The number of subnetwork-unicast packets delivered to a higher-layer protocol. ■ **Broadcast Packets Received** - The total number of good packets received that were directed to the broadcast address.
Receive Packets Discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Packets Received with MAC Errors	■ **Total Packets Received with MAC Errors** - The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. ■ **Jabbers Received** - The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms. ■ **Fragments/Undersize Received** - The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets). ■ **Alignment Errors** - The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets. ■ **Rx FCS Errors -** The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets. ■ **Overruns** - The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow. ■ **uRPF Discards** - The number of packets dropped due to failing the uRPF.

Parameter	Definition
Received Packets Not Forwarded	■ **Total Received Packets Not Forwarded** - A count of valid frames received which were discarded (in other words, filtered) by the forwarding process ■ **Local Traffic Frames** - The total number of frames dropped in the forwarding process because the destination address was located off of this port. ■ **802.3x Pause Frames Received** - A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode. ■ **Unacceptable Frame Type** - The number of frames discarded from this port due to being an unacceptable frame type. ■ **Reserved Address Discards** - The number of frames discarded that are destined to an IEEE 802.1 reserved address and are not supported by the system. ■ **Broadcast Storm Recovery** - The number of frames discarded that are destined for `FF:FF:FF:FF:FF:FF` when Broadcast Storm Recovery is enabled. ■ **CFI Discards** - The number of frames discarded that have CFI bit set and the addresses in RIF are in non-canonical format. ■ **Upstream Threshold** - The number of frames discarded due to lack of cell descriptors available for that packet's priority level.
Packets Transmitted Octets	■ **Total Packets Transmitted (Octets)** - The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. ----- ■ **Packets Transmitted 64 Octets** - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets). ■ **Packets Transmitted 65-127 Octets** - The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets). ■ **Packets Transmitted 128-255 Octets** - The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets). ■ **Packets Transmitted 256-511 Octets** - The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets). ■ **Packets Transmitted 512-1023 Octets** - The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets). ■ **Packets Transmitted 1024-1518 Octets** - The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets). ■ **Packets Transmitted > 1518 Octets** - The total number of packets transmitted that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. ■ **Max Frame Size** - The maximum size of the Info (non-MAC) field that this port will receive or transmit. ■ **Maximum Transmit Unit** - The maximum Ethernet payload size.
Packets Transmitted Successfully	■ **Total Packets Transmitted Successfully**- The number of frames that have been transmitted by this port to its segment. ■ **Unicast Packets Transmitted** - The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent. ■ **Broadcast Packets Transmitted** - The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Transmit Errors	■ **Total Transmit Errors** - The sum of Single, Multiple, and Excessive Collisions. ■ **Tx FCS Errors** - The total number of packets transmitted that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets. ■ **Oversized** - The total number of frames that exceeded the max permitted frame size. This counter has a max increment rate of 815 counts per sec. at 10 Mb/s. ■ **Underrun Errors** - The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission.

Parameter	Definition
Transmit Discards	■ **Total Transmit Packets Discards** - The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded. ■ **Single Collision Frames** - A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. ■ **Multiple Collision Frames** - A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. ■ **Excessive Collisions** - A count of frames for which transmission on a particular interface fails due to excessive collisions. ■ **Port Membership Discards** - The number of frames discarded on egress for this port due to egress filtering being enabled.
Protocol Statistics	■ **802.3x Pause Frames Transmitted** - A count of MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode. ■ **GVRP PDUs Received** - Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol PDUs received. ■ GVRP PDUs Transmitted- GARP VLAN Registration Protocol PDUs transmitted. ■ GVRP Failed Registrations- Number of failed GVRP registrations. ■ GMRP PDUs Received - GARP Multicast Registration Protocol PDUs received. ■ GMRP PDUs Transmitted - GARP Multicast Registration Protocol PDUs transmitted ■ GMRP Failed Registrations - Number of failed GMRP registrations.
Protocol Statistics	■ **STP BPDUs Transmitted** - Spanning Tree Protocol Bridge Protocol Data Units sent. ■ **STP BPDUs Received** - Spanning Tree Protocol Bridge Protocol Data Units received. ■ **RST BPDUs Transmitted** - Rapid Spanning Tree Protocol Bridge Protocol Data Units sent. ■ **RSTP BPDUs Received** - Rapid Spanning Tree Protocol Bridge Protocol Data Units received. ■ **MSTP BPDUs Transmitted** - Multiple Spanning Tree Protocol Bridge Protocol Data Units sent. ■ **MSTP BPDUs Received** - Multiple Spanning Tree Protocol Bridge Protocol Data Units received. ■ **SSTP BPDUs Transmitted** - Shared Spanning Tree Protocol Bridge Protocol Data Units sent. ■ **SSTP BPDUs Received** - Shared Spanning Tree Protocol Bridge Protocol Data Units received.
Dot1x Statistics	■ **EAPOL Frames Transmitted** - The number of EAPOL frames of any type that have been transmitted by this authenticator. ■ **EAPOL Start Frames Received** - The number of valid EAPOL start frames that have been received by this authenticator.
Traffic Load Statistics	■ **Load Interval** - The length of time for which data is used to compute load statistics. The value is given in seconds, and must be a multiple of 30. The allowable range is from 30 to 600 seconds ■ **Bits Per Second Received** - Approximate number of bits per second received. This value is an exponentially weighted average and is affected by the configured load-interval. ■ **Bits Per Second Transmitted**. - Approximate number of bits per second transmitted. This value is an exponentially weighted average and is affected by the configured load-interval. ■ **Packets Per Second Received**- Approximate number of packets per second received. This value is an exponentially weighted average and is affected by the configured load-interval. ■ **Packets Per Second Transmitted** - Approximate number of packets per second transmitted. This value is an exponentially weighted average and is affected by the configured load-interval. ■ **Percent Utilization Received** - Value of link utilization in percentage representation for the RX line. ■ **Percent Utilization Transmitted** - Value of link utilization in percentage representation for the TX line.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

If you use the `all` keyword, the following information appears.

Parameter	Definition
Total Octets Transmitted	The total number of octets of data (including those in bad packets) transmitted on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.
Total Octets Received	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including Frame Check Sequence (FCS) octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. The result of this equation is the value utilization which is the percent utilization of the Ethernet segment on a scale of 0 to 100 percent.
Total Packets Transmitted Successfully	The number of frames that have been transmitted by this port to its segment.
Total Packets Received Without Error	The total number of packets received that were without errors.

If you use the `switchport` keyword, the following information appears.

Parameter	Definition
Octets Received	The total number of octets of data received by the processor (excluding framing bits but including FCS octets).
Total Packets Received Without Error	The total number of packets (including broadcast packets) received by the processor.
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address.
Receive Packets Discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Octets Transmitted	The total number of octets transmitted out of the interface, including framing characters.
Packets Transmitted without Errors	The total number of packets transmitted out of the interface.
Unicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.
Most Address Entries Ever Used	The highest number of Forwarding Database Address Table entries that have been learned by this switch since the most recent reboot.
Address Entries in Use	The number of Learned and static entries in the Forwarding Database Address Table for this switch.
Maximum VLAN Entries	The maximum number of Virtual LANs (VLANs) allowed on this switch.
Most VLAN Entries Ever Used	The largest number of VLANs that have been active on this switch since the last reboot.
Static VLAN Entries	The number of presently active VLAN entries on this switch that have been created statically.
VLAN Deletes	The number of VLANs on this switch that have been created and then deleted since the last reboot.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.

Example: The following shows example CLI display output for the command when you use the `all` keyword.

```
(Routing) #show interface ethernet all
```

```
Port   Bytes Tx  Bytes Rx  Packets Tx   Packets Rx
-----  --------  --------  ----------   ----------
0/1    0         0         0            0
0/2    0         0         0            0
..
..
1/1    0         0         0            0
1/2    0         0         0            0
..
..
```

4.5.0.18 show mac-addr-table

This command displays the forwarding database entries. These entries are used by the transparent bridging function to determine how to forward a received frame.

Enter `all` or no parameter to display the entire table. Enter a MAC Address and VLAN ID to display the table entry for the requested MAC address on the specified VLAN. Enter the `count` parameter to view summary information about the forwarding database table. Use the `interface {slot/port | lag lag-id}` parameter to view MAC addresses on a specific interface. Use the `vlan vlan_id` parameter to display information about MAC addresses on a specified VLAN.

Format `show mac-addr-table [{macaddr vlan_id | all | count | interface {slot/port | lag lag-id | vlan vlan_id} | vlan vlan_id}]`

Mode Privileged EXEC

The following information displays if you do not enter a parameter, the keyword all, or the MAC address and VLAN ID.

Parameter	Definition
VLAN ID	The VLAN in which the MAC address is learned.
MAC Address	A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example `01:23:45:67:89:AB`.
Interface	The port through which this address was learned.
Interface Index	This object indicates the ifIndex of the interface table entry associated with this port.
Status	The status of this entry. The meanings of the values are: ■ *Static*—The value of the corresponding instance was added by the system or a user when a static MAC filter was defined. It cannot be relearned. ■ *Learned*—The value of the corresponding instance was learned by observing the source MAC addresses of incoming traffic, and is currently in use. ■ *Management*—The value of the corresponding instance (system MAC address) is also the value of an existing instance of dot1dStaticAddress. It is identified with interface 0/1. and is currently used when enabling VLANs for routing. ■ *Self*—The value of the corresponding instance is the address of one of the switch's physical interfaces (the system's own MAC address). ■ *Other*—The value of the corresponding instance does not fall into one of the other categories.

If you enter `vlan vlan_id`, only the MAC Address, Interface, and Status fields appear. If you enter the `interface` ***`slot/port`*** parameter, in addition to the MAC Address and Status fields, the VLAN ID field also appears.

The following information displays if you enter the `count` parameter:

Parameter	Definition
Dynamic Address count	Number of MAC addresses in the forwarding database that were automatically learned.
Static Address (User-defined) count	Number of MAC addresses in the forwarding database that were manually entered by a user.
Total MAC Addresses in use	Number of MAC addresses currently in the forwarding database.
Total MAC Addresses available	Number of MAC addresses the forwarding database can handle.

4.5.0.19 process cpu threshold

Use this command to configure the CPU utilization thresholds. The Rising and Falling thresholds are specified as a percentage of CPU resources. The utilization monitoring time period can be configured from 5 seconds to 86400 seconds in multiples of 5 seconds. The CPU utilization threshold configuration is saved across a switch reboot. Configuring the falling utilization threshold is optional. If the falling CPU utilization parameters are not configured, then they take the same value as the rising CPU utilization parameters.

Format `process cpu threshold type total rising` ***`1-100`*** `interval`

Mode Global Config

Parameter	Description
rising threshold	The percentage of CPU resources that, when exceeded for the configured rising interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).
rising interval	The duration of the CPU rising threshold violation, in seconds, that must be met to trigger a notification. The range is 5 to 86400. The default is 0 (disabled).

Parameter	Description
falling threshold	The percentage of CPU resources that, when usage falls below this level for the configured interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled). A notification is triggered when the total CPU utilization falls below this level for a configured period of time. The falling utilization threshold notification is made only if a rising threshold notification was previously done. The falling utilization threshold must always be equal or less than the rising threshold value. The CLI does not allow setting the falling threshold to be greater than the rising threshold.
falling interval	The duration of the CPU falling threshold, in seconds, that must be met to trigger a notification. The range is 5 to 86400. The default is 0 (disabled).

4.5.0.20 show process app-list

This command displays the user and system applications.

NOTE: This command is available in Linux 2.6 only.

Format `show process app-list`

Mode Privileged EXEC

Parameter	Description
ID	The application identifier.
Name	The name that identifies the process.
PID	The number the software uses to identify the process.
Admin Status	The administrative status of the process.
Auto Restart	Indicates whether the process will automatically restart if it stops.
Running Status	Indicates whether the process is currently running or stopped.

Example: The following shows example CLI display output for the command.

```
                            Admin     Auto      Running
ID    Name             PID  Status    Restart   Status
---- ---------------- ----- --------- --------- -------
   1 dataplane        15309 Enabled   Disabled  Running
   2 switchdrvr       15310 Enabled   Disabled  Running
   3 syncdb           15314 Enabled   Disabled  Running
   4 lighttpd         18718 Enabled   Enabled   Running
   5 syncdb-test          0 Disabled  Disabled  Stopped
   6 proctest             0 Disabled  Enabled   Stopped
   7 user.start           0 Enabled   Disabled  Stopped
```

4.5.0.21 show process proc-list

This command displays the configured and in-use processes.

NOTE: This command is available in Linux 2.6 only.

Format `show process proc-list`

Mode Privileged EXEC

Parameter	Description
PID	The number the software uses to identify the process.
Process Name	The name that identifies the process.
Application ID-Name	The application identifier and its associated name.
Child	Indicates whether the process has spawned a child process.
VM Size	Virtual memory size.
VM Peak	The maximum amount of virtual memory the process has used at a given time.
FD Count	The file descriptors count for the process.

Example: The following shows example CLI display output for the command.

```
(Routing) #show process proc-list

      Process         Application               VM Size  VM Peak
PID   Name            ID-Name              Chld  (KB)     (KB)    FD Count
---- ---------------- -------------------- ---- -------- -------- --------
15260 procmgr          0-procmgr             No       1984     1984        8
15309 dataplane        1-dataplane           No     293556   293560       11
15310 switchdrvr       2-switchdrvr          No     177220   177408       57
15314 syncdb           3-syncdb              No       2060     2080        8
18718 lighttpd         4-lighttpd            No       5508     5644       11
18720 lua_magnet       4-lighttpd            Yes     12112    12112        7
18721 lua_magnet       4-lighttpd            Yes     25704    25708        7
```

4.5.0.22 show process app-resource-list

This command displays the configured and in-use resources of each application.

NOTE: This command is available in Linux 2.6 only.

Format `show process app-resource-list`

Mode Privileged EXEC

Parameter	Description
ID	The application identifier.
Name	The name that identifies the process.
PID	The number the software uses to identify the process.
Memory Limit	The maximum amount of memory the process can consume.
CPU Share	The maximum percentage of CPU utilization the process can consume.
Memory Usage	The amount of memory the process is currently using.
Max Mem Usage	The maximum amount of memory the process has used at any given time since it started.

```
(Routing) #show process app-resource-list

                          Memory      CPU       Memory      Max Mem
ID   Name            PID  Limit       Share     Usage       Usage
---- ---------------- ---- ----------- --------- ----------- -----------
   1 switchdrvr       251   Unlimited Unlimited      380 MB      381 MB
   2 syncdb           252   Unlimited Unlimited        0 MB        0 MB
```

```
   3 syncdb-test          0   Unlimited Unlimited        0 MB        0 MB
   4 proctest             0       10 MB       20%        0 MB        0 MB
   5 utelnetd             0   Unlimited Unlimited        0 MB        0 MB
   6 lxshTelnetd          0   Unlimited Unlimited        0 MB        0 MB
   7 user.start           0   Unlimited Unlimited        0 MB        0 MB
```

4.5.0.23 show process cpu threshold

This command provides the percentage utilization of the CPU by different tasks.

NOTE: It is not necessarily the traffic to the CPU, but different tasks that keep the CPU busy.

Format `show process cpu threshold`

Mode Privileged EXEC

The following shows example CLI display output for the command using Linux.

```
(Switching) #show process cpu
Memory Utilization Report
status      bytes
------ ----------
free    106450944
alloc   423227392

 CPU Utilization:

  PID      Name                    5 Secs     60 Secs    300 Secs
--------------------------------------------------------------------
  765    _interrupt_thread          0.00%       0.01%       0.02%
  767    bcmL2X.0                   0.58%       0.35%       0.28%
  768    bcmCNTR.0                  0.77%       0.73%       0.72%
  773    bcmRX                      0.00%       0.04%       0.05%
  786    cpuUtilMonitorTask         0.19%       0.23%       0.23%
  834    dot1s_task                 0.00%       0.01%       0.01%
  810    hapiRxTask                 0.00%       0.01%       0.01%
  805    dtlTask                    0.00%       0.02%       0.02%
  863    spmTask                    0.00%       0.01%       0.00%
  894    ip6MapLocalDataTask        0.00%       0.01%       0.01%
  908    RMONTask                   0.00%       0.11%       0.12%
--------------------------------------------------------------------
 Total CPU Utilization             1.55%       1.58%       1.50%
```

4.5.0.24 show running-config

Use this command to display or capture the current setting of different protocol packages supported on the switch. This command displays or captures commands with settings and configurations that differ from the default value. To display or capture the commands with settings and configurations that are equal to the default value, include the `all` option.

NOTE: Show running-config does not display the User Password, even if you set one different from the default.

The output is displayed in script format, which can be used to configure another switch with the same configuration. If the optional `scriptname` is provided with a file name extension of ".scr", the output is redirected to a script file.

NOTE: Note the following:

- If you issue the `show running-config` command from a serial connection, access to the switch through

remote connections (such as Telnet) is suspended while the output is being generated and displayed.

- If you use a text-based configuration file, the `show running-config` command will only display configured physical interfaces, i.e. if any interface only contains the default configuration, that interface will be skipped from the `show running-config` command output. This is true for any configuration mode that contains nothing but default configuration. That is, the command to enter a particular config mode, followed immediately by its exit command, are both omitted from the `show running-config` command output (and hence from the startup-config file when the system configuration is saved.)

Use the following keys to navigate the command output.

Key	Action
Enter	Advance one line.
Space Bar	Advance one page.
q	Stop the output and return to the prompt.

Note that `--More-- or (q)uit` is displayed at the bottom of the output screen until you reach the end of the output.

This command captures the current settings of OSPFv2 trapflag status:

- If all the flags are enabled, then the command displays `trapflags all`.
- If all the flags in a particular group are enabled, then the command displays `trapflags group name all`.
- If some, but not all, of the flags in that group are enabled, the command displays `trapflags groupname flag-name`.

Format `show running-config [all | scriptname]`

Mode Privileged EXEC

4.5.0.25 show running-config interface

Use this command to display the running configuration for a specific interface. Valid interfaces include physical, LAG, loopback, tunnel and VLAN interfaces.

Format `show running-config interface {interface | lag {lag-intf-num} | loopback {loopback-id} | tunnel {tunnel-id} | vlan {vlan-id}}`

Mode Privileged EXEC

Parameter	Description
interface	Running configuration for the specified interface.
lag-intf-num	Running configuration for the LAG interface.
loopback-id	Running configuration for the loopback interface.
tunnel-id	Running configuration for the tunnel interface.
vlan-id	Running configuration for the VLAN routing interface.

The following information is displayed for the command.

Parameter	Description
slot|port	Enter an interface in slot/port format.
lag	Display the running config for a specified lag interface.

Parameter	Description
loopback	Display the running config for a specified loopback interface.
tunnel	Display the running config for a specified tunnel interface.
vlan	Display the running config for a specified vlan routing interface.

Example: The following shows example CLI display output for the command.

```
(Routing) #show running-config interface 0/1
!Current Configuration:
!
interface  0/1
addport 3/1
exit
(Routing) #
```

4.5.0.26 show

This command displays the content of text-based configuration files from the CLI. The text-based configuration files (startup-config, backup-config and factory-defaults) are saved compressed in flash. With this command, the files are decompressed while displaying their content.

Format `show { startup-config | backup-config | factory-defaults }`

Mode Privileged EXEC

Parameter	Description
startup-config	Display the content of the startup-config file.
backup-config	Display the content of the backup-config file.
factory-defaults	Display the content of the factory-defaults file.

Example: The following shows example CLI display output for the command using the startup-config parameter.

```
(Routing) #show startup-config
!Current Configuration:
!
!System Description "Quanta LB6M, 8.1.14.41, Linux 2.6.27.47, U-Boot 2009.06 (Apr 19 2011 - 15:57:06)"
!System Software Version "8.1.14.41"
!System Up Time          "0 days 0 hrs 48 mins 19 secs"
!Cut-through mode is configured as disabled
!Additional Packages     BGP-4,QOS,IPv6,IPv6 Management,Routing,Data Center
!Current SNTP Synchronized Time: Not Synchronized
!
vlan database
vlan 10
exit
configure
ipv6 router ospf
exit
line console
exit
line telnet
exit
line ssh
exit
```

```
!
--More-- or (q)uit
interface 0/1
description 'intf1'
exit
router ospf
exit
exit
```

Example: The following shows example CLI display output for the command using the backup-config parameter.

```
(Routing) #show backup-config
!Current Configuration:
!
!System Description "Quanta LB6M, 8.1.14.41, Linux 2.6.27.47, U-Boot 2009.06 (Apr 19 2011 - 15:57:06)"
!System Software Version "8.1.14.41"
!System Up Time          "0 days 0 hrs 48 mins 19 secs"
!Cut-through mode is configured as disabled
!Additional Packages     BGP-4,QOS,IPv6,IPv6 Management,Routing,Data Center
!Current SNTP Synchronized Time: Not Synchronized
!
vlan database
vlan 10
exit
configure
ipv6 router ospf
exit
line console
exit
line telnet
exit
line ssh
exit
!
--More-- or (q)uit
interface 0/1
description 'intf1'
exit
router ospf
exit
exit
```

Example: The following shows example CLI display output for the command using the factory-defaults parameter.

```
(Routing) #show factory-defaults
!Current Configuration:
!
!System Description "Quanta LB6M, 8.1.14.41, Linux 2.6.27.47, U-Boot 2009.06 (Apr 19 2011 - 15:57:06)"
!System Software Version "8.1.14.41"
!System Up Time          "0 days 0 hrs 48 mins 19 secs"
!Cut-through mode is configured as disabled
!Additional Packages     BGP-4,QOS,IPv6,IPv6 Management,Routing,Data Center
!Current SNTP Synchronized Time: Not Synchronized
!
vlan database
vlan 10
exit
configure
ipv6 router ospf
exit
line console
```

```
exit
line telnet
exit
line ssh
exit
!
--More-- or (q)uit
interface 0/1
description 'intf1'
exit
router ospf
exit
exit
```

4.5.0.27 show sysinfo

This command displays switch information.

Format `show sysinfo`
Mode Privileged EXEC

Parameter	Definition
Switch Description	Text used to identify this switch.
System Name	Name used to identify the switch.The factory default is blank. To configure the system name, see Section 3.10.0.1, snmp-server.
System Location	Text used to identify the location of the switch. The factory default is blank. To configure the system location, see Section 3.10.0.1, snmp-server.
System Contact	Text used to identify a contact person for this switch. The factory default is blank. To configure the system location, see Section 3.10.0.1, snmp-server.
System ObjectID	The base object ID for the switch's enterprise MIB.
System Up Time	The time in days, hours and minutes since the last switch reboot.
MIBs Supported	A list of MIBs supported by this agent.

4.5.0.28 show tech-support

Use the `show tech-support` command to display system and configuration information for the whole system, or for BGP, BGP-IPv6, OSPF, or OSPFv3 when you contact technical support. The output includes log history files from previous runs. The output of the `show tech-support` command combines the output of the following commands and includes log history files from previous runs:

- show version
- show sysinfo
- show port all
- show isdp neighbors
- show logging
- show event log
- show logging buffered
- show trap log
- show previous run persistent logs
- show running config

- show debugging

NOTE: The log messages are sorted and displayed in reverse chronological order.

Format `show tech-support [bgp|bgp-ipv6|ospf|ospfv3]`
Mode Privileged EXEC

4.5.0.29 length *value*

Use this command to set the pagination length to value number of lines for the sessions specified by configuring on different Line Config modes (telnet/ssh/console) and is persistent.

Example: Length command on Line Console mode applies for Serial Console session.

Default `24`
Format `length value`
Mode Line Config

4.5.0.29.1 no length *value*

Use this command to set the pagination length to the default value number of lines.

Format `no length value`
Mode Line Config

4.5.0.30 terminal length

Use this command to set the pagination length to *value* number of lines for the current session. This command configuration takes an immediate effect on the current session and is nonpersistent.

Default 24 lines per page
Format `terminal length value`
Mode Privileged EXEC

4.5.0.30.1 no terminal length

Use this command to set the *value* to the length value configured on Line Config mode depending on the type of session.

Format `no terminal length value`
Mode Privileged EXEC

4.5.0.31 show terminal length

Use this command to display all the configured terminal length values.

Format `show terminal length`
Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) #show terminal length
Terminal Length:
----------------------
For Current Session..... 24
For Serial Console..... 24
For Telnet Sessions..... 24
For SSH Sessions..... 24
```

4.5.0.32 memory free low-watermark processor

Use this command to get notifications when the CPU free memory falls below the configured threshold. A notification is generated when the free memory falls below the threshold. Another notification is generated once the available free memory rises to 10 percent above the specified threshold. To prevent generation of excessive notifications when the CPU free memory fluctuates around the configured threshold, only one Rising or Falling memory notification is generated over a period of 60 seconds. The threshold is specified in kilobytes. The CPU free memory threshold configuration is saved across a switch reboot.

Format `memory free low-watermark processor` *`1-1034956`*

Mode Global Config

Parameter	Description
low-watermark	When CPU free memory falls below this threshold, a notification message is triggered. The range is 1 to the maximum available memory on the switch. The default is 0 (disabled).

4.5.0.33 clear mac-addr-table

Use this command to dynamically clear learned entries from the forwarding database. Using the following options, the user can specify the set of dynamically-learned forwarding database entries to clear.

Default No default value.

Format `clear mac-addr-table {all | vlan` *`vlanId`* `| interface` *`slot/port`* `|` *`macAddr`* `[`*`macMask`*`] }`

Mode Privileged EXEC

Parameter	Description
all	Clears dynamically learned forwarding database entries in the forwarding database table.
vlan *vlanId*	Clears dynamically learned forwarding database entries for this *vlanId*.
interface *slot/port*	Clears forwarding database entries learned on for the specified interface.
macAddr macMask	Clears dynamically learned forwarding database entries that match the range specified by MAC address and MAC mask. When MAC mask is not entered, only specified MAC is removed from the forwarding database table.

4.6 Logging Commands

This section describes the commands you use to configure system logging, and to view logs and the logging settings.

4.6.0.1 logging buffered

This command enables logging to an in-memory log.

Default	disabled; critical when enabled
Format	`logging buffered`
Mode	Global Config

4.6.0.1.1 no logging buffered

This command disables logging to in-memory log.

Format	`no logging buffered`
Mode	Global Config

4.6.0.2 logging buffered wrap

This command enables wrapping of in-memory logging when the log file reaches full capacity. Otherwise when the log file reaches full capacity, logging stops.

Default	enabled
Format	`logging buffered wrap`
Mode	Global Config

4.6.0.2.1 no logging buffered wrap

This command disables wrapping of in-memory logging and configures logging to stop when the log file capacity is full.

Format	`no logging buffered wrap`
Mode	Global Config

4.6.0.3 logging cli-command

This command enables the CLI command logging feature, which enables the EFOS software to log all CLI commands issued on the system. The commands are stored in a persistent log. Use the `show logging persistent` command to display the stored history of CLI commands.

Default	enabled
Format	`logging cli-command`
Mode	Global Config

4.6.0.3.1 no logging cli-command

This command disables the CLI command Logging feature.

Format `no logging cli-command`
Mode Global Config

4.6.0.4 logging console

This command enables logging to the console. You can specify the `severitylevel` value as either an integer from 0 to 7 or symbolically through one of the following keywords: `emergency` (0), `alert` (1), `critical` (2), `error` (3), `warning` (4), `notice` (5), `info` (6), or `debug` (7).

Default disabled; critical when enabled
Format `logging console [severitylevel]`
Mode Global Config

4.6.0.4.1 no logging console

This command disables logging to the console.

Format `no logging console`
Mode Global Config

4.6.0.5 logging host

This command configures the logging host parameters. You can configure up to eight hosts.

Default
- port: 514 (for UDP) and 6514 (for TLS)
- authentication mode: anonymous
- certificate index: 0
- level: critical (2)

Format `logging host {hostaddress|hostname} addresstype tls [anon|x509name] certificate-index {port severitylevel}`
Mode Global Config

Parameter	Description
hostaddress|hostname	The IP address of the logging host.
address-type	Indicates the type of address being passed: DNS or IPv4.
tls	Enables TLS security for the host.
anon|x509name	The type of authentication mode: anonymous or x509name.
certificate-index	The certificate number to be used for authentication. The valid range is 0–8. Index 0 is used to the default file.
port	A port number from 1 to 65535.
severitylevel	Specify this value as either an integer from 0 to 7, or symbolically through one of the following keywords: `emergency` (0), `alert` (1), `critical` (2), `error` (3), `warning` (4), `notice` (5), `info` (6), or `debug` (7).

Example: The following shows examples of the command.

```
(Routing) (Config)# logging host google.com dns 214
```

```
(Routing) (Config)# logging host 10.130.64.88 ipv4 214 6
(Routing) (Config)# logging host 5.5.5.5 ipv4 tls anon 6514 debug
(Routing) (Config)# logging host 5.5.5.5 ipv4 tls x509name 3 6514 debug
```

4.6.0.6 logging host reconfigure

This command enables logging host reconfiguration.

Format `logging host reconfigure` *`hostindex`*
Mode Global Config

Parameter	Description
hostindex	Enter the Logging Host Index for which to change the IP address.

4.6.0.7 logging host remove

This command disables logging to host. See Section 4.6.0.15, show logging hosts for a list of host indexes.

Format `logging host remove` *`hostindex`*
Mode Global Config

4.6.0.8 logging persistent

Use this command to configure the Persistent logging for the switch. The severity level of logging messages is specified at severity level. Possible values for severity level are (emergency|0, alert|1, critical|2, error|3, warning|4, notice|5, info|6, debug|7).

Default Disable
Format `logging persistent` *`severity level`*
Mode Global Config

4.6.0.8.1 no logging persistent

Use this command to disable the persistent logging in the switch.

Format `no logging persistent`
Mode Global Config

4.6.0.9 logging protocol

Use this command to configure the logging protocol version number as 0 or 1. RFC 3164 uses version 0 and RFC 5424 uses version 1.

Default The default is version 0 (RFC 3164).
Format `logging protocol {0|1}`
Mode Global Config

4.6.0.10 logging syslog

This command enables syslog logging. Use the optional `facility` parameter to set the default facility used in syslog messages for components that do not have an internally assigned facility. The *`facility`* value can be one of the following keywords: `kernel, user, mail, system, security, syslog, lpr, nntp, uucp, cron, auth, ftp, ntp, audit, alert, clock, local0, local1, local2, local3, local4, local5, local6, local7`. The default facility is `local7`.

Default disabled
Format `logging syslog [facility` *`facility`*`]`
Mode Global Config

4.6.0.10.1 no logging syslog

This command disables syslog logging.

Format `no logging syslog [facility]`
Mode Global Config

4.6.0.11 logging syslog port

This command enables syslog logging. The `portid` parameter is an integer with a range of 1-65535.

Default disabled
Format `logging syslog port` *`portid`*
Mode Global Config

4.6.0.11.1 no logging syslog port

This command disables syslog logging.

Format `no logging syslog port`
Mode Global Config

4.6.0.12 logging syslog source-interface

Use this command to specify the physical or logical interface to use as the Syslog client source interface. If configured, the address of source Interface is used for all Syslog communications between the Syslog server and the Syslog client. Otherwise there is no change in behavior. If the configured interface is down, the Syslog client falls back to normal behavior.

Format `logging syslog source-interface {`*`slot/port`*`|{loopback` *`loopback-id`*`}|{vlan vlan-id}}`
Mode Global Config

Parameter	Description
slot/port	Specifies the port to use as the source interface.
loopback-id	Specifies the loopback interface to use as the source interface. The range of the loopback ID is 0 to 7.
tunnel-id	Specifies the tunnel interface to use as the source interface. The range of the tunnel ID is 0 to 7.
vlan-id	Specifies the VLAN to use as the source interface.

4.6.0.12.1 no logging syslog source-interface

Use this command to remove the configured global source interface (Source IP selection) for all Syslog communications between the Syslog client and the server.

Format `no logging syslog source-interface`
Mode Global Config

4.6.0.13 show logging

This command displays logging configuration information.

Format `show logging`
Mode Privileged EXEC

Term	Definition
Logging Client Local Port	Port on the collector/relay to which syslog messages are sent.
Logging Client Source Interface	Shows the configured syslog source-interface (source IP address).
CLI Command Logging	Shows whether CLI Command logging is enabled.
Logging Protocol	The logging protocol version number. ■ 0: RFC 3164 ■ 1: RFC 5424
Console Logging	Shows whether console logging is enabled.
Console Logging Severity Filter	The minimum severity to log to the console log. Messages with an equal or lower numerical severity are logged.
Buffered Logging	Shows whether buffered logging is enabled.
Persistent Logging	Shows whether persistent logging is enabled.
Persistent Logging Severity Filter	The minimum severity at which the logging entries are retained after a system reboot.
Syslog Logging	Shows whether syslog logging is enabled.
Syslog Logging Facility	Shows the value set for the facility in syslog messages.
Log Messages Received	Number of messages received by the log process. This includes messages that are dropped or ignored.
Log Messages Dropped	Number of messages that could not be processed due to error or lack of resources.
Log Messages Relayed	Number of messages sent to the collector/relay.

Example: The following shows example CLI display output for the command.

```
(Routing) #show logging

Logging Client Local Port           : 514
Logging Client USB File Name        :
Logging Client Source Interface     : (not configured)
CLI Command Logging                 : disabled
```

```
Console Logging                      : enabled
Console Logging Severity Filter      : error
Buffered Logging                     : enabled
Buffered Logging Severity Filter     : info
Persistent Logging                   : disabled
Persistent Logging Severity Filter   : alert

Syslog Logging                       : disabled
Syslog Logging Facility              : local7

Log Messages Received                : 229
Log Messages Dropped                 : 0
Log Messages Relayed                 : 0
```

4.6.0.14 show logging buffered

This command displays buffered logging (system startup and system operation logs).

Format `show logging buffered`

Mode Privileged EXEC

Parameter	Definition
Buffered (In-Memory) Logging	Shows whether the In-Memory log is enabled or disabled.
Buffered Logging Wrapping Behavior	The behavior of the In Memory log when faced with a log full situation.
Buffered Log Count	The count of valid entries in the buffered log.

4.6.0.15 show logging hosts

This command displays all configured logging hosts.

Format `show logging hosts`

Mode Privileged EXEC

Term	Definition
Host Index	(Used for deleting hosts.)
IP Address / Hostname	IP address or hostname of the logging host.
Severity Level	The minimum severity to log to the specified address. The possible values are emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), or debug (7).
Port	The server port number, which is the port on the local host from which syslog messages are sent.
Status	Status field provides the current status of snmp row status. (Active, Not in Service, Not Ready).
Mode	The type of security: UDP or TLS.
Auth	The type of authentication mode: anonymous or x509name.
Cert #	The certificate number to be used for authentication. The valid range is 0–8. Index 0 is used to the default file.

Example: The following shows example CLI display output for the command.

```
(Routing) #show logging hosts
Index  IP Address/Hostname  Severity   Port   Status    Mode
-----  --------------------  ---------- ------ --------- -----
1      1.1.1.17              critical   514    Active    udp
2      10.130.191.90         debug      10514  Active    tls
3      5.5.5.5               debug      333    Active    tls

Auth     Cert#
-------- -----

x509name 6
x509name 4
```

4.6.0.16 show logging persistent

Use the **show logging persistent** command to display persistent log entries. If `log-files` is specified, the persistent log files the system are displayed.

Format `show logging persistent [log-files]`

Mode Privileged EXEC

Parameter	Description
Persistent Logging	If persistent logging is enabled or disabled.
Persistent Log Count	The number of persistent log entries.
Persistent Log Files	The list of persistent log files in the system. Only displayed if `log-files` is specified.

Example: The following shows example CLI display output for the command.

```
(Switching) #show logging persistent
Persistent Logging  : disabled
Persistent Log Count: 0

(Switching) #show logging persistent log-files

Persistent Log Files:

slog0.txt
slog1.txt
slog2.txt
olog0.txt
olog1.txt
olog2.txt
```

4.6.0.17 show logging traplogs

This command displays SNMP trap events and statistics.

Format `show logging traplogs`

Mode Privileged EXEC

Parameter	Definition
Number of Traps Since Last Reset	The number of traps since the last boot.
Trap Log Capacity	The number of traps the system can retain.
Number of Traps Since Log Last Viewed	The number of new traps since the command was last executed.
Log	The log number.
System Time Up	How long the system had been running at the time the trap was sent.
Trap	The text of the trap message.

4.6.0.18 clear logging buffered

This command clears buffered logging (system startup and system operation logs).

Format `clear logging buffered`

Mode Privileged EXEC

4.7 Email Alerting and Mail Server Commands

4.7.0.1 logging email

This command enables email alerting and sets the lowest severity level for which log messages are emailed. If you specify a severity level, log messages at or above this severity level, but below the urgent severity level, are emailed in a non-urgent manner by collecting them together until the log time expires. You can specify the `severitylevel` value as either an integer from 0 to 7 or symbolically through one of the following keywords: `emergency` (0), `alert` (1), `critical` (2), `error` (3), `warning` (4), `notice` (5), `info` (6), or `debug` (7).

Default disabled; when enabled, log messages at or above severity Warning (4) are emailed

Format `logging email` *`[severitylevel]`*

Mode Global Config

4.7.0.1.1 no logging email

This command disables email alerting.

Format `no logging email`

Mode Global Config

4.7.0.2 logging email urgent

This command sets the lowest severity level at which log messages are e-mailed immediately in a single e-mail message. Specify the `severitylevel` value as either an integer from 0 to 7 or symbolically through one of the following keywords: `emergency` (0), `alert` (1), `critical` (2), `error` (3), `warning` (4), `notice` (5), `info` (6), or `debug` (7). Specify `none` to indicate that log messages are collected and sent in a batch email at a specified interval.

Default Alert (1) and emergency (0) messages are sent immediately.

Format `logging email urgent {`*`severitylevel`* `| none}`

Mode Global Config

4.7.0.2.1 no logging email urgent

This command resets the urgent severity level to the default value.

Format `no logging email urgent`

Mode Global Config

4.7.0.3 logging email message-type to-addr

This command configures the email address to which messages are sent. The message types supported are `urgent`, `non-urgent`, and `both`. For each supported severity level, multiple email addresses can be configured. The *`to-email-addr`* variable is a standard email address, for example admin@yourcompany.com.

Format `logging email message-type {urgent |non-urgent |both} to-addr` *`to-email-addr`*

Mode Global Config

4.7.0.3.1 no logging email message-type to-addr

This command removes the configured to-addr field of email.

Format `no logging email message-type {urgent |non-urgent |both} to-addr` *`to-email-addr`*
Mode Global Config

4.7.0.4 logging email from-addr

This command configures the email address of the sender (the switch).

Default switch@broadcom.com
Format `logging email from-addr` *`from-email-addr`*
Mode Global Config

4.7.0.4.1 no logging email from-addr

This command removes the configured email source address.

Format `no logging email from-addr` *`from-email-addr`*
Mode Global Config

4.7.0.5 logging email message-type subject

This command configures the subject line of the email for the specified type.

Default For urgent messages: Urgent Log Messages
For non-urgent messages: Non Urgent Log Messages
Format `logging email message-type {urgent |non-urgent |both} subject` *`subject`*
Mode Global Config

4.7.0.5.1 no logging email message-type subject

This command removes the configured email subject for the specified message type and restores it to the default email subject.

Format `no logging email message-type {urgent |non-urgent |both} subject`
Mode Global Config

4.7.0.6 logging email logtime

This command configures how frequently non-urgent email messages are sent. Non-urgent messages are collected and sent in a batch email at the specified interval. The valid range is every 30–1440 minutes.

Default 30 minutes
Format `logging email logtime` *`minutes`*
Mode Global Config

4.7.0.6.1 no logging email logtime

This command resets the non-urgent log time to the default value.

Format `no logging email logtime`
Mode Global Config

4.7.0.7 logging traps

This command sets the severity at which SNMP traps are logged and sent in an email. Specify the `severitylevel` value as either an integer from 0 to 7 or symbolically through one of the following keywords: `emergency` (0), `alert` (1), `critical` (2), `error` (3), `warning` (4), `notice` (5), `info` (6), or `debug` (7).

Default Info (6) messages and higher are logged.
Format `logging traps` *`severitylevel`*
Mode Global Config

4.7.0.7.1 no logging traps

This command resets the SNMP trap logging severity level to the default value.
Format `no logging traps`
Mode Global Config

4.7.0.8 logging email test message-type

This command sends an email to the SMTP server to test the email alerting function.

Format `logging email test message-type {urgent |non-urgent |both} message-body` *`message-body`*
Mode Global Config

4.7.0.9 show logging email config

This command displays information about the email alert configuration.

Format `show logging email config`
Mode Privileged EXEC

Parameter	Definition
Email Alert Logging	The administrative status of the feature: enabled or disabled
Email Alert From Address	The email address of the sender (the switch).
Email Alert Urgent Severity Level	The lowest severity level that is considered urgent. Messages of this type are sent immediately.
Email Alert Non Urgent Severity Level	The lowest severity level that is considered non-urgent. Messages of this type, up to the urgent level, are collected and sent in a batch email. Log messages that are less severe are not sent in an email message at all.
Email Alert Trap Severity Level	The lowest severity level at which traps are logged.
Email Alert Notification Period	The amount of time to wait between non-urgent messages.
Email Alert To Address Table	The configured email recipients.

Parameter	Definition
Email Alert Subject Table	The subject lines included in urgent (Type 1) and non-urgent (Type 2) messages.
For Msg Type urgent, subject is	The configured email subject for sending urgent messages.
For Msg Type non-urgent, subject is	The configured email subject for sending non-urgent messages.

4.7.0.10 show logging email statistics

This command displays email alerting statistics.

Format `show logging email statistics`
Mode Privileged EXEC

Parameter	Definition
Email Alert Operation Status	The operational status of the email alerting feature.
No of Email Failures	The number of email messages that have attempted to be sent but were unsuccessful.
No of Email Sent	The number of email messages that were sent from the switch since the counter was cleared.
Time Since Last Email Sent	The amount of time that has passed since the last email was sent from the switch.

4.7.0.11 clear logging email statistics

This command resets the email alerting statistics.

Format `clear logging email statistics`
Mode Privileged EXEC

4.7.0.12 mail-server

This command configures the SMTP server to which the switch sends email alert messages and changes the mode to Mail Server Configuration mode. The server address can be in the IPv4 or DNS name format.

Format `mail-server {`*`ip-address`* `|` *`hostname`*`}`
Mode Global Config

4.7.0.12.1 no mail-server

This command removes the specified SMTP server from the configuration.

Format `no mail-server {`*`ip-address`* `|` *`hostname`*`}`
Mode Global Config

4.7.0.13 security

This command sets the email alerting security protocol by enabling the switch to use TLS authentication with the SMTP Server. If the TLS mode is enabled on the switch but the SMTP sever does not support TLS mode, no email is sent to the SMTP server.

Default none
Format `security {tlsv1 | none}`
Mode Mail Server Config

4.7.0.14 port (Mail Server Config Mode)

This command configures the TCP port to use for communication with the SMTP server. The recommended port for TLSv1 is 465, and for no security (i.e. none) it is 25. However, any nonstandard port in the range 1 to 65535 is also allowed.

Default 25
Format `port {465 | 25 | 1-65535}`
Mode Mail Server Config

4.7.0.15 username (Mail Server Config)

This command configures the login ID the switch uses to authenticate with the SMTP server.

Default admin
Format `username` *`name`*
Mode Mail Server Config

4.7.0.16 password (Mail Server Config Mode)

This command configures the password the switch uses to authenticate with the SMTP server.

Default admin
Format `password` *`password`*
Mode Mail Server Config

4.7.0.17 show mail-server config

This command displays information about the email alert configuration.

Format `show mail-server {`*`ip-address`* `|` *`hostname`* `| all} config`
Mode Privileged EXEC

Parameter	Definition
No of mail servers configured	The number of SMTP servers configured on the switch.
Email Alert Mail Server Address	The IPv4 address or DNS hostname of the configured SMTP server.
Email Alert Mail Server Port	The TCP port the switch uses to send email to the SMTP server
Email Alert Security Protocol	The security protocol (TLS or none) the switch uses to authenticate with the SMTP server.
Email Alert Username	The username the switch uses to authenticate with the SMTP server.
Email Alert Password	The password the switch uses to authenticate with the SMTP server.

4.8 System Utility and Clear Commands

This section describes the commands you use to help troubleshoot connectivity issues and to restore various configurations to their factory defaults.

4.8.0.1 clear config

This command resets the configuration of the switch to the configuration present in the `factory-defaults` configuration file, if this file is present, without powering off the switch. If the `factory-defaults` configuration file is not present, then EFOS compile time defaults are applied on the switch. When you issue this command, a prompt appears to confirm that the reset should proceed. When you enter `y`, you automatically reset the current configuration on the switch to the default values. It does not reset the switch.

Format `clear config`
Mode Privileged EXEC

4.8.0.2 clear config interface

This command resets the configuration in the specified interface or range of interfaces to the factory defaults without powering off the switch. When you issue this command, a prompt appears to confirm that the reset should proceed. When you enter `y`, you automatically reset the current configuration on the interface or interfaces to the default values. It does not reset the switch.

The `clear config interface` command clears the configuration only for commands issued in Interface Config mode. Interface-related commands which were not issued in Interface Config mode, such as enabling routing on a VLAN interface, cannot be cleared using this command

Format `clear config interface {`*`slot/port`* `|` `lag` *`lag_id`* `|` `vlan` *`vlan_id`* `|` `loopback` *`loopback_id}`*
Mode Privileged EXEC

4.8.0.3 clear counters

This command clears the statistics for a specified *`slot/port,`* for all the ports, or for an interface on a VLAN based on the argument. If a virtual router is specified, the statistics for the ports on the virtual router are cleared. If no router is specified, the information for the default router will be displayed.

Format `clear counters {`*`slot/port`* `|` `all [vrf` *`vrf-name`*`]` `|` `vlan` *`id`*`}`
Mode Privileged EXEC

4.8.0.4 clear ip access-list counters

This command clears the counters of the specified IP ACL and the IP ACL rule.

Format `clear ip access-list counters` *`acl-ID`* `|` *`acl-name rule-id`*
Mode Privileged EXEC

4.8.0.5 clear ipv6 access-list counters

This command clears the counters of the specified IP ACL and the IP ACL rule.

Format `clear ipv6 access-list counters` *`acl-name rule-id`*
Mode Privileged EXEC

4.8.0.6 clear mac access-list counters

This command clears the counters of the specified MAC ACL and MAC ACL rule.

Format `clear mac access-list counters` *`acl-name rule-id`*
Mode Privileged EXEC

4.8.0.7 clear pass

This command resets all user passwords to the factory defaults without powering off the switch. You are prompted to confirm that the password reset should proceed.

Format `clear pass`
Mode Privileged EXEC

4.8.0.8 clear traplog

This command clears the trap log.
Format `clear traplog`
Mode Privileged EXEC

4.8.0.9 clear vlan

This command resets VLAN configuration parameters to the factory defaults.

Format `clear vlan`
Mode Privileged EXEC

4.8.0.10 clear vlan stats

This command clears the supported per-VLAN statistics for the VLAN(s) specified.

Format `clear vlan [`*`vlan-list`*`] stats`
Mode Privileged EXEC

Example: Clear statistics on VLAN 10.

```
(Switching) # clear vlan 10 stats
```

Example: Clear statistics on multiple VLANs 10, 20, and 30.

```
(Switching) # clear vlan 10,20,30 stats
```

Example: Clear statistics on all available VLANs.

```
(Switching) # clear vlan stats
```

4.8.0.11 logout

This command closes the current telnet connection or resets the current serial connection.

NOTE: Save configuration changes before logging out.

Format `logout`

Modes
- Privileged EXEC
- User EXEC

4.8.0.12 ping

Use this command to determine whether another computer is on the network. Ping provides a synchronous response when initiated from the CLI interface.

NOTE: For information about the `ping` command for IPv6 hosts, see Section 3.2.0.15, ping ipv6.

Default
- The default count is 1.
- The default interval is 3 seconds.
- The default size is 0 bytes.

Format `ping [vrf` ***`vrf-name`*** `] {`***`ip-address`***`| `***`hostname`*** `| {ipv6 {interface {`***`slot/port`*** `| vlan `***`1-4093`*** `| loopback `***`loopback-id`*** `| network | serviceport | tunnel `***`tunnel-id`*** `} `***`link-local-address`***`} | `***`ip6addr`*** `| `***`hostname`***`} [count `***`count`***`] [interval 1-60] [size `***`size`***`] [source `***`ip-address`*** `| `***`ip6addr`*** `| {`***`slot/port`*** `| vlan `***`1-4093`*** `| serviceport | network}] [outgoing-interface {`***`slot/port`*** `| vlan 1-4093 | serviceport | network}]`

Modes
- Privileged EXEC
- User EXEC

Using the options described below, you can specify the number and size of Echo Requests and the interval between Echo Requests.

Parameter	Description
vrf-name	The name of the virtual router in which to initiate the ping. If no virtual router is specified, the ping is initiated in the default router instance.
address	IPv4 or IPv6 addresses to ping.
count	Use the `count` parameter to specify the number of ping packets (ICMP Echo requests) that are sent to the destination address specified by the ***`ip-address`*** field. The range for ***`count`*** is 1 to 15 requests.
interval	Use the `interval` parameter to specify the time between Echo Requests, in seconds. Range is 1 to 60 seconds.
size	Use the `size` parameter to specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to 65507 bytes.
source	Use the *source* parameter to specify the source IP/IPv6 address or interface to use when sending the Echo requests packets.
hostname	Use the *hostname* parameter to resolve to an IPv4 or IPv6 address. The *ipv6* keyword is specified to resolve the hostname to IPv6 address. The IPv4 address is resolved if no keyword is specified.
ipv6	The optional keyword *ipv6* can be used before the *ipv6-address* or *hostname* argument. Using the *ipv6* optional keyword before *hostname* tries to resolve it directly to the IPv6 address. Also used for pinging a link-local IPv6 address.
interface	Use the *interface* keyword to ping a link-local IPv6 address over an interface.
link-local-address	The link-local IPv6 address to ping over an interface.
outgoing-interface	Use the outgoing-interface parameter to specify the outgoing interface for multicast IP/IPv6 ping.

The following are examples of the CLI command.

Example: ping success:

```
(Routing) #ping 10.254.2.160 count 3 interval 1 size 255
Pinging 10.254.2.160 with 255 bytes of data:

Received response for icmp_seq = 0. time = 275268 usec
Received response for icmp_seq = 1. time = 274009 usec
Received response for icmp_seq = 2. time = 279459 usec

----10.254.2.160 PING statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (msec) min/avg/max = 274/279/276
```

Example: ping failure:

In Case of Unreachable Destination:

```
(Routing) # ping 192.168.254.222 count 3 interval 1 size 255
Pinging 192.168.254.222 with 255 bytes of data:
Received Response: Unreachable Destination
Received Response :Unreachable Destination
Received Response :Unreachable Destination
----192.168.254.222  PING statistics----
3 packets transmitted,3 packets received, 0% packet loss
round-trip (msec) min/avg/max = 0/0/0
```

In Case Of Request TimedOut:

```
(Routing) # ping 1.1.1.1 count 1 interval 3
Pinging 1.1.1.1 with 0 bytes of data:

----1.1.1.1 PING statistics----
1 packets transmitted,0 packets received, 100% packet loss
round-trip (msec) min/avg/max = 0/0/0
```

4.8.0.13 quit

This command closes the current telnet connection or resets the current serial connection. The system asks you whether to save configuration changes before quitting.

Format `quit`

Modes
- Privileged EXEC
- User EXEC

4.8.0.14 reload

This command resets the switch without powering it off. Reset means that all network connections are terminated and the boot code executes. The switch uses the stored configuration to initialize the switch. You are prompted to confirm that the reset should proceed. The LEDs on the switch indicate a successful reset.

If ONIE is installed, the `os` parameter is added to the reload command. This parameter enables the user to boot back into ONIE.

Format `reload [warm | configuration [`*`scriptname`*`]]`

Mode Privileged EXEC

Parameter	Description
warm	When the Warm Reload feature is present, the reload command adds the `warm` option. This option reduces the time it takes to reboot a Linux switch, thereby reducing the traffic disruption in the network during a switch reboot. For a typical Linux Enterprise switch, the traffic disruption is reduced from about two minutes for a cold reboot to about 20 seconds for a warm reboot. **NOTE:** The Warm Reload starts only the application process. The Warm Reload does not restart the boot code, the Linux kernel and the root file system. Since the Warm Reload does not restart all components, some code upgrades require that customers perform a cold reboot. **NOTE:** Warm resets can only be initiated by the administrator and do not occur automatically.
configuration	Gracefully reloads the configuration. If no configuration file is specified, the startup-config file is loaded.
scriptname	The configuration file to load. The scriptname must include the extension.

4.8.0.15 dying-gasp

Use this command to allow a dying-gasp notification to be sent through Syslog or Ethernet-OAM when the switch loses power or resets abruptly. The switch reset might be due to an unexpected software failure, a LOG_ERROR, or a user-triggered switch reload. The Dying Gasp feature also notifies dying gasp events as *SNMP trap* to the trap receiver

The ability to send a dying-gasp notification on loss of power depends on the platform hardware capability. The switch hardware must be able to supply back power for approximately 300 ms to send the dying gasp notification after the abrupt power loss or reset occurs.

Format `dying-gasp primary {syslog | ethernet-oam | snmptrap} secondary { syslog | ethernet-oam |snmptrap}`

Mode Global Config

Parameter	Description
primary	Dying Gasp primary notification
secondary	Dying Gasp secondary notification
ethernet-oam	Enable Ethernet-OAM notification
syslog	Enable system logger
snmptrap	Enable SNMP trap notification

4.8.0.15.1 no dying-gasp

This command disables the sending of dying gasp notifications.

Format `no dying-gasp`

Mode Global Config

4.8.0.16 show dying-gasp

This command displays the dying gasp configuration status.

Format `show dying-gasp status`

Mode Privileged EXEC

The command displays the information shown in the following table.

Parameter	Description
Dying Gasp Primary Mode	Identifies the primary notification mode, which can be one of the following: ■ Syslog ■ Ethernet-OAM ■ SnmpTrap
Dying Gasp Secondary Mode	Identifies the secondary notification mode, which can be one of the following: ■ Syslog ■ Ethernet-OAM ■ SnmpTrap

4.8.0.17 copy

The `copy` command uploads and downloads files to and from the switch. You can also use the `copy` command to manage the dual images (active and backup) on the file system. Upload and download files from a server using FTP, TFTP, Xmodem, Ymodem, or Zmodem. SFTP and SCP are available as additional transfer methods if the software package supports secure management. If FTP is used, a password is required. CLI-based file transfers using the HTTP and HTTPS protocols are supported on selected platforms where a native wget utility is available.

Format `copy` *`source destination`* `{verify | noverify}`

Mode Privileged EXEC

Replace the *`source`* and *`destination`* parameters with the options in Table 9, Copy Parameters. For the *`url`* source or destination, use one of the following values:
`{xmodem | tftp://`*`ipaddr`*`|`*`hostname`* `|` *`ip6address`*`|`*`hostname/filepath/filename`* `[noval]| sftp|scp://`*`username@ipaddr`* `|` *`ipv6address/filepath/filename`* `|` `ftp://`*`user@ipaddress`* `|` *`hostname/filepath/filename`*`}`

`verify` | *`noverify`* is only available if the image/configuration verify options feature is enabled (see Section 4.8.0.18, file verify). `verify` specifies that digital signature verification will be performed for the specified downloaded image or configuration file. `noverify` specifies that no verification will be performed.

For HTTPS transfers, the `[checkcert | nocheckcert]` options are available to enable or disable server certificate validation. This option is valid only for HTTPS file transfer. If no option is specified, default action is applied for HTTPS file transfer.

The keyword **ias-users** supports the downloading of the IAS user database file. When the IAS users file is downloaded, the switch IAS user's database is replaced with the users and its attributes available in the downloaded file. In the command **copy *url* ias-users**, for *url* one of the following is used for IAS users file:

{ { tftp://<ipaddr | hostname> | <ipv6address | hostname> /<filepath>/<filename> } | { sftp | scp://<username>@<ipaddress>/<filepath>/<filename>} }

NOTE: The maximum length for the file path is 160 characters, and the maximum length for the file name is 31 characters.

For FTP, TFTP, SFTP and SCP, the *`ipaddr`*|*`hostname`* parameter is the IP address or host name of the server, *`filepath`* is the path to the file, and *`filename`* is the name of the file you want to upload or download. For SFTP and SCP, the *`username`* parameter is the username for logging into the remote server via SSH.

NOTE: *`ip6address`* is also a valid parameter for routing packages that support IPv6.

To copy OpenFlow SSL certificates to the switch using TFTP or XMODEM, using only the following options pertinent to the OpenFlow SSL certificates.

Format `copy [<mode/file>] nvram:{openflow-ssl-ca-cert | openflow-ssl-cert | openflow-ssl-priv-key}`

Mode Privileged EXEC

CAUTION! Remember to upload the existing fastpath.cfg file off the switch prior to loading a new release image in order to make a backup.

Table 9: Copy Parameters

Source	Destination	Description
`nvram:application` *`sourcefilename`*	*`url`*	Filename of source application file.
`nvram:backup-config`	`nvram:startup-config`	Copies the backup configuration to the startup configuration.
`nvram:clibanner`	*`url`*	Copies the CLI banner to a server.
`nvram: core-dump`	`tftp://<ipaddress|hostname>/<filepath>/<filename>| ftp://<user>@<ipaddr|hostname>/<path>/<filename> | scp://<user>@<ipaddr|hostname>/<path>/<filename> | sftp://<user>@<ipaddr|hostname>/<path>/<filename>}`	Uploads the core dump file on the local system to an external TFTP/FTP/SCP/SFTP server.
`nvram:crash-log`	`url`	Copies the crash log to a server.
`nvram:errorlog`	*`url`*	Copies the error log file to a server.
`nvram:factory-defaults`	*`url`*	Uploads factory defaults file.
`nvram:fastpath.cfg`	*`url`*	Uploads the binary config file to a server.
`nvram:license-key` *`index`*	*`url`*	Makes a backup of a license file of a specific index.
`nvram:log`	*`url`*	Copies the log file to a server.
`nvram:operational-log`	`url`	Copies the operational log file to a server.
`nvram:script` *`scriptname`*	*`url`*	Copies a specified configuration script file to a server.
`nvram:startup-config`	`nvram:backup-config`	Copies the startup configuration to the backup configuration.
`nvram:startup-config`	*`url`*	Copies the startup configuration to a server.
`nvram:startup-log`	`url`	Copies the startup log to a server.
`nvram: tech-support`	`url`	Uploads the system and configuration information for technical support.
`nvram:traplog`	*`url`*	Copies the trap log file to a server.
`system:image`	`url`	Saves the system image to a server.
`system:running-config`	`nvram:startup-config`	Saves the running configuration to NVRAM.
`system:running-config`	`nvram:factory-defaults`	Saves the running configuration to NVRAM to the `factory-defaults` file.
`url`	`nvram:application` *`destfilename`*	Destination file name for the application file.

Table 9: Copy Parameters (Continued)

Source	Destination	Description
url	nvram: application *destfilename*	Downloads an application to the system.
url	nvram: backup-config	Downloads the backup configuration to the
url	nvram:ca-root *index*	Downloads the CA certificate file to /mnt/fastpath directory and uses the index number name the downloaded file to CA*index*.pem
url	nvram:ca-root-certs	Downloads root CA certificate file(s) to the /mnt/fastpath/root-certificates directory. The root CA certificates can beused by the native wget utility for HTTPS server certificate validation during the file download operation via HTTPS from the `copy` command.
url	nvram:clibanner	Downloads the CLI banner to the system.
url	nvram:client-key *index*	Downloads the client key file to the /mnt/fastpath directory and uses the index number name the downloaded file to CA*index*.key.
url	nvram:client-ssl-cert *1-8*	Downloads the client certificate to the /mnt/fastpath directory and uses the index number to name the downloaded file to CA*index*.pem.
url	nvram:fastpath.cfg	Downloads the binary config file to the system.
url	nvram:license-key [*index*]	Downloads a license file in a specific index. The downloaded file is stored as license.dat <*index*> in persistent storage.
url	nvram:script *destfilename*	Downloads a configuration script file to the system. During the download of a configuration script, the copy command validates the script. In case of any error, the command lists all the lines at the end of the validation process and prompts you to confirm before copying the script file.
url	nvram:script *destfilename* noval	When you use this option, the copy command will not validate the downloaded script file. An example of the CLI command follows:
(Routing) #copy tftp://1.1.1.1/file.scr nvram:script file.scr noval		
url	nvram:sshkey-dsa	Downloads an SSH key file. For more information, see Section 3.5, Secure Shell Commands.
url	nvram:sshkey-rsa1	Downloads an SSH key file.
url	nvram:sshkey-rsa2	Downloads an SSH key file.
url	nvram:openflow-ssl-ca-cert	Downloads Openflow CA Certificate.
url	nvram:openflow-ssl-cert	Downloads Openflow Switch Certificate.
url	nvram:openflow-ssl-priv-key	Downloads Openflow Private Key.
url	nvram:startup-config	Downloads the startup configuration file to the system.
url	ias-users	Downloads an IAS users database file to the system. When the IAS users file is downloaded, the switch IAS user's database is replaced with the users and their attributes available in the downloaded file.
url	nvram:tech-support-cmds	Downloads the file containing list of commands to be displayed using the `show tech-support` command.
url	{active | backup}	Download an image from the remote server to either image.
{active | backup}	*url*	Upload either image to the remote server.
active	backup	Copy the active image to the backup image.
backup	active	Copy the backup image to the active image.

Example: The following shows an example of downloading and applying ias users file.

```
(Routing) #copy tftp://10.131.17.104/aaa_users.txt ias-users

Mode..................................... TFTP
Set Server IP............................ 10.131.17.104
Path..................................... ./
Filename................................. aaa_users.txt
Data Type................................ IAS Users

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer operation completed successfully.

Validating and updating the users to the IAS users database.

Updated IAS users database successfully.
```

Example: The following shows an example of downloading a license file in a specific index.

```
(dhcp-10-130-84-117) #copy scp://testuser@10.89.25.12/license.dat nvram:license-key 2
Remote Password:**********

Mode..................................... SCP
Set Server IP............................ 10.89.25.12
Path..................................... ./
Filename................................. license.dat
Data Type................................ license



Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer in progress. Management access will be blocked for the duration of the transfer. Please
wait...
Warning: Identity file /mnt/fastpath/ssh_host_key not accessible: No such file or directory.
+---------------------------------------------------------------------------+
|   Authorized Use Only.  Use of this system must be in accordance with     |
|   our Acceptable Use Policy located at http://accept-use.broadcom.com.    |
|   Activity on this system is subject to monitoring and logging.           |
+---------------------------------------------------------------------------+
SCP License Key transfer starting...


License Key transfer operation completed successfully. System reboot is required.
```

Example: The following shows an example of making a backup of a license file of a specific index.

```
(localhost) # copy nvram:license-key 1 scp://testuser@10.89.25.12/ license1.dat
```

4.8.0.18 file verify

This command enables digital signature verification while an image and/or configuration file is downloaded to the switch.

Format	`file verify {all | image | none | script}`
Mode	Global Config

Parameter	Description
All	Verifies the digital signature of both image and configuration files.
Image	Verifies the digital signature of image files only.
None	Disables digital signature verification for both images and configuration files.
Script	Verifies the digital signature of configuration files.

4.8.0.18.1 no file verify

Resets the configured digital signature verification value to the factory default value.

Format `no file verify`
Mode Global Config

4.8.0.19 write memory

Use this command to save running configuration changes to NVRAM so that the changes you make will persist across a reboot. This command is the same as `copy system:running-config nvram:startup-config`. Use the `confirm` keyword to directly save the configuration to NVRAM without prompting for a confirmation.

Format `write memory [confirm]`
Mode Privileged EXEC

4.8.0.20 ip scp server enable

This command enables SCP server functionality for SCP push operations on the EFOS switch, which allows files to be transferred from the host device to the switch using the SCP protocol. During an SCP file transfer operation, the management operations on the switch are blocked. After the completion of file download to the EFOS switch, the switch performs file validations similar to other download operations executed via the `copy` command.

To allow the SCP file transfers from the host system to the EFOS switch, the SCP server must be enabled on the switch.

Default Disabled
Format `ip scp server enable`
Mode Privileged EXEC

The transfer is initiated via the CLI on the host system, and not from the EFOS CLI. The following examples show the syntax for SCP push commands executed on a PC host for configuration and firmware images.

- `scp <config file> user@<scp server IP>:startup-config`
- `scp <config file> user@<scp server IP>:backup-config`
- `scp <config file> user@<scp server IP>:factory-defaults`
- `scp <config file> user@<scp server IP>:<scriptfile.scr>`
- `scp <image file> user@<scp server IP>:active`
- `scp <image file> user@<scp server IP>:backup`

4.8.0.20.1 no ip scp server enable

This command resets the SCP server functionality for SCP push operations on the EFOS switch to the default value (disabled).

Format `no ip scp server enable`
Mode Privileged EXEC

4.9 Simple Network Time Protocol Commands

This section describes the commands you use to automatically configure the system time and date by using Simple Network Time Protocol (SNTP).

4.9.0.1 sntp broadcast client poll-interval

This command sets the poll interval for SNTP broadcast clients in seconds as a power of two where `poll-interval` can be a value from 6 to 10.

Default 6
Format `sntp broadcast client poll-interval` *`poll-interval`*
Mode Global Config

4.9.0.1.1 no sntp broadcast client poll-interval

This command resets the poll interval for SNTP broadcast client back to the default value.

Format `no sntp broadcast client poll-interval`
Mode Global Config

4.9.0.2 sntp client mode

This command enables Simple Network Time Protocol (SNTP) client mode and may set the mode to either broadcast or unicast.

Default disabled
Format `sntp client mode` *`[broadcast | unicast]`*
Mode Global Config

4.9.0.2.1 no sntp client mode

This command disables Simple Network Time Protocol (SNTP) client mode.

Format `no sntp client mode`
Mode Global Config

4.9.0.3 sntp client port

This command sets the SNTP client port ID to a 0, 123, or a value between 1025 and 65535. The default value is 0, which means that the SNTP port is not configured by the user. In the default case, the actual client port value used in SNTP packets is assigned by the underlying OS.

Default 0
Format `sntp client port` *`portid`*
Mode Global Config

4.9.0.3.1 no sntp client port

This command resets the SNTP client port back to its default value.

Format `no sntp client port`
Mode Global Config

4.9.0.4 sntp unicast client poll-interval

This command sets the poll interval for SNTP unicast clients in seconds as a power of two where *`poll-interval`* can be a value from 6 to 10.

Default 6
Format `sntp unicast client poll-interval` *`poll-interval`*
Mode Global Config

4.9.0.4.1 no sntp unicast client poll-interval

This command resets the poll interval for SNTP unicast clients to its default value.

Format `no sntp unicast client poll-interval`
Mode Global Config

4.9.0.5 sntp unicast client poll-timeout

This command will set the poll timeout for SNTP unicast clients in seconds to a value from 1-30.

Default 5
Format `sntp unicast client poll-timeout` *`poll-timeout`*
Mode Global Config

4.9.0.5.1 no sntp unicast client poll-timeout

This command will reset the poll timeout for SNTP unicast clients to its default value.

Format `no sntp unicast client poll-timeout`
Mode Global Config

4.9.0.6 sntp unicast client poll-retry

This command will set the poll retry for SNTP unicast clients to a value from 0 to 10.

Default 1
Format `sntp unicast client poll-retry` *`poll-retry`*
Mode Global Config

4.9.0.6.1 no sntp unicast client poll-retry

This command will reset the poll retry for SNTP unicast clients to its default value.

Format `no sntp unicast client poll-retry`
Mode Global Config

4.9.0.7 sntp server

This command configures an SNTP server (a maximum of three). The server address is an IPv4/IPv6 address. The optional priority can be a value of 1-3, the version a value of 1-4, and the port id a value of 1-65535.

Format `sntp server {`*`ipaddress`* `| ipv6address |` *`hostname`*`} [`*`priority`* `[`*`version`* `[`*`portid`*`]]]`
Mode Global Config

4.9.0.7.1 no sntp server

This command deletes an server from the configured SNTP servers.

Format `no sntp server remove {`*`ipaddress`* `| ipv6address |` *`hostname`*`}`
Mode Global Config

4.9.0.8 sntp source-interface

Use this command to specify the physical or logical interface to use as the SNTP client source interface. If configured, the address of source Interface is used for all SNTP communications between the SNTP server and the SNTP client. Otherwise there is no change in behavior. If the configured interface is down, the SNTP client falls back to its default behavior.

Format `sntp source-interface {`*`slot/port`* `| loopback` *`loopback-id`* `|` *`vlan vlan-id`*`}`
Mode Global Config

Parameter	Description
slot/port	Specifies the port to use as the source interface.
loopback-id	Specifies the loopback interface to use as the source interface. The range of the loopback ID is 0 to 7.
tunnel-id	Specifies the tunnel interface to use as the source interface. The range of the tunnel ID is 0 to 7.
vlan-id	Specifies the VLAN to use as the source interface.

4.9.0.8.1 no sntp source-interface

Use this command to reset the SNTP source interface to the default settings.

Format `no sntp source-interface`
Mode Global Config

4.9.0.9 show sntp

This command is used to display SNTP settings and status.

Format `show sntp`
Mode Privileged EXEC

Parameter	Definition
Last Update Time	Time of last clock update.
Last Attempt Time	Time of last transmit query (in unicast mode).
Last Attempt Status	Status of the last SNTP request (in unicast mode) or unsolicited message (in broadcast mode).
Broadcast Count	Current number of unsolicited broadcast messages that have been received and processed by the SNTP client since last reboot.

4.9.0.10 show sntp client

This command is used to display SNTP client settings.

Format `show sntp client`
Mode Privileged EXEC

Parameter	Definition
Client Supported Modes	Supported SNTP Modes (Broadcast or Unicast).
SNTP Version	The highest SNTP version the client supports.
Port	SNTP Client Port. The field displays the value 0 if it is default value. When the client port value is 0, if the client is in broadcast mode, it binds to port 123; if the client is in unicast mode, it binds to the port assigned by the underlying OS.
Client Mode	Configured SNTP Client Mode.

4.9.0.11 show sntp server

This command is used to display SNTP server settings and configured servers.

Format `show sntp server`
Mode Privileged EXEC

Parameter	Definition
Server Host Address	IP address or hostname of configured SNTP Server.
Server Type	Address type of server (IPv4 or IPv6 or DNS).

Parameter	Definition
Server Stratum	Claimed stratum of the server for the last received valid packet.
Server Reference ID	Reference clock identifier of the server for the last received valid packet.
Server Mode	SNTP Server mode.
Server Maximum Entries	Total number of SNTP Servers allowed.
Server Current Entries	Total number of SNTP configured.

For each configured server:

Parameter	Definition
IP Address / Hostname	IP address or hostname of configured SNTP Server.
Address Type	Address Type of configured SNTP server (IPv4 or IPv6 or DNS).
Priority	IP priority type of the configured server.
Version	SNTP Version number of the server. The protocol version used to query the server in unicast mode.
Port	Server Port Number.
Last Attempt Time	Last server attempt time for the specified server.
Last Update Status	Last server attempt status for the server.
Total Unicast Requests	Number of requests to the server.
Failed Unicast Requests	Number of failed requests from server.

4.9.0.12 show sntp source-interface

Use this command to display the SNTP client source interface configured on the switch.

Format `show sntp source-interface`

Mode Privileged EXEC

Field	Description
SNTP Client Source Interface	The interface ID of the physical or logical interface configured as the SNTP client source interface.
SNTP Client Source IPv4 Address	The IP address of the interface configured as the SNTP client source interface.

Example: The following shows example CLI display output for the command.

```
(Routing) #show sntp source-interface

SNTP Client Source Interface.................. 0/2
SNTP Client Source IPv4 Address............... 192.168.2.20          [Up]
```

4.10 Time Zone Commands

4.10.0.1 clock set

This command sets the system time and date.

NOTE: System time and date cannot be set when SNTP is enabled. If SNTP is enabled after you configure the system time and date, the SNTP clock takes precedence over the user-configured system time and date. If the platform supports real-time clock (RTC), the set time and date can be retained after a save and reload. Otherwise, the configured clock will not be retained across reloads.

Format `clock set hh:mm:ss`
`clock set` *`mm/dd/yyyy`*

Mode Global Config

Parameter	Description
hh	Hours in 24-hour format. The range is 0 to 23.
mm	Minutes, the range is 0 to 59.
ss	Seconds, the range is 0 to 59.
mm	Month, in 2-character numeric format. The range is 01 to 12.
dd	Day, in 2-character numeric format. The range is 01 to 31.
yyyy	Year, in 4-character numeric format. The range is 2010 to 2079.

Example: The following shows an example of the command.

```
(Routing)(Config)# clock set 03:17:00
(Routing) (Config)# clock set 11/01/2011
```

4.10.0.2 clock summer-time date

This command sets the Daylight Saving Time (DST), also known as summertime, offset to UTC. You have to specify the start year and end year along with the month, day, and time. If the optional parameters are not specified, they are read as either zero (0) or \0, as appropriate.

Format `clock summer-time date {`*`date month year hh:mm date month year hh:mm`*`}[offset` *`offset`*`] [zone` *`acronym`*`]`

Mode Global Config

Parameter	Description
date	Day of the month. The range is 1 to 31.
month	Month. The range is the first three letters by name (for example, Jan).
year	Year. The range is 2000 to 2097.
hh:mm	Time in 24-hour format in hours and minutes. hh range is 0 to 23, mm range is 0 to 59.
offset	The number of minutes to add during the summertime. The range is 1 to 1440.
acronym	The acronym for the time zone to be displayed when summertime is in effect. The range is up to four characters.

Example: The following shows examples of the command.

```
(Routing) (Config)# clock summer-time date 1 nov 2011 3:18 2 nov 2011 3:18
```

(Routing) (Config)# clock summer-time date 1 nov 2011 3:18 2 nov 2011 3:18 offset 120 zone INDA

4.10.0.3 clock summer-time recurring

This command sets the summertime offset to UTC recursively every year. This means that summertime will affect every year from the time of configuration. You have to specify the start and end parameters which include the month, day, and time. If the optional parameters are not specified, they are read as either zero (0) or \0, as appropriate.

Format `clock summer-time recurring {`*`week day month hh:mm week day month hh:mm`*`}[offset `*`offset`*`] [zone `*`acronym`*`]`

Mode Global Config

Parameter	Description
EU	The system clock uses the standard recurring summer time settings used in countries in the European Union.
USA	The system clock uses the standard recurring daylight saving time settings used in the United States.
week	Week of the month. Range is 1 to 5, first, last.
day	Day of the week. The range is the first three letters by name; sun, for example.
month	Month. The range is the first three letters by name; jan for example.
hh:mm	Time in 24-hour format in hours and minutes. hh range is 0 to 23, mm range is 0 to 59.
offset	The number of minutes to add during the summertime. The range is 1 to 1440.
acronym	The acronym for the time zone to be displayed when summertime is in effect. The range is up to four characters.

Example: The following shows examples of the command.

```
(Routing) (Config)# clock summer-time recurring 2 sun nov 3:18 2 mon nov 3:18
(Routing) (Config)# clock summer-time recurring 2 sun nov 3:18 2 mon nov 3:18 offset 120 zone INDA
```

4.10.0.3.1 no clock summer-time

This command resets the summertime configuration.

Format `no clock summer-time`

Mode Global Config

Example: The following shows an example of the command.

```
(Routing) (Config)# no clock summer-time
```

4.10.0.4 clock timezone

`This command sets the offset to Coordinated Universal Time (UTC). If the optional parameters are not specified, they will be read as either zero (0) or \0 as appropriate.`

Format `clock timezone {`*`hours`*`} [minutes `*`minutes`*`] [zone `*`acronym`*`]`

Mode Global Config

Parameter	Description
hours	Hours difference from UTC. The range is –12 to 14.
minutes	Minutes difference from UTC. The range is zero (0) to 59.
acronym	The acronym for the time zone. The range is up to four characters.

Example: The following shows an example of the command.

```
(Routing) (Config)# clock timezone 5 minutes 30 zone INDA
```

4.10.0.4.1 no clock timezone

This command resets the time zone settings.

Format no clock timezone

Mode Global Config

Example: The following shows an example of the command.

```
(Routing) (Config)# no clock timezone
```

4.10.0.5 show clock

This command displays the time and date from the system clock.

Format show clock

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) # show clock
15:02:09 (UTC+0:00) Nov 1 2011
No time source
```

Example: With the configuration above, the following output appears:

```
(Routing) # show clock

10:55:40 INDA(UTC+7:30) Nov 1 2011
No time source
```

4.10.0.6 show clock detail

This command displays the detailed system time along with the time zone and the summertime configuration.

Format show clock detail

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) # show clock detail

15:05:24 (UTC+0:00) Nov 1 2011
No time source

 Time zone:
 Acronym not configured
 Offset is UTC+0:00
```

```
 Summertime:
 Summer-time is disabled
```

Example: With the configuration above, the following output appears:

```
(Routing) # show clock detail

10:57:57 INDA(UTC+7:30) Nov 1 2011
No time source

 Time zone:
 Acronym is INDA
 Offset is UTC+5:30

 Summertime:
 Acronym is INDA
 Recurring every year
 Begins on second Sunday of Nov at 03:18
 Ends on second Monday of Nov at 03:18
 Offset is 120 minutes
```

4.11 DHCP Server Commands

This section describes the commands you to configure the DHCP server settings for the switch. DHCP uses UDP as its transport protocol and supports a number of features that facilitate in administration address allocations.

4.11.0.1 ip dhcp pool

This command configures a DHCP address pool name on a DHCP server and enters DHCP pool configuration mode.

Default none
Format `ip dhcp pool` *`name`*
Mode Global Config

4.11.0.1.1 no ip dhcp pool

This command removes the DHCP address pool. The name should be previously configured pool name.

Format `no ip dhcp pool` *`name`*
Mode Global Config

4.11.0.2 client-identifier

This command specifies the unique identifier for a DHCP client. Unique-identifier is a valid notation in hexadecimal format. In some systems, such as Microsoft DHCP clients, the client identifier is required instead of hardware addresses. The unique-identifier is a concatenation of the media type and the MAC address. For example, the Microsoft client identifier for Ethernet address c819.2488.f177 is 01c8.1924.88f1.77 where 01 represents the Ethernet media type. For more information, refer to the “Address Resolution Protocol Parameters” section of RFC 1700, Assigned Numbers for a list of media type codes.

Default none
Format `client-identifier` *`uniqueidentifier`*
Mode DHCP Pool Config

4.11.0.2.1 no client-identifier

This command deletes the client identifier.

Format `no client-identifier`
Mode DHCP Pool Config

4.11.0.3 client-name

This command specifies the name for a DHCP client. Name is a string consisting of standard ASCII characters.

Default none
Format `client-name` *`name`*
Mode DHCP Pool Config

4.11.0.3.1 no client-name

This command removes the client name.

Format `no client-name`
Mode DHCP Pool Config

4.11.0.4 default-router

This command specifies the default router list for a DHCP client. {*address1, address2… address8*} are valid IP addresses, each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Default none
Format `default-router` *address1 [address2....address8]*
Mode DHCP Pool Config

4.11.0.4.1 no default-router

This command removes the default router list.

Format `no default-router`
Mode DHCP Pool Config

4.11.0.5 dns-server

This command specifies the IP servers available to a DHCP client. Address parameters are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Default none
Format `dns-server` *address1 [address2....address8]*
Mode DHCP Pool Config

4.11.0.5.1 no dns-server

This command removes the DNS Server list.

Format `no dns-server`
Mode DHCP Pool Config

4.11.0.6 hardware-address

This command specifies the hardware address of a DHCP client. Hardware-address is the MAC address of the hardware platform of the client consisting of 6 bytes in dotted hexadecimal format. Type indicates the protocol of the hardware platform. It is 1 for 10 MB Ethernet and 6 for IEEE 802.

Default ethernet
Format `hardware-address` *hardwareaddress type*
Mode DHCP Pool Config

4.11.0.6.1 no hardware-address

This command removes the hardware address of the DHCP client.

Format `no hardware-address`
Mode DHCP Pool Config

4.11.0.7 host

This command specifies the IP address and network mask for a manual binding to a DHCP client. Address and Mask are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid. The prefix-length is an integer from 0 to 32.

Default none
Format `host address [{mask | prefix-length}]`
Mode DHCP Pool Config

4.11.0.7.1 no host

This command removes the IP address of the DHCP client.

Format `no host`
Mode DHCP Pool Config

4.11.0.8 lease

This command configures the duration of the lease for an IP address that is assigned from a DHCP server to a DHCP client. The overall lease time should be between 1-86400 minutes. If you specify *infinite*, the lease is set for 60 days. You can also specify a lease duration. *Days* is an integer from 0 to 59. *Hours* is an integer from 0 to 23. *Minutes* is an integer from 0 to 59.

Default 1 (day)
Format `lease [{days [hours] [minutes] | infinite}]`
Mode DHCP Pool Config

4.11.0.8.1 no lease

This command restores the default value of the lease time for DHCP Server.

Format `no lease`
Mode DHCP Pool Config

4.11.0.9 network (DHCP Pool Config)

Use this command to configure the subnet number and mask for a DHCP address pool on the server. Network-number is a valid IP address, made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid. Mask is the IP subnet mask for the specified address pool. The prefix-length is an integer from 0 to 32.

Default	none
Format	`network` *`networknumber`* `[{`*`mask`* `|` *`prefixlength`*`}]`
Mode	DHCP Pool Config

4.11.0.9.1 no network

This command removes the subnet number and mask.

Format	`no network`
Mode	DHCP Pool Config

4.11.0.10 bootfile

The command specifies the name of the default boot image for a DHCP client. The *`filename`* specifies the boot image file.

Format	`bootfile` *`filename`*
Mode	DHCP Pool Config

4.11.0.10.1 no bootfile

This command deletes the boot image name.

Format	`no bootfile`
Mode	DHCP Pool Config

4.11.0.11 domain-name

This command specifies the domain name for a DHCP client. The *`domain`* specifies the domain name string of the client.

Default	none
Format	`domain-name` *`domain`*
Mode	DHCP Pool Config

4.11.0.11.1 no domain-name

This command removes the domain name.

Format	`no domain-name`
Mode	DHCP Pool Config

4.11.0.12 domain-name enable

This command enables the domain name functionality in EFOS.

Format	`domain-name enable [name` *`name]`*
Mode	Global Config

Example: The following shows an example of the command.

```
(Switching) (Config)#domain-name enable
(Switching) (Config)#exit
```

4.11.0.12.1 no domain-name enable

This command disables the domain name functionality in EFOS.

Format	`no domain-name enable`
Mode	Global Config

4.11.0.13 netbios-name-server

This command configures NetBIOS Windows Internet Naming Service (WINS) name servers that are available to DHCP clients.

One IP address is required, although one can specify up to eight addresses in one command line. Servers are listed in order of preference (address1 is the most preferred server, address2 is the next most preferred server, and so on).

Default	none
Format	`netbios-name-server` *`address`* `[`*`address2...address8`*`]`
Mode	DHCP Pool Config

4.11.0.13.1 no netbios-name-server

This command removes the NetBIOS name server list.

Format	`no netbios-name-server`
Mode	DHCP Pool Config

4.11.0.14 netbios-node-type

The command configures the NetBIOS node type for Microsoft Dynamic Host Configuration Protocol (DHCP) clients.type Specifies the NetBIOS node type. Valid types are:

- b-node—Broadcast
- p-node—Peer-to-peer
- m-node—Mixed
- h-node—Hybrid (recommended)

Default	none
Format	`netbios-node-type` *`type`*
Mode	DHCP Pool Config

4.11.0.14.1 no netbios-node-type

This command removes the NetBIOS node Type.

Format	`no netbios-node-type`
Mode	DHCP Pool Config

4.11.0.15 next-server

This command configures the next server in the boot process of a DHCP client.The *address* parameter is the IP address of the next server in the boot process, which is typically a TFTP server.

Default	inbound interface helper addresses
Format	`next-server` *address*
Mode	DHCP Pool Config

4.11.0.15.1 no next-server

This command removes the boot server list.

Format	`no next-server`
Mode	DHCP Pool Config

4.11.0.16 option

The `option` command configures DHCP Server options. The *code* parameter specifies the DHCP option code and ranges from 1-254. The *ascii string* parameter specifies an NVT ASCII character string. ASCII character strings that contain white space must be delimited by quotation marks. The *hex string* parameter specifies hexadecimal data. In hexadecimal, character strings are two hexadecimal digits. You can separate each byte by a period (for example, `a3.4f.22.0c`), colon (for example, `a3:4f:22:0c`), or white space (for example, `a3 4f 22 0c`).

Default	none
Format	`option` *code* `{`*ascii string* `|` *hex string1* `[`*string2...string8*`]` `|` `ip` *address1* `[`*address2...address8*`]}`
Mode	DHCP Pool Config

4.11.0.16.1 no option

This command removes the DHCP Server options. The *code* parameter specifies the DHCP option code.

Format	`no option` *code*
Mode	DHCP Pool Config

4.11.0.17 ip dhcp excluded-address

This command specifies the IP addresses that a DHCP server should not assign to DHCP clients. Low-address and high-address are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address `0.0.0.0` is invalid.

Default	none
Format	`ip dhcp excluded-address` *lowaddress [highaddress]*
Mode	Global Config

4.11.0.17.1 no ip dhcp excluded-address

This command removes the excluded IP addresses for a DHCP client. Low-address and high-address are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Format `no ip dhcp excluded-address` *`lowaddress [highaddress]`*
Mode Global Config

4.11.0.18 ip dhcp ping packets

Use this command to specify the number, in a range from 2-10, of packets a DHCP server sends to a pool address as part of a ping operation. By default the number of packets sent to a pool address is 2, which is the smallest allowed number when sending packets. Setting the number of packets to 0 disables this command.

Default 2
Format `ip dhcp ping packets` *`0,2-10`*
Mode Global Config

4.11.0.18.1 no ip dhcp ping packets

This command restores the number of ping packets to the default value.

Format `no ip dhcp ping packets`
Mode Global Config

4.11.0.19 service dhcp

This command enables the DHCP server.

Default disabled
Format `service dhcp`
Mode Global Config

4.11.0.19.1 no service dhcp

This command disables the DHCP server.

Format `no service dhcp`
Mode Global Config

4.11.0.20 ip dhcp bootp automatic

This command enables the allocation of the addresses to the bootp client. The addresses are from the automatic address pool.

Default disabled
Format `ip dhcp bootp automatic`
Mode Global Config

4.11.0.20.1 no ip dhcp bootp automatic

This command disables the allocation of the addresses to the bootp client. The address are from the automatic address pool.

Format `no ip dhcp bootp automatic`
Mode Global Config

4.11.0.21 ip dhcp conflict logging

This command enables conflict logging on DHCP server.

Default enabled
Format `ip dhcp conflict logging`
Mode Global Config

4.11.0.21.1 no ip dhcp conflict logging

This command disables conflict logging on DHCP server.

Format `no ip dhcp conflict logging`
Mode Global Config

4.11.0.22 clear ip dhcp binding

This command deletes an automatic address binding from the DHCP server database. If “*” is specified, the bindings corresponding to all the addresses are deleted. *`address`* is a valid IP address made up of four decimal bytes ranging from 0 to 255. IP address `0.0.0.0` is invalid.

Format `clear ip dhcp binding {`*`address`*` | *}`
Mode Privileged EXEC

4.11.0.23 clear ip dhcp server statistics

This command clears DHCP server statistics counters.

Format `clear ip dhcp server statistics`
Mode Privileged EXEC

4.11.0.24 clear ip dhcp conflict

The command is used to clear an address conflict from the DHCP Server database. The server detects conflicts using a ping. DHCP server clears all conflicts If the asterisk (*) character is used as the address parameter.

Default none
Format `clear ip dhcp conflict {`*`address`*` | *}`
Mode Privileged EXEC

4.11.0.25 show ip dhcp binding

This command displays address bindings for the specific IP address on the DHCP server. If no IP address is specified, the bindings corresponding to all the addresses are displayed.

Format `show ip dhcp binding [address]`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
IP address	The IP address of the client.
Hardware Address	The MAC Address or the client identifier.
Lease expiration	The lease expiration time of the IP address assigned to the client.
Type	The manner in which IP address was assigned to the client.

4.11.0.26 show ip dhcp global configuration

This command displays address bindings for the specific IP address on the DHCP server. If no IP address is specified, the bindings corresponding to all the addresses are displayed.

Format `show ip dhcp global configuration`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Service DHCP	The field to display the status of dhcp protocol.
Number of Ping Packets	The maximum number of Ping Packets that will be sent to verify that an ip address id not already assigned.
Conflict Logging	Shows whether conflict logging is enabled or disabled.
BootP Automatic	Shows whether BootP for dynamic pools is enabled or disabled.

4.11.0.27 show ip dhcp pool configuration

This command displays pool configuration. If `all` is specified, configuration for all the pools is displayed.

Format `show ip dhcp pool configuration {name | all}`

Modes
- Privileged EXEC
- User EXEC

Field	Definition
Pool Name	The name of the configured pool.
Pool Type	The pool type.
Lease Time	The lease expiration time of the IP address assigned to the client.
DNS Servers	The list of DNS servers available to the DHCP client.

Field	Definition
Default Routers	The list of the default routers available to the DHCP client

The following additional field is displayed for Dynamic pool type:

Field	Definition
Network	The network number and the mask for the DHCP address pool.

The following additional fields are displayed for Manual pool type:

Field	Definition
Client Name	The name of a DHCP client.
Client Identifier	The unique identifier of a DHCP client.
Hardware Address	The hardware address of a DHCP client.
Hardware Address Type	The protocol of the hardware platform.
Host	The IP address and the mask for a manual binding to a DHCP client.

4.11.0.28 show ip dhcp server statistics

This command displays DHCP server statistics.

Format `show ip dhcp server statistics`

Modes
- Privileged EXEC
- User EXEC

Field	Definition
Automatic Bindings	The number of IP addresses that have been automatically mapped to the MAC addresses of hosts that are found in the DHCP database.
Expired Bindings	The number of expired leases.
Malformed Bindings	The number of truncated or corrupted messages that were received by the DHCP server.

Message Received:

Message	Definition
DHCP DISCOVER	The number of DHCPDISCOVER messages the server has received.
DHCP REQUEST	The number of DHCPREQUEST messages the server has received.
DHCP DECLINE	The number of DHCPDECLINE messages the server has received.
DHCP RELEASE	The number of DHCPRELEASE messages the server has received.
DHCP INFORM	The number of DHCPINFORM messages the server has received.

Message Sent:

Message	Definition
DHCP OFFER	The number of DHCPOFFER messages the server sent.
DHCP ACK	The number of DHCPACK messages the server sent.
DHCP NACK	The number of DHCPNACK messages the server sent.

4.11.0.29 show ip dhcp conflict

This command displays address conflicts logged by the DHCP Server. If no IP address is specified, all the conflicting addresses are displayed.

Format `show ip dhcp conflict [`*`ip-address`*`]`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
IP address	The IP address of the host as recorded on the DHCP server.
Detection Method	The manner in which the IP address of the hosts were found on the DHCP Server.
Detection time	The time when the conflict was found.

4.12 DNS Client Commands

These commands are used in the Domain Name System (DNS), an Internet directory service. DNS is how domain names are translated into IP addresses. When enabled, the DNS client provides a hostname lookup service to other components of EFOS.

4.12.0.1 ip domain lookup

Use this command to enable the DNS client.

Default enabled

Format `ip domain lookup`

Mode Global Config

4.12.0.1.1 no ip domain lookup

Use this command to disable the DNS client.

Format `no ip domain lookup`

Mode Global Config

4.12.0.2 ip domain name

Use this command to define a default domain name that EFOS software uses to complete unqualified host names (names with a domain name). By default, no default domain name is configured in the system. `name` may not be longer than 255 characters and should not include an initial period. This `name` should be used only when the default domain name list, configured using the `ip domain list command,` is empty.

Default none

Format `ip domain name` *`name`*

Mode Global Config

Example: The CLI command `ip domain name yahoo.com` will configure yahoo.com as a default domain name. For an unqualified hostname xxx, a DNS query is made to find the IP address corresponding to xxx.yahoo.com.

4.12.0.2.1 no ip domain name

Use this command to remove the default domain name configured using the `ip domain name` command.

Format `no ip domain name`

Mode Global Config

4.12.0.3 ip domain list

Use this command to define a list of default domain names to complete unqualified names. By default, the list is empty. Each name must be no more than 256 characters, and should not include an initial period. The default domain name, configured using the `ip domain name` command, is used only when the default domain name list is empty. A maximum of 32 names can be entered in to this list.

Default none

Format `ip domain list` *`name`*

Mode Global Config

4.12.0.3.1 no ip domain list

Use this command to delete a name from a list.

Format `no ip domain list name`

Mode Global Config

4.12.0.4 ip name server

Use this command to configure the available name servers. Up to eight servers can be defined in one command or by using multiple commands. The parameter `server-address` is a valid IPv4 address of the server. The preference of the servers is determined by the order they were entered.

Format `ip name-server server-address1 [server-address2...server-address8]`

Mode Global Config

4.12.0.4.1 no ip name server

Use this command to remove a name server.

Format `no ip name-server [server-address1...server-address8]`

Mode Global Config

4.12.0.5 ip name source-interface

Use this command to specify the physical or logical interface to use as the DNS client source interface. If configured, the address of source Interface is used for all DNS communications between the DNS server and the DNS client. Otherwise there is no change in behavior. If the configured interface is down, the DNS client falls back to its default behavior.

Format `ip name source-interface {slot/port | loopback loopback-id | tunnel tunnel-id | vlan vlan-id}`

Mode Global Config

Parameter	Description
slot/port	Specifies the port to use as the source interface.
loopback-id	Specifies the loopback interface to use as the source interface. The range of the loopback ID is 0 to 7.
tunnel-id	Specifies the tunnel interface to use as the source interface. The range of the tunnel ID is 0 to 7.
vlan-id	Specifies the VLAN to use as the source interface.

4.12.0.5.1 no ip name source-interface

Use this command to reset the DNS source interface to the default settings.

Format `no ip name source-interface`

Mode Global Config

4.12.0.6 ip host

Use this command to define static host name-to-address mapping in the host cache. The parameter `name` is host name and *i*`p address` is the IP address of the host. The hostname can include 1–255 alphanumeric characters, periods, hyphens, underscores, and non-consecutive spaces. Hostnames that include one or more space must be enclosed in quotation marks, for example “lab-pc 45”.

Default none

Format `ip host` *`name ipaddress`*

Mode Global Config

4.12.0.6.1 no ip host

Use this command to remove the name-to-address mapping.

Format `no ip host` *`name`*

Mode Global Config

4.12.0.7 ip domain retry

Use this command to specify the number of times to retry sending Domain Name System (DNS) queries. The parameter `number` indicates the number of times to retry sending a DNS query to the DNS server. This number ranges from 0 to 100.

Default 2

Format `ip domain retry` *`number`*

Mode Global Config

4.12.0.7.1 no ip domain retry

Use this command to return to the default.

Format `no ip domain retry` *`number`*

Mode Global Config

4.12.0.8 ip domain timeout

Use this command to specify the amount of time to wait for a response to a DNS query. The parameter `seconds` specifies the time, in seconds, to wait for a response to a DNS query. The parameter `seconds` ranges from 0 to 3600.

Default 3

Format `ip domain timeout` *`seconds`*

Mode Global Config

4.12.0.8.1 no ip domain timeout

Use this command to return to the default setting.

Format `no ip domain timeout` *`seconds`*

Mode Global Config

4.12.0.9 clear host

Use this command to delete entries from the host name-to-address cache. This command clears the entries from the DNS cache maintained by the software. This command clears IPv4 entries.

Format `clear host {`*`name`* `| all}`
Mode Privileged EXEC

Parameter	Description
name	A particular host entry to remove. The parameter `name` ranges from 1-255 characters.
all	Removes all entries.

4.12.0.10 show hosts

Use this command to display the default domain name, a list of name server hosts, the static and the cached list of host names and addresses. The parameter `name` ranges from 1-255 characters. This command displays IPv4 entries.

Format `show hosts` *`[name]`*
Mode Privileged EXEC
User EXEC

Parameter	Description
Host Name	Domain host name.
Default Domain	Default domain name.
Default Domain List	Default domain list.
Domain Name Lookup	DNS client enabled/disabled.
Number of Retries	Number of time to retry sending Domain Name System (DNS) queries.
Retry Timeout Period	Amount of time to wait for a response to a DNS query.
Name Servers	Configured name servers.

Example: The following shows example CLI display output for the command.

```
(Switching) show hosts

Host name..................... Device
Default domain................ gm.com
Default domain list........... yahoo.com, Stanford.edu, rediff.com
Domain Name lookup............ Enabled
Number of retries............. 5
Retry timeout period.......... 1500
Name servers (Preference order)... 176.16.1.18 176.16.1.19
Configured host name-to-address mapping:

Host                          Addresses
----------------------------- -------------------------------
accounting.gm.com             176.16.8.8

Host             Total   Elapsed     Type      Addresses
---------------- -------- ------    --------     --------------
www.stanford.edu   72      3          IP        171.64.14.203
```

4.13 IP Address Conflict Commands

The commands in this section help troubleshoot IP address conflicts.

4.13.0.1 ip address-conflict-detect run

This command triggers the switch to run active address conflict detection by sending gratuitous ARP packets for IPv4 addresses on the switch.

Format `ip address-conflict-detect run`

Mode
- Global Config
- Virtual Router Config

4.13.0.2 show ip address-conflict

This command displays the status information corresponding to the last detected address conflict.

Format `show ip address-conflict`

Modes Privileged EXEC

Parameter	Definition
Address Conflict Detection Status	Identifies whether the switch has detected an address conflict on any IP address.
Last Conflicting IP Address	The IP Address that was last detected as conflicting on any interface.
Last Conflicting MAC Address	The MAC Address of the conflicting host that was last detected on any interface.
Time Since Conflict Detected	The time in days, hours, minutes and seconds since the last address conflict was detected.

4.13.0.3 clear ip address-conflict-detect

This command clears the detected address conflict status information for the specified virtual router. If no router is specified, the command is executed for the default router.

Format `clear ip address-conflict-detect [vrf` *`vrf-name`*`]`

Modes Privileged EXEC

4.14 Serviceability Packet Tracing Commands

These commands improve the capability of network engineers to diagnose conditions affecting their EFOS product.

CAUTION! The output of **debug** commands can be long and may adversely affect system performance.

4.14.0.1 capture start

Use the command **capture start** to manually start capturing CPU packets for packet trace.

The packet capture operates in three modes:

- capture file
- remote capture
- capture line

The command is not persistent across a reboot cycle.

Format `capture start [{all | receive | transmit}]`
Mode Privileged EXEC

Parameter	Description
all	Capture all traffic.
receive	Capture only received traffic.
transmit	Capture only transmitted traffic.

4.14.0.2 capture stop

Use the command **capture stop** to manually stop capturing CPU packets for packet trace.

Format `capture stop`
Mode Privileged EXEC

4.14.0.3 capture file | remote | line

Use this command to configure file capture options. The command is persistent across a reboot cycle.

Format `capture {file|remote|line}`
Mode Global Config

Parameter	Description
file	In the capture file mode, the captured packets are stored in a file on NVRAM. The maximum file size defaults to 524288 bytes. The switch can transfer the file to a TFTP server via TFTP, SFTP, SCP via CLI, and SNMP. The file is formatted in pcap format, is named cpuPktCapture.pcap, and can be examined using network analyzer tools such as Wireshark® or Ethereal®. Starting a file capture automatically terminates any remote capture sessions and line capturing. After the packet capture is activated, the capture proceeds until the capture file reaches its maximum size, or until the capture is stopped manually using the CLI command **capture stop**.

Parameter	Description
remote	In the remote capture mode, the captured packets are redirected in real time to an external PC running the Wireshark tool for Microsoft® Windows®. A packet capture server runs on the switch side and sends the captured packets via a TCP connection to the Wireshark tool. The remote capture can be enabled or disabled using the CLI. There should be a Windows PC with the Wireshark tool to display the captured file. When using the remote capture mode, the switch does not store any captured data locally on its file system. You can configure the IP port number for connecting Wireshark to the switch. The default port number is 2002. If a firewall is installed between the Wireshark PC and the switch, then these ports must be allowed to pass through the firewall. You must configure the firewall to allow the Wireshark PC to initiate TCP connections to the switch. If the client successfully connects to the switch, the CPU packets are sent to the client PC, then Wireshark receives the packets and displays them. This continues until the session is terminated by either end. Starting a remote capture session automatically terminates the file capture and line capturing.
line	In the capture line mode, the captured packets are saved into the RAM and can be displayed on the CLI. Starting a line capture automatically terminates any remote capture session and capturing into a file. There is a maximum 128 packets of maximum 128 bytes that can be captured and displayed in Line mode.

4.14.0.4 capture remote port

Use this command to configure file capture options. The command is persistent across a reboot cycle. The *id* parameter is a TCP port number from 1024– 49151.

Format `capture remote port` *id*
Mode Global Config

4.14.0.5 capture file size

Use this command to configure file capture options. The command is persistent across a reboot cycle. The *max-file-size* parameter is the maximum size the pcap file can reach, which is 2–512 KB.

Format `capture file size` *max file size*
Mode Global Config

4.14.0.6 capture line wrap

This command enables wrapping of captured packets in line mode when the captured packets reaches full capacity.

Format `capture line wrap`
Mode Global Config

4.14.0.6.1 no capture line wrap

This command disables wrapping of captured packets and configures capture packet to stop when the captured packet capacity is full.

Format `no capture line wrap`
Mode Global Config

4.14.0.7 show capture packets

Use this command to display packets captured and saved to RAM. It is possible to capture and save into RAM, packets that are received or transmitted through the CPU. A maximum 128 packets can be saved into RAM per capturing session. A maximum 128 bytes per packet can be saved into the RAM. If a packet holds more than 128 bytes, only the first 128 bytes are saved; data more than 128 bytes is skipped and cannot be displayed in the CLI.

Capturing packets is stopped automatically when 128 packets are captured and have not yet been displayed during a capture session. Captured packets are not retained after a reload cycle.

Format	`show capture packets`
Mode	Privileged EXEC

4.14.0.8 cpu-traffic direction interface

Use this command to associate CPU filters to an interface or list of interfaces. The interfaces can be a physical or logical LAG. The statistics counters are updated only for the configured interfaces. The traces can also be obtained for the configured interfaces.

NOTE: The offset should consider the VLAN tag headers as the packet to the CPU is always a tagged packet.

Default	None
Format	`cpu-traffic direction {tx|rx|both} interface` *`interface-range`*
Mode	Global Config

4.14.0.8.1 no cpu-traffic direction interface

Use this command to remove all interfaces from the CPU filters.

Format	`no cpu-traffic direction {tx|rx|both} interface` *`interface-range`*
Mode	Global Config

4.14.0.9 cpu-traffic direction match cust-filter

Use this command to configure a custom filter. The statistics and/or traces for configured filters are obtained for the packet matching configured data at the specific offset. If the mask is not specified then the default mask is 0xFF. There can be three different offsets specified as match conditions. Each time a custom filter is configured, the switch overrides the previous configuration.

NOTE: The offset should consider the VLAN tag headers as the packet to the CPU is always a tagged packet.

Default	None
Format	`cpu-traffic direction {tx|rx|both} match cust-filter` *`offset1 data1`* `[mask1` *`mask1`*`]` *`offset2 data2`* `[mask2` *`mask2`*`]` *`offset3 data3`* `[mask3` *`mask3`*`]`
Mode	Global Config

4.14.0.9.1 no cpu-traffic direction match cust-filter

Use this command to remove the configured custom filter.

Format `no cpu-traffic direction {tx|rx|both} match cust-filter` *`offset1 data1`* `[mask1` *`mask1`*`]` *`offset2 data2`* `[mask2` *`mask2`*`]` *`offset3 data3`* `[mask3` *`mask3`*`]`

Mode Global Config

4.14.0.10 cpu-traffic direction match srcip

Use this command to configure the source IP address-specific filter. The statistics and/or the traces for configured filters are obtained for the packet matching configured source IP/Mask.

Default None

Format `cpu-traffic direction {tx|rx|both} match srcip` *`ipaddress`* `[mask` *`mask`*`]`

Mode Global Config

4.14.0.10.1 no cpu-traffic direction match srcip

Use this command to disable the configured source IP address filter.

Format `no cpu-traffic direction {tx|rx|both} match srcip` *`ipaddress`* `[mask` *`mask`*`]`

Mode Global Config

4.14.0.11 cpu-traffic direction match dstip

Use this command to configure the destination IP address-specific filter. The statistics and/or the traces for configured filters are obtained for the packet matching configured destination IP/Mask.

Default None

Format `cpu-traffic direction {tx|rx|both} match dstip` *`ipaddress`* `[mask` *`mask`*`]`

Mode Global Config

4.14.0.11.1 no cpu-traffic direction match dstip

Use this command to disable the configured destination IP address filter.

Format `no cpu-traffic direction {tx|rx|both} match dstip` *`ipaddress`* `[mask` *`mask`*`]`

Mode Global Config

4.14.0.12 cpu-traffic direction match tcp

Use this command to configure the source or destination TCP port-specific filter. The statistics and/or traces for configured filters are obtained for the packet matching configured source/destination TCP port.

Default None

Format `cpu-traffic direction {tx|rx|both} match {srctcp|dsttcp}` *`port`* `[mask` *`mask`*`]`

Mode Global Config

4.14.0.12.1 no cpu-traffic direction match tcp

Use this command to remove the configured source/destination TCP port filter.

Format `no cpu-traffic direction {tx|rx|both} match {srctcp|dsttcp} port [mask mask]`
Mode Global Config

4.14.0.13 cpu-traffic direction match udp

Use this command to configure the source or destination UDP port-specific filter. The statistics and/or traces for configured filters are obtained for the packet matching configured source/destination UDP port.

Default None
Format `cpu-traffic direction {tx|rx|both} match {srcudp|dstudp} port [mask mask]`
Mode Global Config

4.14.0.13.1 no cpu-traffic direction match udp

Use this command to remove the configured source/destination UDP port filter.

Format `no cpu-traffic direction {tx|rx|both} match {srcudp|dstudp} port [mask mask]`
Mode Global Config

4.14.0.14 cpu-traffic mode

Use this command to configure CPU-traffic mode. The packets in the RX/TX direction are matched when the mode is enabled.

Default Disabled
Format `cpu-traffic mode`
Mode Global Config

4.14.0.14.1 no cpu-traffic mode

Use this command to disable CPU-traffic mode.

Format `no cpu-traffic mode`
Mode Global Config

4.14.0.15 cpu-traffic trace

Use this command to configure CPU packet tracing. The packet can be received by multiple components. If the feature is enabled and tracing configured, the packets are traced per the defined filter. If dump-pkt is enabled, the first 64 bytes of the packet are displayed along with the trace statistics.

Default Disabled
Format `cpu-traffic trace {dump-pkt}`
Mode Global Config

4.14.0.15.1 no cpu-traffic trace

Use this command to disable CPU packet tracing and dump-pkt (if configured).

Format `no cpu-traffic trace {dump-pkt}`
Mode Global Config

4.14.0.16 show cpu-traffic

Use this command to display the current configuration parameters.

Default None
Format `show cpu-traffic`
Mode Privileged EXEC

Example:

```
(Routing) #show cpu-traffic

Admin Mode..................................... Disable
Packet Trace................................... Disable
Packet Dump.................................... Disable

Direction TX:
Filter Options................................. N/A
Interface...................................... N/A
Src TCP parameters............................. 0 0
Dst TCP parameters............................. 0 0
Src UDP parameters............................. 0 0
Dst UDP parameters............................. 0 0
Src IP parameters.............................. 0.0.0.0 0.0.0.0
Dst IP parameters.............................. 0.0.0.0 0.0.0.0
Src MAC parameters............................. 00:00:00:00:00:00 00:00:00:00:00:00
Dst MAC parameters............................. 00:00:00:00:00:00 00:00:00:00:00:00
Custom filter parameters1...................... Offset=0x0 Value=0x0 Mask=0x0
Custom filter parameters2...................... Offset=0x0 Value=0x0 Mask=0x0
Custom filter parameters3...................... Offset=0x0 Value=0x0 Mask=0x0

Direction RX:
Filter Options................................. N/A
Interface...................................... N/A
Src TCP parameters............................. 0 0
Dst TCP parameters............................. 0 0
Src UDP parameters............................. 0 0
Dst UDP parameters............................. 0 0
Src IP parameters.............................. 0.0.0.0 0.0.0.0
Dst IP parameters.............................. 0.0.0.0 0.0.0.0
Src MAC parameters............................. 00:00:00:00:00:00 00:00:00:00:00:00
Dst MAC parameters............................. 00:00:00:00:00:00 00:00:00:00:00:00
Custom filter parameters1...................... Offset=0x0 Value=0x0 Mask=0x0
Custom filter parameters2...................... Offset=0x0 Value=0x0 Mask=0x0
Custom filter parameters3...................... Offset=0x0 Value=0x0 Mask=0x0
```

4.14.0.17 show cpu-traffic interface

Use this command to display per interface statistics for configured filters. The statistics can be displayed for a specific filter (e.g., stp, udld, arp etc). If no filter is specified, statistics are displayed for all configured filters. Similarly, source/destination IP, TCP, UDP or MAC along with custom filter can be used as command option to get statistics.

Default None

Format `show cpu-traffic interface {all | slot/port | cpu } filter`

Mode Privileged EXEC

4.14.0.18 show cpu-traffic summary

Use this command to display summary statistics for configured filters for all interfaces.

Default None

Format `show cpu-traffic summary`

Mode Privileged EXEC

Example:

```
(Routing) #show cpu-traffic summary

Filter       Received   Transmitted
------------ ---------- -----------
STP          0          0
LACPDU       0          0
ARP          0          0
UDLD         0          0
LLDP         0          0
IP           0          0
OSPF         0          0
BGP          0          0
DHCP         0          0
BCAST        0          0
MCAST        0          0
UCAST        0          0
SRCIP        0          0
DSTIP        0          0
SRCMAC       0          0
DSTMAC       0          0
CUSTOM       0          0
SRCTCP       0          0
DSTTCP       0          0
SRCUDP       0          0
```

4.14.0.19 show cpu-traffic trace

Use this command to display traced information. The trace information can be displayed either for all available packets or for specific filter (e.g., stp, udld, arp etc). Similarly, source/destination IP or MAC along with custom filter can be used as command option to get specific traces from history. If enabled, packet dump information is displayed along with packet trace statistics. By default, packet dump buffer size is set to store first 64 bytes of packet.

Default None

Format `show cpu-traffic trace` *`filter`*
Mode Privileged EXEC

Example:

```
(Routing) #show cpu-traffic summary
Packet #1: IP; DHCP; UCAST; SRCMAC=00:10:10:10:10:10;
<08:06:10> Sysnet received in sysNetNotifyPduReceive()
<08:06:10> Packet delivered to IP via ipMapRecvIP()
<08:06:10> Freed
0000 00 10 18 82 18 b3 00 10 10 10 10 10 81 00 00 01    ................
0010 08 00 45 10 01 21 00 00 00 00 40 11 79 bd 00 00    ..E..!....@.y...
0020 00 00 ff ff ff ff 00 44 00 43 01 0d 48 10 03 01    .......D.C..H...
0030 06 00 18 85 4a 83 00 00 80 00 00 00 00 00 00 00    ....J...........
```

4.14.0.20 clear cpu-traffic

Use this command to clear cpu-traffic statistics or trace information on all interfaces.

Default None
Format `clear cpu-traffic {counters | traces}`
Mode Global Config

4.14.0.21 debug aaa accounting

This command is useful to debug accounting configuration and functionality in User Manager.

Format `debug aaa accounting`
Mode Privileged EXEC

4.14.0.21.1 no debug aaa accounting

Use this command to turn off debugging of User Manager accounting functionality.

Format `no debug aaa accounting`
Mode Privileged EXEC

4.14.0.22 debug aaa authorization commands

Use this command to enable the tracing for AAA in User Manager. This is useful to debug authorization configuration and functionality in the User Manager.

Format `debug aaa authorization commands`
Mode Privileged EXEC

4.14.0.22.1 no debug aaa authorization

Use this command to turn off debugging of the User Manager authorization functionality.

Format `no debug aaa authorization commands`

Mode Privileged EXEC

Example: The following is an example of the command.

```
(Routing) #debug aaa authorization commands
User Mgr authorization debug is enabled.

(Routing) #no debug aaa authorization commands

User Mgr authorization debug is Disabled.
```

4.14.0.23 debug arp

Use this command to enable ARP debug protocol messages. Optionally, a virtual router can be specified in which to execute the command.

Default disabled

Format `debug arp [vrf` *`vrf-name`*`]`

Mode Privileged EXEC

4.14.0.23.1 no debug arp

Use this command to disable ARP debug protocol messages.

Format `no debug arp`

Mode Privileged EXEC

4.14.0.24 debug auto-voip

Use this command to enable Auto VOIP debug messages. Use the optional parameters to trace H323, SCCP, or SIP packets respectively.

Default disabled

Format `debug auto-voip [H323|SCCP|SIP|oui]`

Mode Privileged EXEC

4.14.0.24.1 no debug auto-voip

Use this command to disable Auto VOIP debug messages.

Format `no debug auto-voip`

Mode Privileged EXEC

4.14.0.25 debug clear

This command disables all previously enabled “debug” traces.

Default disabled

Format `debug clear`

Mode Privileged EXEC

4.14.0.26 debug console

This command enables the display of “debug” trace output on the login session in which it is executed. Debug console display must be enabled in order to view any trace output. The output of debug trace commands will appear on all login sessions for which debug console has been enabled. The configuration of this command remains in effect for the life of the login session. The effect of this command is not persistent across resets.

NOTE: The debug console command is used to direct debug data to a login session. The severity level of messages appearing in the session is still decided by the console logging severity filter specified with the `logging console` command.

Default disabled

Format `debug console`

Mode Privileged EXEC

4.14.0.26.1 no debug console

This command disables the display of “debug” trace output on the login session in which it is executed.

Format `no debug console`

Mode Privileged EXEC

4.14.0.27 debug crashlog

Use this command to view information contained in the crash log file that the system maintains when it experiences an unexpected reset. The crash log file contains the following information:

- Call stack information in both primitive and verbose forms
- Log Status
- Buffered logging
- Event logging
- Persistent logging
- System Information (output of sysapiMbufDump)
- Message Queue Debug Information
- Memory Debug Information
- Memory Debug Status
- OS Information (output of osapiShowTasks)
- /proc information (meminfo, cpuinfo, interrupts, version and net/sockstat)

Default disabled

Format `debug crashlog {[kernel] crashlog-number [upload url] | proc | verbose | deleteall}`

Mode Privileged EXEC

Parameter	Description
kernel	View the crash log file for the kernel

Parameter	Description
crashlog-number	Specifies the file number to view. The system maintains up to four copies, and the valid range is 1–4."deb
upload *url*	To upload the crash log (or crash dump) to a TFTP server, use the `upload` keyword and specify the required TFTP server information.
proc	View the application process crashlog.
verbose	Enable the verbose crashlog.
deleteall	Delete all crash log files on the system.
data	Crash log data recorder.
crashdump-number	Specifies the crash dump number to view. The valid range is 0–2.
download *url*	To download a crash dump to the switch, use the `download` keyword and specify the required TFTP server information.
component-id	The ID of the component that caused the crash.
item-number	The item number.
additional-parameter	Additional parameters to include.

4.14.0.28 debug crashlog kernel

Use this command to display the dmesg log from the specified kdump slot.

Default disabled

Format `debug crashlog kernel` *`crashlog-number`*

Mode Privileged EXEC

4.14.0.29 debug crashlog kernel upload

Use this command to upload the specified kernel dump to the TFTP server.

Default disabled

Format `debug crashlog kernel` *`crashlog-number`* `upload` *`tftpaddress`*

Mode Privileged EXEC

4.14.0.30 debug dcbx packet

Use this command to enable debug tracing for DCBX packets that are transmitted or received.

Default disabled

Format `debug dcbx packet {receive | transmit}`

Mode Privileged EXEC

4.14.0.31 debug debug-config

Use this command to download or upload the debug-config.ini file. The debug-config. ini file executes CLI commands (including devshell and drivshell commands) on specific predefined events. The debug config file is created manually and downloaded to the switch.

Default disabled

Format `debug debug-config {download <`*`url`*`> | upload <`*`url`*`>}`

Mode Privileged EXEC

4.14.0.32 debug dhcp packet

This command displays “debug” information about DHCPv4 client activities and traces DHCPv4 packets to and from the local DHCPv4 client.

Default disabled
Format `debug dhcp packet [transmit | receive]`
Mode Privileged EXEC

4.14.0.32.1 no debug dhcp

This command disables the display of “debug” trace output for DHCPv4 client activity.

Format `no debug dhcp packet [transmit | receive]`
Mode Privileged EXEC

4.14.0.33 debug dot1x packet

Use this command to enable dot1x packet debug trace.

Default disabled
Format `debug dot1x [transmit | receive]`
Mode Privileged EXEC

4.14.0.33.1 no debug dot1x packet

Use this command to disable dot1x packet debug trace.

Format `no debug dot1x [transmit | receive]`
Mode Privileged EXEC

4.14.0.34 debug igmpsnooping packet

This command enables tracing of IGMP Snooping packets received and transmitted by the switch.

Default disabled
Format `debug igmpsnooping packet [transmit | receive]`
Mode Privileged EXEC

4.14.0.34.1 no debug igmpsnooping packet

This command disables tracing of IGMP Snooping packets.

Format `no debug igmpsnooping packet`
Mode Privileged EXEC

4.14.0.35 debug igmpsnooping packet transmit

This command enables tracing of IGMP Snooping packets transmitted by the switch. Snooping should be enabled on the device and the interface in order to monitor packets for a particular interface.

Default disabled

Format `debug igmpsnooping packet transmit`

Mode Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 02:45:06 192.168.17.29-1 IGMPSNOOP[185429992]: igmp_snooping_debug.c(116) 908 % Pkt TX -
Intf: 0/20(20), Vlan_Id:1 Src_Mac: 00:03:0e:00:00:00 Dest_Mac: 01:00:5e:00:00:01 Src_IP: 9.1.1.1
Dest_IP: 225.0.0.1 Type: V2_Membership_Report Group: 225.0.0.1
```

The following parameters are displayed in the trace message:

Parameter	Definition
TX	A packet transmitted by the device.
Intf	The interface that the packet went out on. Format used is *slot/port* (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.
Src_Mac	Source MAC address of the packet.
Dest_Mac	Destination multicast MAC address of the packet.
Src_IP	The source IP address in the IP header in the packet.
Dest_IP	The destination multicast IP address in the packet.
Type	The type of IGMP packet. Type can be one of the following: ■ Membership Query – IGMP Membership Query ■ V1_Membership_Report – IGMP Version 1 Membership Report ■ V2_Membership_Report – IGMP Version 2 Membership Report ■ V3_Membership_Report – IGMP Version 3 Membership Report ■ V2_Leave_Group – IGMP Version 2 Leave Group
Group	Multicast group address in the IGMP header.

4.14.0.35.1 no debug igmpsnooping transmit

This command disables tracing of transmitted IGMP snooping packets.

Format `no debug igmpsnooping transmit`

Mode Privileged EXEC

4.14.0.36 debug igmpsnooping packet receive

This command enables tracing of IGMP Snooping packets received by the switch. Snooping should be enabled on the device and the interface in order to monitor packets for a particular interface.

Default disabled

Format `debug igmpsnooping packet receive`

Mode Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 02:45:06 192.168.17.29-1 IGMPSNOOP[185429992]: igmp_snooping_debug.c(116) 908 % Pkt RX -
Intf: 0/20(20), Vlan_Id:1 Src_Mac: 00:03:0e:00:00:10 Dest_Mac: 01:00:5e:00:00:05 Src_IP: 11.1.1.1
Dest_IP: 225.0.0.5 Type: Membership_Query Group: 225.0.0.5
```

The following parameters are displayed in the trace message:

Parameter	Definition
RX	A packet received by the device.
Intf	The interface that the packet went out on. Format used is slot/port (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.
Src_Mac	Source MAC address of the packet.
Dest_Mac	Destination multicast MAC address of the packet.
Src_IP	The source IP address in the ip header in the packet.
Dest_IP	The destination multicast ip address in the packet.
Type	The type of IGMP packet. Type can be one of the following: ■ Membership_Query – IGMP Membership Query ■ V1_Membership_Report – IGMP Version 1 Membership Report ■ V2_Membership_Report – IGMP Version 2 Membership Report ■ V3_Membership_Report – IGMP Version 3 Membership Report ■ V2_Leave_Group – IGMP Version 2 Leave Group
Group	Multicast group address in the IGMP header.

4.14.0.36.1 no debug igmpsnooping receive

This command disables tracing of received IGMP Snooping packets.

Format `no debug igmpsnooping receive`
Mode Privileged EXEC

4.14.0.37 debug ip acl

Use this command to enable debug of IP Protocol packets matching the ACL criteria.

Default disabled
Format `debug ip acl` *`acl Number`*
Mode Privileged EXEC

4.14.0.37.1 no debug ip acl

Use this command to disable debug of IP Protocol packets matching the ACL criteria.

Format `no debug ip acl acl Number`
Mode Privileged EXEC

4.14.0.38 debug ip bgp

To enable debug tracing of BGP events, use the **debug ip bgp** command in privileged EXEC mode. Debug messages are sent to the system log at the DEBUG severity level. To print them on the console, enable console logging at the DEBUG level (**logging console debug** command) - see Section 4.6.0.4, logging console.

The debug options enabled for a specific peer are the union of the options enabled globally and the options enabled specifically for the peer.

Enabling one of the packet type options enables packet tracing in both the inbound and outbound directions.

Default No debug tracing is enabled by default

Format `debug ip bgp [vrf vrf-name] {ipv4-address|ipv6-address} [ events | in | interface {slot/port | vlan 1-4093} | keepalives | notification | open | out | refresh | updates ]`

Mode Privileged EXEC

Parameter	Description
peer-address	(Optional) The IPv4 address of a BGP peer. Debug traces are enabled for a specific peer when this option is specified. The command can be issued multiple times to enable simultaneous tracing for multiple peers.
events	(Optional) Trace adjacency state events.
keepalives	(Optional) Trace transmit and receive of KEEPALIVE packets.
notification	(Optional) Trace transmit and receive of NOTIFICATION packets.
open	(Optional) Trace transmit and receive of OPEN packets.
refresh	(Optional) Traces transmit and receive of ROUTE REFRESH packets.
updates	(Optional) Traces transmit and receive of UPDATE packets.

4.14.0.38.1 no debug bgp

Use this command to disable debug tracing of BGP events.

Format `no debug ip bgp [peer-address|events|keepalives|notification|open|refresh|updates]`

Mode Privileged EXEC

4.14.0.39 debug ipv6 dhcp

This command displays “debug” information about DHCPv6 client activities and traces DHCPv6 packets to and from the local DHCPv6 client.

Default disabled

Format `debug ipv6 dhcp`

Mode Privileged EXEC

4.14.0.39.1 no debug ipv6 dhcp

This command disables the display of “debug” trace output for DHCPv6 client activity.

Format `no debug ipv6 dhcp`

Mode Privileged EXEC

4.14.0.40 debug ipv6 ospfv3 packet

Use this command to enable IPv6 OSPFv3 packet debug trace.

Default disabled

Format `debug ipv6 ospfv3 packet`
Mode Privileged EXEC

4.14.0.40.1 no debug ipv6 ospfv3 packet

Use this command to disable tracing of IPv6 OSPFv3 packets.

Format `no debug ipv6 ospfv3 packet`
Mode Privileged EXEC

4.14.0.41 debug ip vrrp

Use this command to enable debug tracing of VRRP events. Debug messages are sent to the system log at the DEBUG severity level. To print them on the console, enable console logging at the DEBUG level (logging console debug).

The debug options enabled for a specific peer are the union of the options enabled globally and the options enabled specifically for the peer. Enabling one of the packet type options enables packet tracing in both the inbound and outbound directions.

Default Enabled
Format `debug ip vrrp`
Mode Privileged Exec

4.14.0.41.1 no debug ip vrrp

Use this command to disable debug tracing of VRRP events.

Format `no debug ip vrrp`
Mode Privileged Exec

4.14.0.42 debug isdp packet

This command enables tracing of ISDP packets received and/or transmitted by the switch.
Default disabled
Format `debug isdp packet [{transmit | receive}]`
Mode Privileged EXEC

4.14.0.42.1 no debug isdp packet

This command disables tracing of ISDP transmit and/or received packets.

Format `no debug isdp packet [{transmit | receive}]`
Mode Privileged EXEC

4.14.0.43 debug lacp packet

This command enables tracing of LACP packets received and transmitted by the switch.

Default disabled

Format `debug lacp packet`

Mode Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 14:04:51 10.254.24.31-1 DOT3AD[183697744]: dot3ad_debug.c(385) 58 %%
 Pkt TX - Intf: slot/port(1), Type: LACP, Sys: 00:11:88:14:62:e1, State: 0x47, Key:
0x36
```

4.14.0.43.1 no debug lacp packet

This command disables tracing of LACP packets.

Format `no debug lacp packet`

Mode Privileged EXEC

4.14.0.44 debug mldsnooping packet

Use this command to trace MLD snooping packet reception and transmission. **receive** traces only received MLD snooping packets and **transmit** traces only transmitted MLD snooping packets. When neither keyword is used in the command, then all MLD snooping packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Default disabled

Format `debug mldsnooping packet [receive | transmit]`

Mode Privileged EXEC

4.14.0.44.1 no debug mldsnooping packet

Use this command to disable debug tracing of MLD snooping packet reception and transmission.

4.14.0.45 debug ospf packet

This command enables tracing of OSPF packets received and transmitted by the switch or, optionally, a virtual router can be specified.

Default disabled

Format `debug ospf packet [vrf` *`vrf-name`*`]`

Mode Privileged EXEC

Sample outputs of the trace messages are shown below.

```
<15> JAN 02 11:03:31 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(297) 25430 % Pkt RX - Intf:2/0/48 Src
Ip:192.168.50.2 DestIp:224.0.0.5 AreaId:0.0.0.0 Type:HELLO NetMask:255.255.255.0 D
esigRouter:0.0.0.0 Backup:0.0.0.0

<15> JAN 02 11:03:35 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(293) 25431 % Pkt TX - Intf:2/0/48 Src
```

```
Ip:10.50.50.1 DestIp:192.168.50.2 AreaId:0.0.0.0 Type:DB_DSCR Mtu:1500 Options:E
Flags: I/M/MS Seq:126166

<15> JAN 02 11:03:36 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(297) 25434 % Pkt RX - Intf:2/0/48 Src
Ip:192.168.50.2 DestIp:192.168.50.1 AreaId:0.0.0.0 Type:LS_REQ Length: 1500

<15> JAN 02 11:03:36 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(293) 25435 % Pkt TX - Intf:2/0/48 Src
Ip:10.50.50.1 DestIp:192.168.50.2 AreaId:0.0.0.0 Type:LS_UPD Length: 1500

<15> JAN 02 11:03:37 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(293) 25441 % Pkt TX - Intf:2/0/48 Src
Ip:10.50.50.1 DestIp:224.0.0.6 AreaId:0.0.0.0 Type:LS_ACK Length: 1500
```

The following parameters are displayed in the trace message:

Parameter	Definition
TX/RX	TX refers to a packet transmitted by the device. RX refers to packets received by the device.
Intf	The interface that the packet came in or went out on. Format used is slot/port (internal interface number).
SrcIp	The source IP address in the IP header of the packet.
DestIp	The destination IP address in the IP header of the packet.
AreaId	The area ID in the OSPF header of the packet.
Type	Could be one of the following: HELLO – Hello packet DB_DSCR – Database descriptor LS_REQ – LS Request LS_UPD – LS Update LS_ACK – LS Acknowledge

The remaining fields in the trace are specific to the type of OSPF Packet.

HELLO packet field definitions:

Parameter	Definition
Netmask	The netmask in the hello packet.
DesignRouter	Designated Router IP address.
Backup	Backup router IP address.

DB_DSCR packet field definitions:

Field	Definition
MTU	MTU
Options	Options in the OSPF packet.
Flags	Could be one or more of the following: ■ I – Init ■ M – More ■ MS – Master/Slave
Seq	Sequence Number of the DD packet.

LS_REQ packet field definitions.

Field	Definition
Length	Length of packet

LS_UPD packet field definitions.

Field	Definition
Length	Length of packet

LS_ACK packet field definitions.

Field	Definition
Length	Length of packet

4.14.0.45.1 no debug ospf packet

This command disables tracing of OSPF packets.

Format `no debug ospf packet`
Mode Privileged EXEC

4.14.0.46 debug ping packet

This command enables tracing of ICMP echo requests and responses. The command traces pings on the network port/ service port for switching packages. For routing packages, pings are traced on the routing ports as well. If specified, pings can be traced on the virtual router.

Default disabled
Format `debug ping packet [vrf` *`vrf-name`*`]`
Mode Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 00:21:22 192.168.17.29-1 SIM[181040176]: sim_debug.c(128) 20 % Pkt TX - Intf: 0/1(1),
SRC_IP:10.50.50.2, DEST_IP:10.50.50.1, Type:ECHO_REQUEST


<15> JAN 01 00:21:22 192.168.17.29-1 SIM[182813968]: sim_debug.c(82) 21 % Pkt RX - Intf: 0/1(1), S
RC_IP:10.50.50.1, DEST_IP:10.50.50.2, Type:ECHO_REPLY
```

The following parameters are displayed in the trace message:

Parameter	Definition
TX/RX	TX refers to a packet transmitted by the device. RX refers to packets received by the device.
Intf	The interface that the packet came in or went out on. Format used is slot/port (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.
SRC_IP	The source IP address in the IP header in the packet.
DEST_IP	The destination IP address in the IP header in the packet.
Type	Type determines whether or not the ICMP message is a REQUEST or a RESPONSE.

4.14.0.46.1 no debug ping packet

This command disables tracing of ICMP echo requests and responses.

Format	`no debug ping packet`
Mode	Privileged EXEC

4.14.0.47 debug sflow packet

Use this command to enable sFlow debug packet trace.

Default	disabled
Format	`debug sflow packet`
Mode	Privileged EXEC

4.14.0.47.1 no debug sflow packet

Use this command to disable sFlow debug packet trace.

Format	`no debug sflow packet`
Mode	Privileged EXEC

4.14.0.48 debug spanning-tree bpdu

This command enables tracing of spanning tree BPDUs received and transmitted by the switch.

Default	disabled
Format	`debug spanning-tree bpdu`
Mode	Privileged EXEC

4.14.0.48.1 no debug spanning-tree bpdu

This command disables tracing of spanning tree BPDUs.

Format	`no debug spanning-tree bpdu`
Mode	Privileged EXEC

4.14.0.49 debug spanning-tree bpdu receive

This command enables tracing of spanning tree BPDUs received by the switch. Spanning tree should be enabled on the device and on the interface in order to monitor packets for a particular interface.

Default	disabled
Format	`debug spanning-tree bpdu receive`
Mode	Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 01:02:04 192.168.17.29-1 DOT1S[191096896]: dot1s_debug.c(1249) 101 % Pkt RX - Intf: 0/
9(9), Source_Mac: 00:11:88:4e:c2:10 Version: 3, Root Mac: 00:11:88:4e:c2:00, Root Priority: 0x8000
Path Cost: 0
```

The following parameters are displayed in the trace message:

Parameter	Definition
RX	A packet received by the device.
Intf	The interface that the packet came in on. Format used is unit/port/slot (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.
Source_Mac	Source MAC address of the packet.
Version	Spanning tree protocol version (0-3). 0 refers to STP, 2 RSTP and 3 MSTP.
Root_Mac	MAC address of the CIST root bridge.
Root_Priority	Priority of the CIST root bridge. The value is between 0 and 61440. It is displayed in hex in multiples of 4096.
Path_Cost	External root path cost component of the BPDU.

4.14.0.49.1 no debug spanning-tree bpdu receive

This command disables tracing of received spanning tree BPDUs.

Format `no debug spanning-tree bpdu receive`

Mode Privileged EXEC

4.14.0.50 debug spanning-tree bpdu transmit

This command enables tracing of spanning tree BPDUs transmitted by the switch. Spanning tree should be enabled on the device and on the interface in order to monitor packets on a particular interface.

Default disabled

Format `debug spanning-tree bpdu transmit`

Mode Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 01:02:04 192.168.17.29-1 DOT1S[191096896]: dot1s_debug.c(1249) 101 % Pkt TX - Intf: 0/
7(7), Source_Mac: 00:11:88:4e:c2:00 Version: 3, Root_Mac: 00:11:88:4e:c2:00, Root_Priority: 0x8000
Path_Cost: 0
```

The following parameters are displayed in the trace message:

Parameter	Definition
TX	A packet transmitted by the device.
Intf	The interface that the packet went out on. Format used is unit/port/slot (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.
Source_Mac	Source MAC address of the packet.
Version	Spanning tree protocol version (0-3). 0 refers to STP, 2 RSTP and 3 MSTP.
Root_Mac	MAC address of the CIST root bridge.
Root_Priority	Priority of the CIST root bridge. The value is between 0 and 61440. It is displayed in hex in multiples of 4096.
Path_Cost	External root path cost component of the BPDU.

4.14.0.50.1 no debug spanning-tree bpdu transmit

This command disables tracing of transmitted spanning tree BPDUs.

Format `no debug spanning-tree bpdu transmit`
Mode Privileged EXEC

4.14.0.51 debug tacacs

Use the `debug tacacs packet` command to turn on TACACS+ debugging.

Format `debug tacacs {packet [receive | transmit] | accounting | authentication}`
Mode Global Config

Parameter	Description
packet receive	Turn on TACACS+ receive packet debugs.
packet transmit	Turn on TACACS+ transmit packet debugs.
accounting	Turn on TACACS+ authentication debugging.
authentication	Turn on TACACS+ authorization debugging.

4.14.0.52 debug telnetd start

Use this command to start the debug telnet daemon. The debug telnet daemon gives access to a Linux shell prompt. The telnet user ID is “root”. If the telnet daemon is already running when this command is issued, the command stops and restarts the telnet daemon.

Format `debug telnetd start [password][port]`
Mode Privileged EXEC

Parameter	Description
password	The optional telnet password. If no password is specified, the default password lvl7dbg is used.
port	The optional telnet port number. If no telnet port is specified, the default port 2323 is used.

4.14.0.53 debug telnetd stop

Use this command to stop the telnet daemon previously started by the Section 4.14.0.52, debug telnetd start command. If the daemon is not running when this command is issued, the command has no effect.

Format `debug telnetd stop`
Mode Privileged EXEC

4.14.0.54 debug transfer

This command enables debugging for file transfers.

Format `debug transfer`

Mode Privileged EXEC

4.14.0.54.1 no debug transfer

This command disables debugging for file transfers.

Format `no debug transfer`
Mode Privileged EXEC

4.14.0.55 debug udld events

This command enables debugging for the UDLD events.

Default `Disabled`
Format `debug udld events`
Mode Privileged EXEC

4.14.0.56 debug udld packet receive

This command enables debugging on the received UDLD PDUs.

Default `Disabled`
Format `debug udld packet receive`
Mode Privileged EXEC

4.14.0.57 debug udld packet transmit

This command enables debugging on the transmitted UDLD PDUs.

Default `Disabled`
Format `debug udld packet transmit`
Mode Privileged EXEC

4.14.0.58 show debugging

Use the `show debugging` command to display enabled packet tracing configurations.

Format `show debugging`
Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing)# debug arp
Arp packet tracing enabled.

(Routing)# show debugging
Arp packet tracing enabled.\
```

4.14.0.59 exception core-file

Use this command to configure a prefix for a core-file name. The core file name is generated with the prefix as follows:

If `hostname` is selected:
`file-name-prefix_hostname_Time_Stamp``.bin`

If `hostname` is not selected:
`file-name-prefix_MAC_Address_Time_Stamp``.bin`

If `hostname` is configured the core file name takes the `hostname`, otherwise the core-file names uses the MAC address when generating a core dump file. The prefix length is 15 characters.

NOTE: This command is only available on selected Linux-based platforms.

Default	Core
Format	`exception core-file {`*`file-name-prefix`* `| [hostname] | [time-stamp]}`
Mode	Global Config

4.14.0.59.1 no exception core-file

Use this command to reset the exception core file prefix configuration to its factory default value. The hostname and time-stamp are disabled.

NOTE: This command is only available on selected Linux-based platforms.

Default	Core
Format	`no exception core-file`
Mode	Global Config

4.14.0.60 exception dump active-port

NOTE: This command is only available on selected Linux- based platforms.

This command specifies the interface enabled for the core dump. It is the only port used to upload the core dump.

Default	None
Format	`exception dump active-port` *`slot/port`*
Mode	Global Config

4.14.0.60.1 no exception dump active-port

This command resets the interface enabled for the core dump to the default.

Default	None
Format	`no exception dump active-port`
Mode	Global Config

4.14.0.61 exception dump filepath

Use this command to configure a file-path to dump core file to a TFTP or FTP server, NFS mount or USB device subdirectory.

NOTE: This command is only available on selected Linux-based platforms.

Default	None
Format	`exception dump filepath` *`dir`*
Mode	Global Config

4.14.0.61.1 no exception dump filepath

Use this command to reset the exception dump filepath configuration to its factory default value.

NOTE: This command is only available on selected Linux-based platforms.

Default	None
Format	`exception dump  filepath`
Mode	Global Config

4.14.0.62 exception dump nfs

Use this command to configure an NFS mount point in order to dump core file to the NFS file system.

NOTE: This command is only available on selected Linux-based platforms.

Default	None
Format	`exception dump nfs` *`ip-address/dir`*
Mode	Global Config

4.14.0.62.1 no exception dump nfs

Use this command to reset the exception dump NFS mount point configuration to its factory default value.

NOTE: This command is only available on selected Linux-based platforms.

Default	None
Format	`no exception dump nfs`
Mode	Global Config

4.14.0.63 exception dump tftp-server

Use this command to configure the IP address of a remote TFTP server in order to dump core files to an external server.

NOTE: This command is only available on selected Linux-based platforms.

Default	None
Format	`exception dump tftp-server {`*`ip-address`*`}`
Mode	Global Config

4.14.0.63.1 no exception dump tftp-server

Use this command to reset the exception dump remote server configuration to its factory default value.

NOTE: This command is only available on selected Linux-based platforms.

Default	None
Format	`no exception dump tftp-server`
Mode	Global Config

4.14.0.64 exception kernel-dump

Use this command to enable kernel crash core dump (kdump) functionality. This command requires reboot if the command was not enabled since the last reboot.

Default	None
Format	`exception kernel-dump`
Mode	Global Config

4.14.0.64.1 no exception kernel-dump

Use this command to disable kernel crash core dump (kdump) functionality. If a crash log number is specified, the specified slot is deleted.

Default	None
Format	`no exception kernel-dump` *`crashlog-number`*
Mode	Global Config

4.14.0.65 exception kernel-dump path

Use this command to set the path where the kernel crash core dump (kdump) entries are stored.

Default	None
Format	`exception kernel-dump path` *`path`*
Mode	Global Config

4.14.0.65.1 no exception kernel-dump path

Use this command to return the path where the kernel crash core dump (kdump) entries are stored to the default value.

Default	None
Format	`no exception kernel-dump path`
Mode	Global Config

4.14.0.66 exception protocol

Use this command to specify the protocol used to store the core dump file.

NOTE: This command is only available on selected Linux-based platforms.

Default	None
Format	`exception protocol {nfs | tftp | ftp | local | usb | none}`
Mode	Global Config

4.14.0.66.1 no exception protocol

Use this command to reset the exception protocol configuration to its factory default value.

NOTE: This command is only available on selected Linux-based platforms.

4.14.0.67 exception switch-chip-register

This command enables or disables the switch-chip-register dump in case of an exception. The switch-chip-register dump is taken only for a master unit and not for member units.

NOTE: This command is only available on selected Linux-based platforms.

Default	Disable
Format	`exception switch-chip-register {enable | disable}`
Mode	Global Config

4.14.0.68 exception dump ftp-server

This command configures the IP address of remote FTP server to dump core files to an external server. If the username and password are not configured, the switch uses anonymous FTP. (The FTP server should be configured to accept anonymous FTP.)

Default	None
Format	`exception dump ftp-server` ***`ip-address`*** `[{username` ***`user-name`*** `password` ***`password`***`}]`
Mode	Global Config

4.14.0.68.1 no exception dump ftp-server

This command resets exception dump remote FTP server configuration to its factory default value. This command also resets the FTP username and password to empty string.

Default	None
Format	`no exception dump ftp-server`
Mode	Global Config

4.14.0.69 exception dump compression

This command enables compression mode.

Default	Enabled
Format	`exception dump compression`
Mode	Global Config

4.14.0.69.1 no exception dump compression

This command disables compression mode.

Default	None
Format	`no exception compression`
Mode	Global Config

4.14.0.70 exception nmi

This command enables or disables taking core dump in case of NMI occurs.

Default	Disable
Format	`exception nmi {enable | disable}`
Mode	Global Config

4.14.0.71 show exception kernel-dump

Use this command to display the current kernel dump settings and slots available to view.

Format	`show exception kernel-dump`
Mode	Privileged Exec

4.14.0.72 show exception kernel-dump list

Use this command to display the currently captured dumps.

Format	`show exception kernel-dump list`
Mode	Privileged Exec

4.14.0.73 show exception kernel-dump log

Use this command to display the dmesg log from a specified kdump slot.

Format	`show exception kernel-dump log` *`crashlog-number`*
Mode	Privileged Exec

4.14.0.74 mbuf

Use this command to configure memory buffer (MBUF) threshold limits and generate notifications when MBUF limits have been reached.

Format	`mbuf {falling-threshold | rising threshold | severity}`

Mode Global Config

Field	Description
Rising Threshold	The percentage of the memory buffer resources that, when exceeded for the configured rising interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).
Falling Threshold	The percentage of memory buffer resources that, when usage falls below this level for the configured interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).
Severity	The severity level at which Mbuf logs messages. The range is 1 to 7. The default is 5 (L7_LOG_SEVERITY_NOTICE).

4.14.0.75 write core

Use the *write core* command to generate a core dump file on demand. The `write core test` command is helpful when testing the core dump setup. For example, if the TFTP protocol is configured, `write core test` communicates with the TFTP server and informs the user if the TFTP server can be contacted. Similarly, if protocol is configured as `nfs`, this command mounts and unmounts the file system and informs the user of the status.

NOTE: `write core` reloads the switch which is useful when the device malfunctions, but has not crashed.

For the `write core test` command, the destination file name is used for the TFTP test. Optionally, you can specify the destination file name when the protocol is configured as TFTP.

NOTE: This command is only available on selected Linux-based platforms.

Default None

Format `write core [test [`*`dest_file_name`*`]]`

Mode Privileged EXEC

4.14.0.76 debug exception

The command displays core dump features support.

Default None

Format `debug exception`

Mode Privileged EXEC

4.14.0.77 show exception

Use this command to display the configuration parameters for generating a core dump file.

NOTE: This command is only available on selected Linux-based platforms.

Default None

Format `show exception`

Mode Privileged EXEC

Example: The following shows an example of this command.

```
show exception
```

```
Coredump file name                core
Coredump filename uses hostname   False
Coredump filename uses time-stamp TRUE
TFTP Server Address               TFTP server configuration
FTP Server IP                     FTP server configuration
FTP user name                     FTP user name
FTP password                      FTP password
NFS Mount point                   NFS mount point configuration
File path                         Remote file path
Core File name prefix             Core file prefix configuration.
Hostname                         Core file name contains hostname if enabled.
Timestamp                         Core file name contains timestamp if enabled.
Switch Chip Register Dump         Switch chip register dump configuration
Compression mode                  TRUE/FALSE
Active network port               0/28
```

4.14.0.78 show exception core-dump-file

This command displays core dump files existing on the local file system.

Default None

Format `show exception core-dump-file`

Mode Privileged EXEC, Config Mode

4.14.0.79 show exception log

This command displays core dump traces on the local file system.

Default None

Format `show exception log [previous]`

Mode Privileged EXEC, Config Mode

4.14.0.80 show mbuf total

Use this command to display the memory buffer (MBUF) Utilization Monitoring parameters.

Format `show mbuf total`

Mode Privileged EXEC

Field	Description
Rising Threshold	The percentage of the memory buffer resources that, when exceeded for the configured rising interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).
Falling Threshold	The percentage of memory buffer resources that, when usage falls below this level for the configured interval, triggers a notification. The range is 1 to 100. The default is 0 (disabled).
Severity	The severity level.

4.14.0.81 show msg-queue

Use this command to display the message queues.

Default	None
Format	`show msg-queue`
Mode	Privileged EXEC mode

4.14.0.82 debug packet-trace

Use this command to enable traces for the packet trace feature.

Default	None
Format	`debug packet-trace`
Mode	Privileged Exec

4.14.0.83 packet-trace eth

Use this command to specify the ethernet packet fields for a packets for which a trace profile is required. If the optional vlan parameter is not specified, the PVID/internal VLAN associated with the ingress port (specified in the show packet-trace command) is used in the VLAN tag.

Default	None
Format	`packet-trace eth src-mac` ***`src-mac`*** `dst-mac` ***`dst-mac`*** `vlan` ***`vlan`***
Mode	Privileged Exec

4.14.0.84 packet-trace ipv4

Use this command to specify the IPv4 packet header fields.

Default	None
Format	`packet-trace ipv4 src-ip` ***`src-ip`*** `dst-ip` ***`dst-ip`*** `tos` ***`tos`***
Mode	Privileged Exec

4.14.0.85 packet-trace ipv6

Use this command to specify the IPv6 packet header fields.

Default	None
Format	`packet-trace ipv6 src-ip` ***`src-ip`*** `dst-ip` ***`dst-ip`*** `tos` ***`tos`***
Mode	Privileged Exec

4.14.0.86 packet-trace l4

Use this command to specify TCP packet fields.

Default	None
Format	`packet-trace l4 src-port` ***`src-port`*** `dst-port` ***`dst-port`***
Mode	Privileged Exec

4.14.0.87 show packet-trace ecmp

Use this command for getting a summary (link utilization percentage) for all complete packets present in the PCAP file (uploaded onto the system using the copy command).

Default None

Format `show packet-trace ecmp` ***`prefix/prefix-length`*** `port` ***`slot/port`*** `pcap summary`

Mode Privileged Exec

4.14.0.88 show packet-trace lag

Use this command for getting a summary (link utilization percentage) for all complete packets present in the PCAP file (uploaded onto the system using the copy command).

Default None

Format `show packet-trace lag` ***`lag-id`*** `port` ***`slot/port`*** `pcap summary`

Mode Privileged Exec

Example:

```
(Routing)#show packet-trace lag 1 port 0/1 pcap summary

LAG   ............................... 3/1
Link State..................................... Up
Admin Mode..................................... Enabled
Type........................................... Static
Port-channel Min-links......................... 1
Load Balance Option............................ 3
(Src/Dest MAC, VLAN, EType, incoming port)

Mbr    Device/       Port      Port
Ports  Timeout       Speed     Active
------ ------------- --------- -------
0/3   actor/long    10G Full  True
        partner/long
0/2   actor/long    10G Full  True
        partner/long

LAG 1 member port link utilization %:
-------------------------------------
Total number of valid packets in pcap file: 20
Member port 0/3 utilization: 20%
Member port 0/4 utilization: 80%
```

4.14.0.89 show packet-trace packet-data

Use this command to dump all the configured packet header fields.

Default By default, all packet fields are set to 0.

Format `show packet-trace trace-data`

Mode Privileged Exec

Example:

```
DUT#show packet-trace packet-data

L2 Header fields:
-----------------------
Src MAC: 00 00 00 0a 0b 0c
Dst MAC: 00 00 00 0d 0e 0f
VLAN: 10

L3 Header fields:
-------------------------
IPv4:
Src IP: 10.0.10.1
Dst IP: 10.0.10.10
TOS: 0

IPv6:
Src IP: 4001::1/8
Dst IP: 5001::1/8
Traffic Class: 0

L4 header fields:
-----------------------
Src Port: 80
Dst Port: 80
```

4.14.0.90 show packet-trace port

Use this command for getting detailed information for the maximum packets in the PCAP file.

Default	None
Format	`show packet-trace port` ***`slot/port`*** `pcap detailed` ***`maxpkts`***
Mode	Privileged Exec

Example:

```
DUT#show packet-trace port 0/1 pcap detailed 5

            Packet fields:
src-Mac      --------------     00:00:00:00:00:0a
dst-mac      --------------     00:00:00:00:00:0b
vlan         --------------     10
src-ip       --------------     10.0.1.10
dst-ip       --------------     10.0.1.20

LAG                Destination member port
---------         ---------------------------------
Lag 1                      0/4


Packet fields:
src-Mac      --------------     00:00:00:00:00:0c
dst-mac      --------------     00:00:00:00:00:0d
vlan         --------------     10
src-ip       --------------     10.0.1.10
dst-ip       --------------     10.0.1.20
```

```
LAG                Destination member port
---------         ---------------------------------
Lag 1                      0/3


Packet fields:
src-Mac      --------------     00:00:00:00:00:0e
dst-mac      --------------     00:00:00:00:00:0f
vlan         --------------     10
src-ip       --------------     10.0.1.10
dst-ip       --------------     10.0.1.20

LAG                Destination member port
---------         ---------------------------------
Lag 1                      0/2

Packet fields:
src-Mac      --------------     00:00:00:00:00:1a
dst-mac      --------------     00:00:00:00:00:1b
vlan         --------------     10
src-ip       --------------     10.0.1.10
dst-ip       --------------     10.0.1.20

LAG                Destination member port
---------         ---------------------------------
Lag 1                      0/4

Packet fields:
src-Mac      --------------     00:00:00:00:00:1c
dst-mac      --------------     00:00:00:00:00:1d
vlan         --------------     10
src-ip       --------------     10.0.1.10
dst-ip       --------------     10.0.1.20

LAG                Destination member port
---------         ---------------------------------
Lag 1                      0/3
```

4.14.0.91 show packet-trace port eth

Use this command to retrieve the trace profile for an ethernet packet created from the configured packet fields. The trace profile indicates if the packet went out on LAG/ECMP route and also the corresponding member/link information.

Default None

Format `show packet-trace port` ***slot/port*** `eth`

Mode Privileged Exec

Example:

```
(Routing)# show packet-trace port 0/1 eth

LAG                Destination member port
---------         ---------------------------------
Lag 1                             0/3
```

```
LAG   ............................... 3/1
Link State..................................... Up
Admin Mode..................................... Enabled
Type........................................... Static
Port-channel Min-links......................... 1
Load Balance Option............................ 3
(Src/Dest MAC, VLAN, EType, incoming port)

Mbr    Device/       Port      Port
Ports  Timeout       Speed     Active
------ ------------- --------- -------
0/3   actor/long    10G Full  True
        partner/long
0/2   actor/long    10G Full  True
        partner/long
```

4.14.0.92 show packet-trace port ipv4

Use this command to retrieve the trace profile for an IPv4 packet created from the configured packet fields. The trace profile indicates if the packet went out on LAG/ECMP route and also the corresponding member/link information. Note that in order to get the trace profile for an IP packet, both the Ethernet and IP packet fields need to be configured.

Default None

Format `show packet-trace port` ***slot/port*** `ipv4`

Mode Privileged Exec

Example:

```
(Routing)# show packet-trace port 0/1 ipv4
ECMP               Egress port            Next Hop IP
-----------      ----------------         -----------------
10.0.0.2/16             0/4                 3.3.3.3

ECMP routes to 10.0.0.2/16:
-------------------------------
via 3.3.3.3 on interface 0/4
via 2.2.2.2 on interface 0/5
```

4.14.0.93 show packet-trace port ipv6

Use this command to retrieve the trace profile for an IPv6 packet created from the configured packet fields. The trace profile indicates if the packet went out on LAG/ECMP route and also the corresponding member/link information. Note that in order to get the trace profile for an IP packet, both the ethernet and IP packet fields need to be configured.

Default None

Format `show packet-trace port` ***slot/port*** `ipv6`

Mode Privileged Exec

Example:

```
(Routing)# show packet-trace port 0/1 udpv6

ECMP               Egress port            Next Hop IP
-----------      ----------------         -----------------
6001::200/64          0/4                   8001::200
```

```
ECMP routes to 6001::200/64:
------------------------------
via 8001::200 on interface 0/32
via 7001::200 on interface 0/5
```

4.14.0.94 show packet-trace port tcpv4

Use this command to retrieve the trace profile for a TCP-IPv4 packet created from the configured packet fields. The trace profile indicates if the packet went out on LAG/ECMP route and also corresponding member/link information. Note that in order to get the trace profile for a TCP packet, the ethernet, IP and L4 packet fields need to be configured.

Default	None
Format	`show packet-trace port` ***slot/port*** `tcpv4`
Mode	Privileged Exec

4.14.0.95 show packet-trace port tcpv6

Use this command to retrieve the trace profile for a TCP-IPv6 packet created from the configured packet fields. The trace profile indicates if the packet went out on LAG/ECMP route and also the corresponding member/link information. Note that in order to get the trace profile for a TCP packet, the ethernet, IP and L4 packet fields need to be configured.

Default	None
Format	`show packet-trace port` ***slot/port*** `tcpv6`
Mode	Privileged Exec

4.14.0.96 show packet-trace port udpv4

Use this command to retrieve the trace profile for a UDP-IPv4 packet created from the configured packet fields. The trace profile indicates if the packet went out on LAG/ECMP route and also the corresponding member/link information. Note that in order to get the trace profile for a UDP packet, the ethernet, IP and L4 packet fields need to be configured.

Default	None
Format	`show packet-trace port` ***slot/port*** `udpv4`
Mode	Privileged Exec

4.14.0.97 show packet-trace port udpv6

Use this command to retrieve the trace profile for a UDP-IPv4 packet created from the configured packet fields. The trace profile indicates if the packet went out on LAG/ECMP route and also the corresponding member/link information. Note that in order to get the trace profile for a UDP packet, the ethernet, IP and L4 packet fields need to be configured.

Default	None
Format	`show packet-trace port` ***slot/port*** `udpv6`
Mode	Privileged Exec

4.14.0.98 clear packet-trace packet-data

Use this command to clear the configured packet header fields.

Format `clear packet-trace packet-data`
Mode Privileged Exec

4.14.0.99 watchdog clear

This command clears the watchdog settings and history and resets the timeout interval to the default value.

Format `watchdog clear`
Mode Privileged EXEC

4.14.0.100 watchdog disable

This command disables watchdog services. Watchdog is automatically changed (that is, no reboot is required).

Default Disabled
Format `watchdog disable`
Mode Privileged EXEC

4.14.0.101 watchdog enable

This command enables watchdog services. Watchdog services give EFOS the ability to recover when it is no longer executing properly. When a recovery is attempted, debug information is saved and the switch is reset.

Default Disabled
Format `watchdog enable`
Mode Privileged EXEC

4.15 BCM Shell Command

The BCM (SDK) shell is mainly used for debugging the Broadcom SDK. BCM shell commands can be executed directly from the CLI without entering the BCM shell itself by using the keyword `drivshell` before the BCM command. However, you can also enter the BCM shell to directly execute any of the BCM commands on the shell using the `bcmsh` command.

4.15.0.1 bcmsh

The `bcmsh` command is used to enter into the BCM shell from Privileged EXEC mode. Only users with Level 15 permissions can execute this command. Management is blocked during this mode; the user is notified and asked whether to continue. This command is only supported on the serial console and not via telnet/ssh.

Format	`bcmsh`
Mode	Privileged EXEC

NOTE: To exit the shell and return to the CLI, enter `exit`.

4.16 Cable Test Command

The cable test feature enables you to determine the cable connection status on a selected port.

NOTE: Note the following:

- The cable test feature is supported only for copper cable. It is not supported for optical fiber cable.
- If the port has an active link while the cable test is run, the link can go down for the duration of the test.

4.16.0.1 cablestatus

This command returns the status of the specified port.

Format `cablestatus` *slot/port*

Mode Privileged EXEC

Parameter	Description
Cable Status	One of the following statuses is returned: ■ **Normal**: The cable is working correctly. ■ **Open**: The cable is disconnected or there is a faulty connector. ■ **Short**: There is an electrical short in the cable. ■ **Cable Test Failed**: The cable status could not be determined. The cable may in fact be working. ■ **Crosstalk:** There is crosstalk present on the cable. ■ **No Cable:** There is no cable present.
Cable Length	If this feature is supported by the PHY for the current link speed, the cable length is displayed as a range between the shortest estimated length and the longest estimated length. Note that if the link is down and a cable is attached to a 10/100 Ethernet adapter, then the cable status may display as Open or Short because some Ethernet adapters leave unused wire pairs unterminated or grounded. Unknown is displayed if the cable length could not be determined.

4.17 Link Debounce Commands

In network deployments where the switch detects random spurious link flaps, network performance is affected due to the frequent unwanted re-convergence of topology for protocols like spanning tree, OSPF, and link aggregation.

The link debounce feature tries to solve this problem by delaying the link-down event notification to applications by waiting for a configurable duration of time known as the *debounce time*. During this time, the link may cycle through down-and-up states several times before it finally settles down. If the link goes down (and stays down), applications are notified after the debounce time period expires; otherwise it is ignored.

4.17.0.1 link debounce time

This command sets the duration of the link debounce timer. The link debounce timer starts when a link-down event occurs on an interface and runs for the configured amount of milliseconds. While the timer is running, any link flaps (up and down cycles) are ignored, and no link-down notifications are sent to higher-layer applications. After the debounce timer expires, if the link is still down, notifications are sent. The value for `milliseconds` is from 100 to 5000 in a multiple of 100 milliseconds.

Default 0 (No timer)
Format `link debounce time` *`milliseconds`*
Mode Interface Config

4.17.0.1.1 no link debounce time

This command resets the duration of the link debounce timer to the default value, effectively disabling the timer.

Format `no link debounce time`
Mode Interface Config

4.17.0.2 show interface debounce

This command displays the configured debounce time and occurrences of link flaps for all interfaces.

Format `show interface debounce`
Mode Privileged EXEC

Parameter	Definition
Interface	The physical port, LAG, or CPU interface associated with the rest of the data in the row.
Debounce Time	The time, in milliseconds, to delay a link-down event notification to applications after a link-down event occurs on the interface. If the link goes down (and stays down), applications are notified after the debounce time period expires; otherwise it is ignored. While the debounce timer is running, link flaps (up and down cycles) are counted but ignored.
Flaps	The number of link flaps (up and down cycles) the interface experienced while the debounce time was running.

Example: The following shows example CLI display output for the command.

```
(Routing) #show interface debounce
```

```
Interface Debounce Time (ms) Flaps
--------- ------------------ -------
0/1       0                  0
0/2       0                  0
0/3       0                  0
0/4       0                  0
0/5       0                  0
0/6       0                  0
0/7       0                  0
0/8       0                  0
0/9       0                  0
0/10      0                  0
0/11      0                  0
0/12      0                  0
--More-- or (q)uit
```

4.18 Port Locator Commands

The port locator commands identify ports that have network cabling errors and/or cabling complications (mis-wiring) by providing a command that blinks a single interface's LED or the LEDs of multiple interfaces and turns off all other interface LEDs so that the mis-wired interface can be easily identified. The LEDs blink at the rate of one second on and one second off. The LED of interfaces that are linked up will have their LEDs solidly lit only if port locator is not enabled on that interface. Traffic present on any interface will not cause the LED to blink to indicate traffic. A port–locator enabled interface will blink and not light solid if the link is up. In other words, port locator has precedence over link status.

If an interface has two LEDs, one for link and a second for activity, only the link LED is used for the port locator function. The activity LED is turned off while the port locator feature is active. If an interface has one LED for link and activity, the LED will not blink if activity is present on the interface while the port locator feature is active.

Out-of-band port LEDs are not affected by this feature. This feature is configurable on physical ports, LAGs, diagnostically disabled ports, and pluggable module ports.

4.18.0.1 port-locator disable

This command globally disables the port locator function and restores all port LEDs to normal operation.

Format `port-locator disable`

Mode
- Privileged EXEC
- Interface Config

Example:

```
(Routing)(Config)# port-locator disable
```

4.18.0.2 port-locator enable

This command turns on the LED for the interface or interfaces.

Format `port-locator enable`

Mode Interface Config

Example:

```
(Routing)(Interface 0/1,0/3,0/5,0/7)#port-locator enable

(Routing)(Interface 0/54,0/55,0/56,0/57)#port-locator enable

Error! Interface 0/55  is in Detach state
Error! Interface 0/56  is in Detach state
Error! Interface 0/57  is in Detach state
```

4.18.0.3 show port- locator

This command displays which port or ports currently have locator mode enabled. LAG interfaces are also displayed if port-locator was enabled on a LAG.

Format `show port-locator`

Mode Privileged EXEC

Example:

```
(Routing)#show port-locator

          Locator
Intf      Mode
--------- --------
0/1       Enable
0/2       Disable
0/3       Enable
0/4       Disable
0/5       Enable
0/6       Disable
0/7       Enable
0/8       Disable
0/9       Enable
```

Example: Below interface 3/1 is a LAG interface, members are 0/1 and 0/45.

```
(Routing)#show port-locator  | include enable

0/1       enable
0/45      enable
3/1       enable
```

4.19 sFlow Commands

sFlow is the standard for monitoring high-speed switched and routed networks. sFlow technology is built into network equipment and gives complete visibility into network activity, enabling effective management and control of network resources.

4.19.0.1 sflow receiver

Use this command to configure the sFlow collector parameters (owner string, receiver timeout, max datagram size, IP address, and port).

NOTE: Use this command to configure a receiver as a nontimeout entry. Unlike entries configured with a specific timeout value, this command is shown in `show running-config` and retained after reboot. As the sFlow receiver is configured as a nontimeout entry, information related to sampler and pollers are also shown in the running-config and are retained after reboot. (If a receiver is configured with a specific value, these configurations are not shown in running-config. Sampler and poller information related to this receiver are also not shown running-config.)

Format `sflow receiver` ***rcvr_idx*** `{owner` ***owner-string*** `{timeout` ***rcvr_timeout*** `| notimeout} | max datagram` ***size*** `| ip` ***ip*** `| port` ***port***`}`

Mode Global Config

Parameter	Description
Receiver Owner	The identity string for the receiver, the entity making use of this sFlowRcvrTable entry. The range is 127 characters. The default is a null string. The empty string indicates that the entry is currently unclaimed and the receiver configuration is reset to the default values. An entity wishing to claim an sFlowRcvrTable entry must ensure that the entry is unclaimed before trying to claim it. The entry is claimed by setting the owner string to a non-null value. The entry must be claimed before assigning a receiver to a sampler or poller.
Receiver Timeout	The time, in seconds, remaining before the sampler or poller is released and stops sending samples to receiver. A management entity wanting to maintain control of the sampler is responsible for setting a new value before the old one expires. The allowed range is 0-2147483647 seconds. The default is zero (0).
No Timeout	Entries configured with a notimeout entry will be in the running config until the user explicitly removes the entry.
Receiver Max Datagram Size	The maximum number of data bytes that can be sent in a single sample datagram. The management entity should set this value to avoid fragmentation of the sFlow datagrams. The allowed range is 200 to 9116). The default is 1400.
Receiver IP	The sFlow receiver IP address. If set to 0.0.0.0, no sFlow datagrams will be sent. The default is 0.0.0.0.
Receiver Port	The destination Layer4 UDP port for sFlow datagrams. The range is 1-65535. The default is 6343.

4.19.0.1.1 no sflow receiver

Use this command to set the sFlow collector parameters back to the defaults.

Format `no sflow receiver` ***indx*** `{ip` ***ip-address*** `| maxdatagram` ***size*** `| owner` ***string*** `timeout` ***interval*** `| port` ***14-port***`}`

Mode Global Config

4.19.0.2 sflow receiver owner timeout

Use this command to configure a receiver as a timeout entry. As the sFlow receiver is configured as a timeout entry, information related to sampler and pollers are also shown in the running-config and are retained after reboot.

If a receiver is configured with a specific value, these configurations will not be shown in running-config. Samplers and pollers information related to this receiver will also not be shown in running-config.

Format `sflow receiver` *`index`* `owner` *`owner-string`* `timeout`
Mode Global Config

Field	Description
index	Receiver index identifier. The range is 1 to 8.
Receiver Owner	The owner name corresponds to the receiver name. The identity string for the receiver, the entity making use of this sFlowRcvrTable entry. The range is 127 characters. The default is a null string. The empty string indicates that the entry is currently unclaimed and the receiver configuration is reset to the default values. An entity wishing to claim an sFlowRcvrTable entry must ensure that the entry is unclaimed before trying to claim it. The entry is claimed by setting the owner string to a non-null value. The entry must be claimed before assigning a receiver to a sampler or poller.

4.19.0.3 sflow receiver owner notimeout

Use this command to configure a receiver as a non-timeout entry. Unlike entries configured with a specific timeout value, this command will be shown in show running-config and retained after reboot. As the sFlow receiver is configured as a non-timeout entry, information related to sampler and pollers will also be shown in the running-config and will be retained after reboot.

If a receiver is configured with a specific value, these configurations will not be shown in running-config. Samplers and pollers information related to this receiver will also not be shown in running-config.

Format `sflow receiver` *`rcvr_idx`* `owner` *`owner-string`* `notimeout`
Mode Global Config

Parameter	Description
rcvr_idx	Receiver index identifier.
Receiver Owner	The owner name corresponds to the receiver name. The identity string for the receiver, the entity making use of this sFlowRcvrTable entry. The range is 127 characters. The default is a null string. The empty string indicates that the entry is currently unclaimed and the receiver configuration is reset to the default values. An entity wishing to claim an sFlowRcvrTable entry must ensure that the entry is unclaimed before trying to claim it. The entry is claimed by setting the owner string to a non-null value. The entry must be claimed before assigning a receiver to a sampler or poller.

4.19.0.4 sflow remote-agent ip

Use this command to assign an IPv4 address to a remote agent. When sFlow hardware sampling is enabled, the switch/hardware sends sampled packets encapsulated in sFlow custom packet to this IP address.

Default 0.0.0.0
Format `sflow remote-agent` *`index`* `ip` *`ipv4-address`*
Mode Global Config

4.19.0.4.1 no sflow remote-agent ip

Use this command to remove the remote agent IPv4 address.

Format `no sflow remote-agent` *`index`* `ip`
Mode Global Config

4.19.0.5 sflow remote-agent monitor-session

Use this command to assign the monitor ID (MTP) for the remote agent session. The destination port is an outgoing interface for sFlow sampled packets. The sflow sampled packets are sent to all the configured destination ports, irrespective of monitor session index.

Default 0 for both monitor session and destination port
Format `sflow remote-agent` *`index`* `monitor-session` *`session id range 1-4`* `destination interface slot/port`
Mode Global Config

4.19.0.5.1 no sflow remote-agent monitor-session

This command removes the remote-agent configuration.

Format `no sflow remote-agent` *`index`* `monitor-session`
Mode Global Config

4.19.0.6 sflow remote-agent port

This command configures the destination UDP port for the remote-agent.

Default 16343
Format `sflow remote-agent` *`index`* `port` *`value`*
Mode Global Config

4.19.0.6.1 no sflow remote-agent port

This command removes remote agent port configuration.

Format `no sflow remote-agent port`
Mode Global Config

4.19.0.7 sflow remote-agent source-interface

Use this command to specify the physical or logical interface to use as the sFlow client source interface for the remote-agent. If configured, the address of source interface is used for all sFlow communications between the sFlow receiver and the sFlow client. Otherwise, there is no change in behavior. If the configured interface is down, the sFlow client falls back to normal behavior.

Format *`sflow remote-agent source-interface {slot/port | loopback loopback-id | tunnel tunnel-id | vlan vlan-id}`*

Mode Global Config

4.19.0.7.1 no sflow remote-agent source-interface

Use this command to reset the sFlow source interface for the remote-agent to the default settings.

Format `no sflow remote-agent port`
Mode Global Config

4.19.0.8 sflow sampler

A data source configured to collect flow samples is called a poller. Use this command to configure a new sFlow sampler instance on an interface or range of interfaces for this data source if `rcvr_idx` is valid.

Format `sflow sampler {`*`rcvr-indx`* `| rate` *`sampling-rate`* `| maxheadersize` *`size`*`}`
Mode Interface Config

Parameter	Description
Receiver Index	The sFlow Receiver for this sFlow sampler to which flow samples are to be sent. A value of zero (0) means that no receiver is configured, no packets will be sampled. Only active receivers can be set. If a receiver expires, then all samplers associated with the receiver will also expire. Possible values are 1-8. The default is 0.
Maxheadersize	The maximum number of bytes that should be copied from the sampler packet. The range is 20-256. The default is 128. When set to zero (0), all the sampler parameters are set to their corresponding default value.
Sampling Rate	The statistical sampling rate for packet sampling from this source. A sampling rate of 1 counts all packets. A value of zero (0) disables sampling. A value of N means that out of N incoming packets, 1 packet will be sampled. The range is 1024-65536 and 0. The default is 0.

4.19.0.8.1 no sflow sampler

Use this command to reset the sFlow sampler instance to the default settings.

Format `no sflow sampler {`*`rcvr-indx`* `| rate` *`sampling-rate`* `| maxheadersize` *`size`*`}`
Mode Interface Config

4.19.0.9 sflow poller

A data source configured to collect counter samples is called a poller. Use this command to enable a new sFlow poller instance on an interface or range of interfaces for this data source if `rcvr_idx` is valid.

Format `sflow poller {`*`rcvr-indx`* `| interval` *`poll-interval`*`}`
Mode Interface Config

Parameter	Description
Receiver Index	Enter the sFlow Receiver associated with the sampler/poller. A value of zero (0) means that no receiver is configured. The range is 1-8. The default is 0.

Parameter	Description
Poll Interval	Enter the sFlow instance polling interval. A poll interval of zero (0) disables counter sampling. When set to zero (0), all the poller parameters are set to their corresponding default value. The range is 0-86400. The default is 0. A value of N means once in N seconds a counter sample is generated.

NOTE: The sFlow task is heavily loaded when the sFlow polling interval is configured at the minimum value (i.e., one second for all the sFlow supported interfaces). In this case, the sFlow task is always busy collecting the counters on all the configured interfaces. This can cause the device to hang for some time when the user tries to configure or issue show sFlow commands. To overcome this situation, sFlow polling interval configuration on an interface or range of interfaces is controlled as mentioned below:

1. The maximum number of allowed interfaces for the polling intervals max (1, (interval – 10)) to min ((interval + 10), 86400) is: interval * 5
2. For every one second increment in the polling interval that is configured, the number of allowed interfaces that can be configured increases by 5.

4.19.0.9.1 no sflow poller

Use this command to reset the sFlow poller instance to the default settings.

Format `no sflow poller {`*`rcvr-indx`* `| interval` *`poll-interval`*`}`
Mode Interface Config

4.19.0.10 sflow sampler rate

Use this command to set the sampling rate for ingress/egress/flow-based sampling on this interface.

Default 0 for the ingress sampling rate.
Format `sflow sampler rate` *`value`* `{ingress | egress | flow-based}`
Mode Interface Config

4.19.0.10.1 no sflow sample rate

Use this command to remove the sampling rate for ingress/egress/flow-based sampling on this interface.

Format `no sflow sampler rate` *`value`* `{ingress | egress | flow-based}`
Mode Interface Config

4.19.0.11 sflow sampler remote-agent

Use this command to enable a new sFlow sampler remote agent instance for this data source.

Default None
Format `sflow sampler remote-agent` *`index`*
Mode Interface Config

4.19.0.11.1 no sflow sampler remote-agent

Use this command to disable an sFlow sampler remote agent instance for this data source.

Format `no sflow sampler remote-agent`
Mode Interface Config

4.19.0.12 sflow source-interface

Use this command to specify the physical or logical interface to use as the sFlow client source interface. If configured, the address of source Interface is used for all sFlow communications between the sFlow receiver and the sFlow client. Otherwise there is no change in behavior. If the configured interface is down, the sFlow client falls back to normal behavior.

Format `sflow source-interface {slot/port | loopback` *`loopback-id`* `|` *`tunnel tunnel-id`* `|` *`vlan vlan-id`*`}`
Mode Global Config

Parameter	Description
slot/port	Specifies the port to use as the source interface.
loopback-id	Specifies the loopback interface to use as the source interface. The range of the loopback ID is 0 to 7.
tunnel-id	Specifies the tunnel interface to use as the source interface. The range of the tunnel ID is 0 to 7.
vlan-id	Specifies the VLAN to use as the source interface.

4.19.0.12.1 no sflow source-interface

Use this command to reset the sFlow source interface to the default settings.

Format `no sflow source-interface`
Mode Global Config

4.19.0.13 show sflow agent

The sFlow agent collects time-based sampling of network interface statistics and flow-based samples. These are sent to the configured sFlow receivers. Use this command to display the sFlow agent information.

Format `show sflow agent`
Mode Privileged EXEC

Parameter	Description
sFlow Version	Uniquely identifies the version and implementation of this MIB. The version string must have the following structure: MIB Version; Organization; Software Revision where: ■ MIB Version: 1.3, the version of this MIB. ■ Organization: Broadcom Corp. ■ Revision: 1.0
IP Address	The IP address associated with this agent.

Example: The following shows example CLI display output for the command.

```
(Routing) #show sflow agent

sFlow Version..................................... 1.3;Broadcom Corp;1.2
IP Address........................................ 10.131.12.66
```

4.19.0.14 show sflow pollers

Use this command to display the sFlow polling instances created on the switch. Use “-” for range.

Format `show sflow pollers`

Mode Privileged EXEC

Parameter	Description
Poller Data Source	The sFlowDataSource (slot/port) for this sFlow sampler. This agent will support Physical ports only.
Receiver Index	The sFlowReceiver associated with this sFlow counter poller.
Poller Interval	The number of seconds between successive samples of the counters associated with this data source.

4.19.0.15 show sflow receivers

Use this command to display configuration information related to the sFlow receivers.

Format `show sflow receivers [`*`index`*`]`

Mode Privileged EXEC

Parameter	Description
Receiver Index	The sFlow Receiver associated with the sampler/poller.
Owner String	The identity string for receiver, the entity making use of this sFlowRcvrTable entry.
Time Out	The time (in seconds) remaining before the receiver is released and stops sending samples to sFlow receiver. The **no timeout** value of this parameter means that the sFlow receiver is configured as a non-timeout entry.
Max Datagram Size	The maximum number of bytes that can be sent in a single sFlow datagram.
Port	The destination Layer4 UDP port for sFlow datagrams.
IP Address	The sFlow receiver IP address.
Address Type	The sFlow receiver IP address type. For an IPv4 address, the value is 1.
Datagram Version	The sFlow protocol version to be used while sending samples to sFlow receiver.

Example: The following shows example CLI display output for the **show sflow receivers** command.

```
(Routing) #show sflow receivers 1
Receiver Index.................................... 1
Owner String...................................... tulasi
Time out.......................................... 0
IP Address:....................................... 0.0.0.0
Address Type...................................... 1
Port.............................................. 6343
Datagram Version.................................. 5
Maximum Datagram Size............................. 1400
```

Example: The following examples show CLI display output for the command when a receiver is configured as a non-timeout entry.

```
(Routing) #show sflow receivers

Rcvr Owner                           Timeout    Max Dgram Port  IP Address
Indx String                                     Size
---- ------------------------------- ---------- --------- ----- ---------------
1    tulasi                          No Timeout 1400      6343  0.0.0.0
2                                    0          1400      6343  0.0.0.0
3                                    0          1400      6343  0.0.0.0
4                                    0          1400      6343  0.0.0.0
5                                    0          1400      6343  0.0.0.0
6                                    0          1400      6343  0.0.0.0
7                                    0          1400      6343  0.0.0.0
8                                    0          1400      6343  0.0.0.0


(Routing) #show sflow receivers 1

Receiver Index.............................. 1
Owner String................................ tulasi
Time out.................................... No Timeout
IP Address:................................. 0.0.0.0
Address Type................................ 1
Port........................................ 6343
Datagram Version............................ 5
Maximum Datagram Size....................... 1400
```

4.19.0.16 show sflow remote-agents

Use this command to display the details for configured sFlow remote agents.

Format `show sflow remote-agents`

Mode Privileged EXEC

Example:

```
(Routing) (Config)#show sflow remote-agents

Rem Agent  Port      IP Address       Monitor     Dest.
Index                               Session     Port
---------- --------  ---------------  ---------   ----------
1          16343     1.1.1.1           1          0/4
2          26343     2.2.1.1           2          0/8
3          16343     0.0.0.0
4          16343     0.0.0.0
```

4.19.0.17 show sflow remote-agents source-interface

Use this command to display the source interface configured on the switch for the sFlow remote agent.

Format `show sflow remote-agents`

Mode Privileged EXEC

Example:

```
(Routing) #show sflow remote-agents source-interface

sFlow Remote Agent Source Interface..... serviceport
sFlow Remote Agent Client Source IPv4 Address.. 10.130.86.191          [Up]
```

4.19.0.18 show sflow samplers

Use this command to display the sFlow sampling instances created on the switch.

Format `show sflow samplers`

Mode Privileged EXEC

Field	Description
Sampler Data Source	The sFlowDataSource (slot/port) for this sFlow sampler. This agent will support Physical ports only.
Receiver Index	The sFlowReceiver configured for this sFlow sampler.
Remote Agent	The remote agent instance index number.
Ingress Sampling Rate	The sampling rate for the ingress.
Flow Sampling Rate	The statistical sampling rate for packet sampling from this source.
Egress Sampling Rate	The sampling rate for the egress.
Max Header Size	The maximum number of bytes that should be copied from a sampled packet to form a flow sample.

Example:

```
(Routing) (Config)#show sflow samplers
Sampler      Receiver    Remote     Ingress      Flow         Egress        Max
Data         Index       Agent      Sampling     Sampling     Sampling      Header
Source                              Rate         Rate         Rate          Size
----------   ----------  --------   -----------   ------------  ---------- --------
 0/1         1           2          1024         2048          4096         128
```

4.19.0.19 show sflow source-interface

Use this command to display the sFlow source interface configured on the switch.

Format `show sflow source-interface`

Mode Privileged EXEC

Field	Description
sFlow Client Source Interface	The interface ID of the physical or logical interface configured as the sFlow client source interface.
sFlow Client Source IPv4 Address	The IP address of the interface configured as the sFlow client source interface.

4.20 Switch Database Management Template Commands

A Switch Database Management (SDM) template is a description of the maximum resources a switch or router can use for various features. Different SDM templates allow different combinations of scaling factors, enabling different allocations of resources depending on how the device is used. In other words, SDM templates enable you to reallocate system resources to support a different mix of features based on your network requirements.

The IPv4 and IPv6 route limits on an SDM template give the over-subscribed maximum routes supported by the switch when only the respective route type (IPv4 or IPv6) is present on the switch. The actual maximum number of routes will be less when both IPv4 and IPv6 routes are present and will depend on the mix of these two route types.

4.20.0.1 sdm prefer

Use this command to change the template that will be active after the next reboot. The keywords are as follows:

- **dual-ipv4-and-ipv6**—Filters subsequent template choices to those that support both IPv4 and IPv6. The `default` template maximizes the number of IPv4 and IPv6 unicast routes, while limiting the number of ECMP next hops in each route to 4. The `data-center` template support increases the number of ECMP next hops to 32. The `alpm` and `alpm-mpls-data-center` templates accommodate larger routes. The values for the `alpm` and `alpm-mpls-data-center` templates are shown below:

```
dual-ipv4-and-ipv6 alpm:

ARP Entries..................................... 2560
IPv4 Unicast Routes............................. 32768
IPv6 NDP Entries................................ 2560
IPv6 Unicast Routes............................. 24576
ECMP Next Hops.................................. 48
IPv4 Multicast Routes........................... 0
IPv6 Multicast Routes........................... 0


dual-ipv4-and-ipv6 alpm-mpls-data-center:

ARP Entries..................................... 2560
IPv4 Unicast Routes............................. 32768
IPv6 NDP Entries................................ 2560
IPv6 Unicast Routes............................. 24576
ECMP Next Hops.................................. 16
IPv4 Multicast Routes........................... 0
IPv6 Multicast Routes........................... 0
```

- **ipv4-routing**—Filters subsequent template choices to those that support IPv4, and not IPv6. The IPv4-routing `default` template maximizes the number of IPv4 unicast routes, while limiting the number of ECMP next hops in each route to 4. The `data-center default` template supports increases the number of ECMP next hops to 32 and reduces the number of routes. The `data-center plus` template increases the number of ECMP next hops to 32 while keeping the maximum IPv4 routes.

The max ARP template supports 16k ARP entries for the StrataXGS® IV platforms. The other EFOS platforms support 6k (unchanged, existing value) ARP entries.

NOTE: After setting the template, you must reboot in order for the configuration change to take effect.

Default ipv4-routing data-center plus

Format `sdm prefer { dual-ipv4-and-ipv6 { alpm | alpm-mpls-data-center | data-center | dcvpn-data-center | default | mpls-data-center } | ipv4-routing { default | data-center { dcvpn-data-center | plus | max-arp} | unicast-only}}`

Mode Global Config

4.20.0.1.1 no sdm prefer

Use this command to revert to the default template after the next reboot.

Format `no sdm prefer`

Mode Global Config

4.20.0.2 show sdm prefer

Use this command to view the currently active SDM template and its scaling parameters, or to view the scaling parameters for an inactive template. When invoked with no optional keywords, this command lists the currently active template and the template that will become active on the next reboot, if it is different from the currently active template. If the system boots with a non-default template, and you clear the template configuration, either using `no sdm prefer` or by deleting the startup configuration, `show sdm prefer` lists the default template as the next active template. To list the scaling parameters of a specific template, use that template's keyword as an argument to the command.

Use the optional keywords to list the scaling parameters of a specific template.

Format `show sdm prefer { dual-ipv4-and-ipv6 { alpm | alpm-mpls-data-center | data-center | dcvpn-data-center | default | mpls-data-center } | ipv4-routing { default | data-center { dcvpn-data-center | default | plus | max-arp} | unicast-only} }`

Mode Privileged EXEC

Syntax	Description
dual-ipv4-and-ipv6 default	(Optional) List the scaling parameters for the template supporting IPv4 and IPv6.
dual-ipv4-and-ipv6 data-center	(Optional) List the scaling parameters for the Dual IPv4 and IPv6 template supporting more ECMP next hops.
dual-ipv4-and-ipv6 alpm	(Optional) Lists the scaling parameters for the alpm template.
dual-ipv4-and-ipv6 alpm-mpls-data-center	(Optional) Lists the scaling parameters for the alpm-mpls-data-center template.
ipv4-routing default	(Optional) List the scaling parameters for the IPv4-only template maximizing the number of unicast routes.
ipv4-routing data-center default	(Optional) List the scaling parameters for the IPv4-only template supporting more ECMP next hops.
ipv4-routing data-center plus	(Optional) List the scaling parameters for the IPv4-only template maximizing the number of unicast routes and also supporting more ECMP next hops.
dcvpn-data-center	(Optional) List the scaling parameters for the IPv4-only template for DCVPN feature.
default	(Optional) List the scaling parameters for the IPv4-only template.
plus	(Optional) List the scaling parameters for the IPv4-only template maximizing the ipv4 routes.

Syntax	Description
max-arp	(Optional) List the scaling parameters for the IPv4-only template supporting max number of arp entries.
unicast-only	(Optional) List the scaling parameters for the IPv4-only template supporting only unicast routes
alpm	(Optional) List the scaling parameters for IPv4 and IPv6 template maximizing the number of IPv4 and IPv6 routes
alpm-mpls-data-center	(Optional) List the scaling parameters for IPv4 and IPv6 template maximizing the number of IPv4 and IPv6 routes for data center.
data-center	(Optional) List the scaling parameters for IPv4 and IPv6 template to support routes for data-center.
dcvpn-data-center	(Optional) List the scaling parameters for IPv4 and IPv6 template for the DCVPN feature
mpls-data-center	(Optional) List the scaling parameters for IPv4 and IPv6 template for the MPLS feature

Field	Description
ARP Entries	The maximum number of entries in the IPv4 Address Resolution Protocol (ARP) cache for routing interfaces.
IPv4 Unicast Routes	The maximum number of IPv4 unicast forwarding table entries.
IPv6 NDP Entries	The maximum number of IPv6 Neighbor Discovery Protocol (NDP) cache entries.
IPv6 Unicast Routes	The maximum number of IPv6 unicast forwarding table entries.
ECMP Next Hops	The maximum number of next hops that can be installed in the IPv4 and IPv6 unicast forwarding tables.

Example: This example shows the current SDM template. The user has not changed the next active SDM template.

```
(router)#show sdm prefer

The current template is the Dual IPv4 and IPv6 template.

ARP Entries..................................... 4096
IPv4 Unicast Routes............................. 8160
IPv6 NDP Entries................................ 1024
IPv6 Unicast Routes............................. 4096
ECMP Next Hops.................................. 4
```

Now the user sets the next active SDM template.

```
(router) # configure
(router) (Config)  # sdm prefer ipv4-only data-center
Changes to the running SDM preferences have been stored, but cannot take effect until the next reload.
Use 'show sdm prefer' to see what SDM preference is currently active.

(router) # show sdm prefer

The current template is the dual IPv4 and IPv6 template.

ARP Entries.................................4096
IPv4 Unicast Routes.........................8160
IPv6 NDP Entries............................1024
IPv6 Unicast Routes.........................4096
```

```
ECMP Next Hops.............................4
```

On the next reload, the template will be the IPv4 data center template.

To list the scaling parameters for the data center template, invoke the command with the **ipv4-only data-center** keywords.

```
(router) # show sdm prefer ipv4-only data-center

Scaling parameters for the IPv4 data center template:

ARP Entries................................4096
IPv4 Unicast Routes........................8160
IPv6 NDP Entries...........................0
IPv6 Unicast Routes........................0
ECMP Next Hops.............................32
```

4.21 SFP Transceiver Commands

These commands show details for the SFP transceivers. Transceivers that are compliant with the SFF-8472(SFP+) and SFF-8436(QSFP+) standards are supported.

4.21.0.1 show fiber-ports optical-transceiver

This command displays the diagnostic information of the SFP. The values are derived from the SFP's A2 (Diagnostics) table using the I2c interface.

Format `show fiber-ports optical-transceiver {all|slot/port}`

Mode Privileged EXEC

Parameter	Description
Temp	Internally measured transceiver temperature.
Voltage	Internally measured supply voltage.
Current	Measured TX bias current.
Output Power	Measured optical output power relative to 1mW.
Input Power	Measured optical power received relative to 1mW.
TX Fault	Transmitter fault.
LOS	Loss of signal.

Example: The following shows example CLI display output for the command.

```
(Routing) #show fiber-ports optical-transceiver all

                                    Output    Input
Port      Temp  Voltage  Current     Power    Power   TX     LOS
           [C]   [Volt]     [mA]     [dBm]    [dBm]   Fault
--------  ----  -------  -------   -------  -------   -----  ---
0/49      39.3    3.256      5.0    -2.234   -2.465   No     No
0/50      33.9    3.260      5.3    -2.374  -40.000   No     Yes
0/51      32.2    3.256      5.6    -2.300   -2.897   No     No


(Routing) #show fiber-ports optical-transceiver 0/49

                                    Output    Input
Port      Temp  Voltage  Current     Power    Power   TX     LOS
           [C]   [Volt]     [mA]     [dBm]    [dBm]   Fault
--------  ----  -------  -------   -------  -------   -----  ---
0/49      39.3    3.256      5.0    -2.234   -2.465   No     No
```

4.21.0.2 show fiber-ports optical-transceiver-info

This command displays the SFP vendor-related information. The values are derived from the SFP's A0 table using the I2c interface.

Format `show fiber-ports optical-transceiver-info {all|slot/port}`

Mode Privileged EXEC

Parameter	Description
Vendor Name	The vendor name is the full name of the corporation, an abbreviation for the name of the corporation, the SCSI company code for the corporation, or the stock exchange symbol for the corporation. The name is 1 to 16 ASCII characters in length.
Link Length 50um	This value specifies the link length that is supported by the transceiver while operating in compliance with applicable standards using 50 micron multimode OM2 [500 MHz * km at 850nm] fiber. A value of zero means that the transceiver does not support 50 micron multimode fiber or that the length information must be determined from the transceiver technology.
Link Length 62.5um	This value specifies the link length that is supported by the transceiver while operating in compliance with applicable standards using 62.5 micron multimode OM1 [200 MHz * km at 850nm, 500 MHz * km at 1310nm] fiber. A value of zero means that the transceiver does not support 62.5 micron multimode fiber or that the length information must be determined from the transceiver technology.
Serial Number	The vendor serial number for the transceiver. The serial number is 1 to 16 ASCII characters in length. A value of all zeros in the field indicates that the vendor serial number is unspecified.
Part Number	The vendor part number or product name. A value of all zeros in the 16-byte field indicates that the vendor part number is unspecified.
Nominal Bit Rate	The nominal bit (signaling) rate, specified in units of 100 MBd, rounded off to the nearest 100 MBd. The bit rate includes those bits necessary to encode and delimit the signal, as well as those bits carrying data information. A value of zero indicates that the bit rate is not specified and must be determined from the transceiver technology. The actual information transfer rate depends on the encoding of the data, as defined by the encoding value.
Rev	The vendor's product revision number. A blank value in this field indicates that the vendor revision is unspecified.

Example: The following shows example CLI display output for the command.

```
(Switching) #show fiber-ports optical-transceiver-info all

                         Link Link                                    Nominal
                       Length Length                                      Bit
                         50um 62.5um                                    Rate
Port     Vendor Name       [m] [m]  Serial Number    Part Number     [Mbps] Rev
-------- ---------------- --- ---- ---------------- ---------------- ------ ----
0/49     NETGEAR            8    3 A7N2018414       AXM761            10300 10
0/51     NETGEAR            8    3 A7N2018472       AXM761            10300 10
0/52     NETGEAR            8    3 A7N2018501       AXM761            10300 10


(Switching) #show fiber-ports optical-transceiver-info 0/49

                         Link Link                                    Nominal
                       Length Length                                      Bit
                         50um 62.5um                                    Rate
Port     Vendor Name       [m] [m]  Serial Number    Part Number     [Mbps] Rev
-------- ---------------- --- ---- ---------------- ---------------- ------ ----
0/49     NETGEAR            8    3 A7N2018414       AXM761            10300 10
```

4.22 Remote Monitoring Commands

Remote Monitoring (RMON) is a method of collecting a variety of data about network traffic. RMON supports 64-bit counters (RFC 3273) and High Capacity Alarm Table (RFC 3434).

NOTE: There is no configuration command for ether stats and high capacity ether stats. The data source for ether stats and high capacity ether stats are configured during initialization.

4.22.0.1 rmon alarm

This command sets the RMON alarm entry in the RMON alarm MIB group.

Format `rmon alarm` *`alarm number variable sample interval`* `{absolute|delta} rising-threshold` *`value`* `[`*`rising-event-index`*`] falling-threshold` *`value`* `[`*`falling-event-index`*`] [startup {`*`rising`*`|`*`falling`*`|`*`rising-falling`*`}] [owner` *`string`*`]`

Mode Global Config

Parameter	Description
Alarm Index	An index that uniquely identifies an entry in the alarm table. Each entry defines a diagnostic sample at a particular interval for an object on the device. The range is 1 to 65535.
Alarm Variable	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of integer.
Alarm Interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. The range is 1 to 2147483647. The default is 1.
Alarm Absolute Value	The value of the statistic during the last sampling period. This object is a read-only, 32-bit signed value.
Alarm Rising Threshold	The rising threshold for the sample statistics. The range is 2147483648 to 2147483647. The default is 1.
Alarm Rising Event Index	The index of the eventEntry that is used when a rising threshold is crossed. The range is 1 to 65535. The default is 1.
Alarm Falling Threshold	The falling threshold for the sample statistics. The range is 2147483648 to 2147483647. The default is 1.
Alarm Falling Event Index	The index of the eventEntry that is used when a falling threshold is crossed. The range is 1 to 65535. The default is 2.
Alarm Startup Alarm	The alarm that may be sent. Possible values are **rising, falling** or both **rising-falling**. The default is **rising-falling**.
Alarm Owner	The owner string associated with the alarm entry. The default is **monitorAlarm**.

Example: The following shows an example of the command.

```
(Routing) (Config)# rmon alarm 1 ifInErrors.2 30 absolute rising-threshold 100 1 falling-threshold 10
2 startup rising owner myOwner
```

4.22.0.1.1 no rmon alarm

This command deletes the RMON alarm entry.

Format `no rmon alarm` *`alarm number`*

Mode Global Config

Example: The following shows an example of the command.

```
(Routing) (Config)# no rmon alarm 1
```

4.22.0.2 rmon hcalarm

This command sets the RMON hcalarm entry in the High Capacity RMON alarm MIB group.

Format `rmon hcalarm` ***`alarm number variable sample interval`*** `{absolute|delta} rising-threshold high` ***`value`*** `low` ***`value`*** `status {positive|negative} [`***`rising-event-index`***`] falling-threshold high` ***`value`*** `low` ***`value`*** `status {positive|negative} [`***`falling-event-index`***`] [startup {`***`rising`***`|`***`falling`***`|`***`rising-falling`***`}] [owner` ***`string`***`]`

Mode Global Config

Parameter	Description
High Capacity Alarm Index	An arbitrary integer index value used to uniquely identify the high capacity alarm entry. The range is 1 to 65535.
High Capacity Alarm Variable	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of integer.
High Capacity Alarm Interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. The range is 1 to 2147483647. The default is 1.
High Capacity Alarm Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds. Possible types are **Absolute Value** or **Delta Value**. The default is **Absolute Value**.
High Capacity Alarm Absolute Value	The absolute value (that is, the unsigned value) of the hcAlarmVariable statistic during the last sampling period. The value during the current sampling period is not made available until the period is complete. This object is a 64-bit unsigned value that is Read-Only.
High Capacity Alarm Absolute Alarm Status	This object indicates the validity and sign of the data for the high capacity alarm absolute value object (hcAlarmAbsValueobject). Possible status types are **valueNotAvailable**, **valuePositive**, or **valueNegative**. The default is **valueNotAvailable**.
High Capacity Alarm Startup Alarm	High capacity alarm startup alarm that may be sent. Possible values are **rising**, **falling**, or **rising-falling**. The default is **rising-falling**.
High Capacity Alarm Rising-Threshold Absolute Value Low	The lower 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 1.
High Capacity Alarm Rising-Threshold Absolute Value High	The upper 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 0.
High Capacity Alarm Rising-Threshold Value Status	This object indicates the sign of the data for the rising threshold, as defined by the objects hcAlarmRisingThresAbsValueLow and hcAlarmRisingThresAbsValueHigh. Possible values are **valueNotAvailable**, **valuePositive**, or **valueNegative**. The default is **valuePositive**.
High Capacity Alarm Falling-Threshold Absolute Value Low	The lower 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 1.
High Capacity Alarm Falling-Threshold Absolute Value High	The upper 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 0.
High Capacity Alarm Falling-Threshold Value Status	This object indicates the sign of the data for the falling threshold, as defined by the objects hcAlarmFallingThresAbsValueLow and hcAlarmFallingThresAbsValueHigh. Possible values are **valueNotAvailable**, **valuePositive**, or **valueNegative**. The default is **valuePositive**.
High Capacity Alarm Rising Event Index	The index of the eventEntry that is used when a rising threshold is crossed. The range is 1 to 65535. The default is 1.
High Capacity Alarm Falling Event Index	The index of the eventEntry that is used when a falling threshold is crossed. The range is 1 to 65535. The default is 2.

Parameter	Description
High Capacity Alarm Failed Attempts	The number of times the associated hcAlarmVariable instance was polled on behalf of the hcAlarmEntry (while in the active state) and the value was not available. This object is a 32-bit counter value that is read-only.
High Capacity Alarm Owner	The owner string associated with the alarm entry. The default is **monitorHCAlarm**.
High Capacity Alarm Storage Type	The type of non-volatile storage configured for this entry. This object is read-only. The default is **volatile**.

Example: The following shows an example of the command.

```
(Routing) (Config)# rmon hcalarm 1 ifInOctets.1 30 absolute rising-threshold high 1 low 100 status
positive 1 falling-threshold high 1 low 10 status positive startup rising owner myOwner
```

4.22.0.2.1 no rmon hcalarm

This command deletes the rmon hcalarm entry.

Format `no rmon hcalarm` *`alarm number`*

Mode Global Config

Example: The following shows an example of the command.

```
(Routing) (Config)# no rmon hcalarm 1
```

4.22.0.3 rmon event

This command sets the RMON event entry in the RMON event MIB group.

Format `rmon event` *`event number`* `[description` *`string`*`|log|owner` *`string`*`|trap` *`community`*`]`

Mode Global Config

Parameter	Description
Event Index	An index that uniquely identifies an entry in the event table. Each such entry defines one event that is to be generated when the appropriate conditions occur. The range is 1 to 65535.
Event Description	A comment describing the event entry. The default is **alarmEvent**.
Event Type	The type of notification that the probe makes about the event. Possible values are **None**, and **Log**, **SNMP Trap**, **Log and SNMP Trap**. The default is **None**.
Event Owner	Owner string associated with the entry. The default is **monitorEvent**.
Event Community	The SNMP community specific by this octet string which is used to send an SNMP trap. The default is **public**.

Example: The following shows an example of the command.

```
(Routing) (Config)# rmon event 1 log description test
```

4.22.0.3.1 no rmon event

This command deletes the rmon event entry.

Format `no rmon event` *`event number`*

Mode Global Config

Example: The following shows an example of the command.

```
(Routing) (Config)# no rmon event 1
```

4.22.0.4 rmon collection history

This command sets the history control parameters of the RMON historyControl MIB group.

NOTE: This command is not supported on interface range. Each RMON history control collection entry can be configured on only one interface. If you try to configure on multiple interfaces, DUT displays an error.

Format `rmon collection history` ***index number*** `[buckets` ***number***`|interval` ***interval in sec***`|owner` ***string***`]`

Mode `Interface` Config

Parameter	Description
History Control Index	An index that uniquely identifies an entry in the historyControl table. Each such entry defines a set of samples at a particular interval for an interface on the device. The range is 1 to 65535.
History Control Data Source	The source interface for which historical data is collected.
History Control Buckets Requested	The requested number of discrete time intervals over which data is to be saved. The range is 1 to 65535. The default is 50.
History Control Buckets Granted	The number of discrete sampling intervals over which data shall be saved. This object is read-only. The default is 10.
History Control Interval	The interval in seconds over which the data is sampled. The range is 1 to 3600. The default is 1800.
History Control Owner	The owner string associated with the history control entry. The default is monitorHistoryControl.

Example: The following shows an example of the command.

```
(Routing) (Interface 0/1)# rmon collection history 1 buckets 10 interval 30 owner myOwner
```

Example: The following shows an example of the command.

```
(Routing) (Interface 0/1-0/10)#rmon collection history 1 buckets 10 interval 30 owner myOwner

Error: 'rmon collection history' is not supported on range of interfaces.
```

4.22.0.4.1 no rmon collection history

This command will delete the history control group entry with the specified index number.

Format `no rmon collection history` ***index number***

Mode `Interface` Config

Example: The following shows an example of the command.

```
(Routing) (Interface 0/1-0/10)# no rmon collection history 1
```

4.22.0.5 show rmon

This command displays the entries in the RMON alarm table.

Format `show rmon {alarms | alarm` ***alarm-index***`}`

Mode Privileged EXEC

Parameter	Description
Alarm Index	An index that uniquely identifies an entry in the alarm table. Each entry defines a diagnostic sample at a particular interval for an object on the device. The range is 1 to 65535.
Alarm Variable	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of integer.
Alarm Interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. The range is 1 to 2147483647. The default is 1.
Alarm Absolute Value	The value of the statistic during the last sampling period. This object is a read-only, 32-bit signed value.
Alarm Rising Threshold	The rising threshold for the sample statistics. The range is 2147483648 to 2147483647. The default is 1.
Alarm Rising Event Index	The index of the eventEntry that is used when a rising threshold is crossed. The range is 1 to 65535. The default is 1.
Alarm Falling Threshold	The falling threshold for the sample statistics. The range is 2147483648 to 2147483647. The default is 1.
Alarm Falling Event Index	The index of the eventEntry that is used when a falling threshold is crossed. The range is 1 to 65535. The default is 2.
Alarm Startup Alarm	The alarm that may be sent. Possible values are **rising, falling** or both **rising-falling**. The default is **rising-falling**.
Alarm Owner	The owner string associated with the alarm entry. The default is **monitorAlarm**.

Example: The following shows example CLI display output for the command.

```
(Routing) #show rmon alarms

Index    OID                       Owner
-------------------------------------------
1      alarmInterval.1             MibBrowser
2      alarmInterval.1             MibBrowser
```

Example: The following shows example CLI display output for the command.

```
(Routing) #show rmon alarm 1

Alarm 1
----------
OID: alarmInterval.1
Last Sample Value: 1
Interval: 1
Sample Type: absolute
Startup Alarm: rising-falling
Rising Threshold: 1
Falling Threshold: 1
Rising Event: 1
Falling Event: 2
Owner: MibBrowser
```

4.22.0.6 show rmon collection history

This command displays the entries in the RMON history control table.

Format `show rmon collection history [interfaces` *`slot/port`*`]`

Mode Privileged EXEC

Parameter	Description
History Control Index	An index that uniquely identifies an entry in the historyControl table. Each such entry defines a set of samples at a particular interval for an interface on the device. The range is 1 to 65535.
History Control Data Source	The source interface for which historical data is collected.
History Control Buckets Requested	The requested number of discrete time intervals over which data is to be saved. The range is 1 to 65535. The default is 50.
History Control Buckets Granted	The number of discrete sampling intervals over which data shall be saved. This object is read-only. The default is 10.
History Control Interval	The interval in seconds over which the data is sampled. The range is 1 to 3600. The default is 1800.
History Control Owner	The owner string associated with the history control entry. The default is monitorHistoryControl.

Example: The following shows example CLI display output for the command.

```
(Routing) #show rmon collection history

Index   Interface    Interval   Requested   Granted     Owner
                                 Samples     Samples
-------------------------------------------------------------------
1       0/1          30         10          10          myowner
2       0/1          1800       50          10          monitorHistoryControl
3       0/2          30         50          10          monitorHistoryControl
4       0/2          1800       50          10          monitorHistoryControl
5       0/3          30         50          10          monitorHistoryControl
6       0/3          1800       50          10          monitorHistoryControl
7       0/4          30         50          10          monitorHistoryControl
--More-- or (q)uit
```

Example: The following shows example CLI display output for the command.

```
(Routing) #show rmon collection history interfaces 0/1

Index   Interface    Interval   Requested   Granted     Owner
                                 Samples     Samples
-------------------------------------------------------------------
1       0/1          30         10          10          myowner
2       0/1          1800       50          10          monitorHistoryControl
```

4.22.0.7 show rmon events

This command displays the entries in the RMON event table.

Format `show rmon events`

Mode Privileged EXEC

Parameter	Description
Event Index	An index that uniquely identifies an entry in the event table. Each such entry defines one event that is to be generated when the appropriate conditions occur. The range is 1 to 65535.
Event Description	A comment describing the event entry. The default is **alarmEvent**.
Event Type	The type of notification that the probe makes about the event. Possible values are **None**, **Log**, **SNMP Trap**, **Log and SNMP Trap**. The default is **None**.

Parameter	Description
Event Owner	Owner string associated with the entry. The default is **monitorEvent**.
Event Community	The SNMP community specific by this octet string which is used to send an SNMP trap. The default is **public**.
Owner	Event owner. The owner string associated with the entry.
Last time sent	The last time over which a log or a SNMP trap message is generated.

Example: The following shows example CLI display output for the command.

```
(Routing) # show rmon events

Index  Description       Type      Community   Owner      Last time sent
-------------------------------------------------------------------------
1      test              log       public      MIB        0 days 0 h:0 m:0 s
```

4.22.0.8 show rmon history

This command displays the specified entry in the RMON history table.

Format `show rmon history` *`index`* `{errors |other |throughput | high-capacity}[period` *`seconds`*`]`

Mode Privileged EXEC

Parameter	Description
Common Fields	
Sample set	The index (identifier) for the RMON history entry within the RMON history group. Each such entry defines a set of samples at a particular interval for an interface on the device.
Owner	The owner string associated with the history control entry. The default is monitorHistoryControl.
Interface	The interface that was sampled.
Interval	The time between samples, in seconds.
Requested Samples	The number of samples (intervals) requested for the RMON history entry.
Granted Samples	The number of samples granted for the RMON history entry.
Maximum Table Size	Maximum number of entries that the history table can hold.
Output for Errors Parameter	
Time	Time at which the sample is collected, displayed as period seconds.
CRC Align	Number of CRC align errors.
Undersize Packets	Total number of undersize packets. Packets are less than 64 octets long (excluding framing bits, including FCS octets).
Oversize Packets	Total number of oversize packets. Packets are longer than 1518 octets (excluding framing bits, including FCS octets).
Fragments	Total number of fragment packets. Packets are not an integral number of octets in length or had a bad Frame Check Sequence (FCS), and are less than 64 octets in length (excluding framing bits, including FCS octets).
Jabbers	Total number of jabber packets. Packets are longer than 1518 octets (excluding framing bits, including FCS octets), and are not an integral number of octets in length or had a bad Frame Check Sequence (FCS).
Output for Others Parameter	
Time	Time at which the sample is collected, displayed as period seconds.
Dropped Collisions	Total number of dropped collisions.
Output for Throughput Parameter	

Parameter	Description
Time	Time at which the sample is collected, displayed as period seconds.
Octets	Total number of octets received on the interface.
Packets	Total number of packets received (including error packets) on the interface.
Broadcast	Total number of good broadcast packets received on the interface.
Multicast	Total number of good multicast packets received on the interface.
Util	Port utilization of the interface associated with the history index specified.
Output for High-Capacity Parameter	
Time	Time at which the sample is collected, displayed as period seconds.
Overflow Pkts	The number of times the associated packet counter has overflowed.
Pkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Overflow Octets	The number of times the associated octet counter has overflowed.
Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).

Example: The following shows example CLI display output for the command.

```
(Routing) #show rmon history 1 errors

Sample set: 1   Owner: myowner
Interface: 0/1   Interval: 30
Requested Samples: 10   Granted Samples: 10
Maximum table size: 1758

Time                  CRC Align  Undersize Oversize  Fragments  Jabbers
--------------------- ---------- --------- --------- ---------- -------
Jan 01 1970 21:41:43  0          0         0         0          0
Jan 01 1970 21:42:14  0          0         0         0          0
Jan 01 1970 21:42:44  0          0         0         0          0
Jan 01 1970 21:43:14  0          0         0         0          0
Jan 01 1970 21:43:44  0          0         0         0          0
Jan 01 1970 21:44:14  0          0         0         0          0
Jan 01 1970 21:44:45  0          0         0         0          0
Jan 01 1970 21:45:15  0          0         0         0          0
Jan 01 1970 21:45:45  0          0         0         0          0
Jan 01 1970 21:46:15  0          0         0         0          0
```

Example: The following shows example CLI display output for the command.

```
(Routing) #show rmon history 1 throughput

Sample set: 1   Owner: myowner
Interface: 0/1   Interval: 30
Requested Samples: 10   Granted Samples: 10
Maximum table size: 1758

Time                 Octets     Packets   Broadcast Multicast  Util
-------------------- ---------- --------- --------- ---------- --------
Jan 01 1970 21:41:43 0          0         0         0          1
Jan 01 1970 21:42:14 0          0         0         0          1
Jan 01 1970 21:42:44 0          0         0         0          1
Jan 01 1970 21:43:14 0          0         0         0          1
Jan 01 1970 21:43:44 0          0         0         0          1
Jan 01 1970 21:44:14 0          0         0         0          1
```

```
Jan 01 1970 21:44:45 0          0         0         0          1
Jan 01 1970 21:45:15 0          0         0         0          1
Jan 01 1970 21:45:45 0          0         0         0          1
Jan 01 1970 21:46:15 0          0         0         0          1

(Routing) #show rmon history 1 other

Sample set: 1   Owner: myowner
Interface: 0/1   Interval: 30
Requested Samples: 10   Granted Samples: 10
Maximum table size: 1758

Time                 Dropped Collisions
-------------------- ------- ----------
Jan 01 1970 21:41:43 0       0
Jan 01 1970 21:42:14 0       0
Jan 01 1970 21:42:44 0       0
Jan 01 1970 21:43:14 0       0
Jan 01 1970 21:43:44 0       0
Jan 01 1970 21:44:14 0       0
Jan 01 1970 21:44:45 0       0
Jan 01 1970 21:45:15 0       0
Jan 01 1970 21:45:45 0       0
Jan 01 1970 21:46:15 0       0
```

Example: The following shows example CLI display output for the command.

```
(Routing) #show rmon history 1 high-capacity

Sample set: 1   Owner: monitorHistoryControl
Interface: 0/1   Interval: 30
Requested Samples: 50   Granted Samples: 10
Maximum table size: 414

Time                  OverFlow Pkts    Pkts             Overflow Octets   Octets
--------------------  -------------    ----             -------------   ------

Jan 17 2017 09:12:56  0                0                0                 0
Jan 17 2017 09:13:27  0                0                0                 0
Jan 17 2017 09:13:57  0                0                0                 0
Jan 17 2017 09:14:27  0                0                0                 0
Jan 17 2017 09:14:57  0                0                0                 0
Jan 17 2017 09:15:28  0                0                0                 0
Jan 17 2017 09:15:58  0                0                0                 0
Jan 17 2017 09:16:28  0                0                0                 0
Jan 17 2017 09:16:58  0                0                0                 0
Jan 17 2017 09:17:29  0                0                0                 0
```

4.22.0.9 show rmon log

This command displays the entries in the RMON log table.

Format `show rmon log [`*`event-index`*`]`

Mode Privileged EXEC

Parameter	Description
Maximum table size	Maximum number of entries that the log table can hold.
Event	Event index for which the log is generated.
Description	A comment describing the event entry for which the log is generated.
Time	Time at which the event is generated.

Example: The following shows example CLI display output for the command.

```
(Routing) #show rmon log

Event   Description                   Time
------------------------------------------------
```

Example: The following shows example CLI display output for the command.

```
(Routing) #show rmon log 1

Maximum table size: 10

Event   Description                   Time
------------------------------------------------
```

4.22.0.10 show rmon statistics interfaces

This command displays the RMON statistics for the given interfaces.

Format `show rmon statistics interfaces` *`slot/port`*
Mode Privileged EXEC

Parameter	Description
Port	slot/port
Dropped	Total number of dropped events on the interface.
Octets	Total number of octets received on the interface.
Packets	Total number of packets received (including error packets) on the interface.
Broadcast	Total number of good broadcast packets received on the interface.
Multicast	Total number of good multicast packets received on the interface.
CRC Align Errors	Total number of packets received have a length (excluding framing bits, including FCS octets) of between 64 and 1518 octets inclusive.
Collisions	Total number of collisions on the interface.
Undersize Pkts	Total number of undersize packets. Packets are less than 64 octets long (excluding framing bits, including FCS octets).
Oversize Pkts	Total number of oversize packets. Packets are longer than 1518 octets (excluding framing bits, including FCS octets).
Fragments	Total number of fragment packets. Packets are not an integral number of octets in length or had a bad Frame Check Sequence (FCS), and are less than 64 octets in length (excluding framing bits, including FCS octets).
Jabbers	Total number of jabber packets. Packets are longer than 1518 octets (excluding framing bits, including FCS octets), and are not an integral number of octets in length or had a bad Frame Check Sequence (FCS).

Parameter	Description
64 Octets	Total number of packets which are 64 octets in length (excluding framing bits, including FCS octets).
65-127 Octets	Total number of packets which are between 65 and 127 octets in length (excluding framing bits, including FCS octets).
128-255 Octets	Total number of packets which are between 128 and 255 octets in length (excluding framing bits, including FCS octets).
256-511 Octets	Total number of packets which are between 256 and 511 octets in length (excluding framing bits, including FCS octets).
512-1023 Octets	Total number of packets which are between 512 and 1023 octets in length (excluding framing bits, including FCS octets).
1024-1518 Octets	Total number of packets which are between 1024 and 1518 octets in length (excluding framing bits, including FCS octets).
HC Overflow Pkts	Total number of times the packet counter has overflowed.
HC Overflow Octets	Total number of times the octet counter has overflowed.
HC Overflow Pkts 64 Octets	The number of times the associated 64-octet counter has overflowed.
HC Overflow Pkts 65 - 127 Octets	The number of times the associated 65–127 octet counter has overflowed.
HC Overflow Pkts 128 - 255 Octets	The number of times the associated 128–255 octet counter has overflowed.
HC Overflow Pkts 256 - 511 Octets	The number of times the associated 256–511 octet counter has overflowed.
HC Overflow Pkts 512 - 1023 Octets	The number of times the associated 512–1023 octet counter has overflowed.
HC Overflow Pkts 1024 - 1518 Octets	The number of times the associated 1024–1518 octet counter has overflowed.

Example: The following shows example CLI display output for the command.

```
(Routing) # show rmon statistics interfaces 0/1
Port: 0/1
Dropped: 0
Octets: 0  Packets: 0
Broadcast: 0  Multicast: 0
CRC Align Errors: 0  Collisions: 0
Undersize Pkts: 0  Oversize Pkts: 0
Fragments: 0  Jabbers: 0
64 Octets: 0  65 - 127 Octets: 0
128 - 255 Octets: 0  256 - 511 Octets: 0
512 - 1023 Octets: 0  1024 - 1518 Octets: 0
HC Overflow Pkts: 0  HC Pkts: 0
HC Overflow Octets: 0  HC Octets: 0
HC Overflow Pkts 64 Octets: 0  HC Pkts 64 Octets: 0
HC Overflow Pkts 65 - 127 Octets: 0  HC Pkts 65 - 127 Octets: 0
HC Overflow Pkts 128 - 255 Octets: 0  HC Pkts 128 - 255 Octets: 0
HC Overflow Pkts 256 - 511 Octets: 0  HC Pkts 256 - 511 Octets: 0
HC Overflow Pkts 512 - 1023 Octets: 0  HC Pkts 512 - 1023 Octets: 0
HC Overflow Pkts 1024 - 1518 Octets: 0  HC Pkts 1024 - 1518 Octets: 0
```

4.22.0.11 show rmon hcalarms

This command displays the entries in the RMON high-capacity alarm table.

Format `show rmon {hcalarms|hcalarm` ***alarm index***`}`

Mode Privileged EXEC

Parameter	Description
High Capacity Alarm Index	An arbitrary integer index value used to uniquely identify the high capacity alarm entry. The range is 1 to 65535.
High Capacity Alarm Variable	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of integer.
High Capacity Alarm Interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. The range is 1 to 2147483647. The default is 1.
High Capacity Alarm Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds. Possible types are **Absolute Value** or **Delta Value**. The default is **Absolute Value**.
High Capacity Alarm Absolute Value	The absolute value (that is, the unsigned value) of the hcAlarmVariable statistic during the last sampling period. The value during the current sampling period is not made available until the period is complete. This object is a 64-bit unsigned value that is Read-Only.
High Capacity Alarm Absolute Alarm Status	This object indicates the validity and sign of the data for the high capacity alarm absolute value object (hcAlarmAbsValueobject). Possible status types are **valueNotAvailable**, **valuePositive**, or **valueNegative**. The default is **valueNotAvailable**.
High Capacity Alarm Startup Alarm	High capacity alarm startup alarm that may be sent. Possible values are **rising**, **falling**, or **rising-falling**. The default is **rising-falling**.
High Capacity Alarm Rising-Threshold Absolute Value Low	The lower 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 1.
High Capacity Alarm Rising-Threshold Absolute Value High	The upper 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 0.
High Capacity Alarm Rising-Threshold Value Status	This object indicates the sign of the data for the rising threshold, as defined by the objects hcAlarmRisingThresAbsValueLow and hcAlarmRisingThresAbsValueHigh. Possible values are **valueNotAvailable**, **valuePositive**, or **valueNegative**. The default is **valuePositive**.
High Capacity Alarm Falling-Threshold Absolute Value Low	The lower 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 1.
High Capacity Alarm Falling-Threshold Absolute Value High	The upper 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 0.
High Capacity Alarm Falling-Threshold Value Status	This object indicates the sign of the data for the falling threshold, as defined by the objects hcAlarmFallingThresAbsValueLow and hcAlarmFallingThresAbsValueHigh. Possible values are **valueNotAvailable**, **valuePositive**, or **valueNegative**. The default is **valuePositive**.
High Capacity Alarm Rising Event Index	The index of the eventEntry that is used when a rising threshold is crossed. The range is 1 to 65535. The default is 1.
High Capacity Alarm Falling Event Index	The index of the eventEntry that is used when a falling threshold is crossed. The range is 1 to 65535. The default is 2.
High Capacity Alarm Failed Attempts	The number of times the associated hcAlarmVariable instance was polled on behalf of the hcAlarmEntry (while in the active state) and the value was not available. This object is a 32-bit counter value that is read-only.
High Capacity Alarm Owner	The owner string associated with the alarm entry. The default is **monitorHCAlarm**.
High Capacity Alarm Storage Type	The type of non-volatile storage configured for this entry. This object is read-only. The default is **volatile**.

Example: The following shows example CLI display output for the command.

```
(Routing) #show rmon hcalarms

Index    OID                        Owner
---------------------------------------------
1      alarmInterval.1              MibBrowser
2      alarmInterval.1              MibBrowser
```

```
(Routing) #show rmon hcalarm 1

Alarm 1
----------
OID: alarmInterval.1
Last Sample Value: 1
Interval: 1
Sample Type: absolute
Startup Alarm: rising-falling
Rising Threshold High: 0
Rising Threshold Low: 1
Rising Threshold Status: Positive
Falling Threshold High: 0
Falling Threshold Low: 1
Falling Threshold Status: Positive
Rising Event: 1
Falling Event: 2
Startup Alarm: Rising-Falling
Owner: MibBrowser
```

4.23 Buffer Statistics Tracking

Buffer Statistics Tracking (BST) provides better visibility into device buffer usage in order to aid in resource monitoring and buffer allocation.

4.23.0.1 bst enable

This command enables buffer statistics tracking (BST).

Default Disabled
Format `bst enable`
Mode Global Config

4.23.0.1.1 no bst enable

This command disables BST for the system.

Format `no bst enable`
Mode Global Config

4.23.0.2 bst device threshold

This command configures the threshold value for the entire device.

Format `bst device threshold` *`value`*
Mode Global Config

Parameter	Description
value	The threshold percentage value for the device. The value can be from 1–100.

4.23.0.2.1 no bst device threshold

This command clears the threshold value for the device.

Format `no bst device threshold`
Mode Global Config

4.23.0.3 bst egress cpu-queue attach profile

This command attaches a profile for the egress CPU queue. The threshold of the profile will be applicable for this CPU queue.

Default None
Format `bst egress cpu-queue` *`number`* `attach profile` *`profile-number`*
Mode Global Config

Parameter	Description
number	The CPU queue number.
profile-number	The profile number. The value can be from 0-5.

4.23.0.3.1 no bst egress cpu-queue attach profile

This command removes a profile from the egress CPU queue.

Format `no bst egress cpu-queue num attach profile`
Mode Global Config

4.23.0.4 bst egress cpu-queue create profile

This command configures a profile for the egress CPU queue. Once a profile is created, the CPU queues from 0-43 can attach to them.

Default None
Format `bst egress cpu-queue create profile number value`
Mode Global Config

Parameter	Description
number	The profile number.
value	The profile value.

4.23.0.4.1 no bst egress cpu-queue create profile

This command removes a profile from the egress CPU queue.

Default None
Format `no bst egress cpu-queue create profile number`
Mode Global Config

4.23.0.5 bst egress mc-queue attach profile

This command attaches the egress multicast queue resource to a previously configured profile.

Format `bst egress mc-queue number attach profile number`
Mode Interface Config

Parameter	Description
mc-queue *number*	The number of the multicast queue. The value can be from 0–7.
profile *value*	The profile to which the queue will be attached. The value can be from 0–5.

4.23.0.5.1 no bst egress mc-queue attach profile

This command detaches the egress multicast queue resource from a previously configured profile.

Format `no bst egress mc-queue` *`number`* `attach profile`
Mode Interface Config

4.23.0.6 bst egress mc-queue create profile

This command configures a profile for the egress multicast queue.

Format `bst egress mc-queue create profile` *`number value`*
Mode Global Config

Parameter	Description
number	The profile number.
value	The threshold value, as a percentage, for the given profile value.

4.23.0.6.1 no bst egress mc-queue create profile

This command removes a profile from the egress multicast queue.

Format `no bst egress mc-queue create profile` *`num`*
Mode Global Config

4.23.0.7 bst egress port-service-pool mc-shared create profile

This command configures a profile for multicast traffic on egress per port service pool.

Format `bst egress port-service-pool mc-shared create profile` *`number value`*
Mode Global Config

Parameter	Description
number	The profile number.
value	The threshold value, as a percentage, for the given profile number.

4.23.0.7.1 no bst egress port-service-pool mc-shared create profile

This command removes a profile for multicast traffic on egress per port service pool.

Format `no bst egress port-service-pool mc-shared create profile` *`number value`*
Mode Global Config

4.23.0.8 bst egress port-service-pool uc-shared create profile

This command configures a profile for unicast traffic on egress per port service pool.

Format `bst egress port-service-pool uc-shared create profile` *`number value`*
Mode Global Config

Parameter	Description
number	The profile number.
value	The threshold value, as a percentage, for the given profile number.

4.23.0.8.1 no bst egress port-service-pool uc-shared create profile

This command removes a profile for unicast traffic on egress per port service pool.

Format `no bst egress port-service-pool uc-shared create profile` *`number`*
Mode Global Config

4.23.0.9 bst egress rqe-queue threshold

This command configures the threshold value for the egress replication queue.

Format `bst egress rqe-queue` *`number`* `threshold` *`value`*
Mode Global Config

Parameter	Description
number	The replication queue number.
value	The threshold value percentage. The value can be from 1–100.

4.23.0.9.1 no bst egress rqe-queue threshold

This command clears the threshold value for the egress replication queue.

Format `bst egress rqe-queue` *`number`* `threshold`
Mode Global Config

4.23.0.10 bst egress service-pool attach profile

This command attaches the egress port service pool resource type to a previously configured profile.

Format `bst egress service-pool {uc-shared | mc-shared } attach profile` *`number`*
Mode Interface Config

Parameter	Description
number	The profile to which to attach the egress port service pool.

4.23.0.10.1 no bst egress service-pool attach profile

This command detaches the egress port service pool resource type from a previously configured profile.

Format `no bst egress service-pool {uc-shared | mc-shared } attach profile`
Mode Interface Config

4.23.0.11 bst egress service-pool mc-shared threshold

This command configures the threshold value for multicast traffic on the service pool shared by all egress ports.

Format `bst egress service-pool mc-shared threshold` *`value`*
Mode Global Config

Parameter	Description
value	The threshold percentage. The value can be from 1–100.

4.23.0.11.1 no bst egress service-pool mc-shared threshold

This command clears the threshold value for multicast traffic on the service pool shared by all egress ports.

Format `no bst egress service-pool mc-shared threshold`
Mode Global Config

4.23.0.12 bst egress service-pool uc-shared threshold

This command configures the threshold value for unicast traffic on the service pool shared by all egress ports.

Format `bst egress service-pool uc-shared threshold` *`value`*
Mode Global Config

Parameter	Description
value	The threshold value, as a percentage.

4.23.0.12.1 no bst egress service-pool uc-shared threshold

This command clears the threshold value for unicast traffic on the service pool shared by all egress ports.

Format `no bst egress service-pool uc-shared threshold`
Mode Global Config

4.23.0.13 bst egress uc-queue attach profile

This command attaches the egress unicast queue resource to a previously configured profile.

Format `bst egress uc-queue` *`number`* `attach profile` *`number`*

Mode Interface Config

Parameter	Description
uc-queue *number*	The number of the unicast queue. The value can be from 0–7.
profile *value*	The profile to which the queue will be attached. The value can be from 0–5.

4.23.0.13.1 no bst egress uc-queue attach profile

This command detaches the egress unicast queue resource from a previously configured profile.

Format `no bst egress uc-queue` *`number`* `attach profile`
Mode Interface Config

4.23.0.14 bst egress uc-queue create profile

This command configures a profile for the egress unicast queue.

Format `bst egress uc-queue create profile` *`number value`*
Mode Global Config

Parameter	Description
number	The profile number.
value	The threshold value, as a percentage, for the given profile number.

4.23.0.14.1 no bst egress uc-queue create profile

This command removes a profile for the egress unicast queue.

Format `no bst egress uc-queue create profile` *`number`*
Mode Global Config

4.23.0.15 bst ingress pg attach profile

This command attaches the resource type port priority group (PG) to a previously configured profile.

Format `bst ingress pg` *`number`* `shared attach profile` *`number`*
Mode Interface Config

Parameter	Description
pg *number*	The number of the resource group port priority group.
profile *number*	The profile to which the queue will be attached. The value can be from 0–5.

4.23.0.15.1 no bst ingress pg attach profile

This command detaches the resource type port priority group (PG) from a previously configured profile.

Format `no bst ingress pg` *`number`* `shared attach profile`
Mode Interface Config

4.23.0.16 bst ingress port-pg-shared create profile

This command configures a profile for an ingress per-port priority group shared buffer.

Format `bst ingress port-pg-shared create profile` *`number value`*
Mode Global Config

Parameter	Description
number	The profile number.
value	The threshold value, as a percentage, for the given profile number.

4.23.0.16.1 no bst ingress port-pg-shared create profile

This command removes a profile from an ingress per-port priority group shared buffer.

Format `bst ingress port-pg-shared create profile` *`number`*
Mode Global Config

4.23.0.17 bst ingress port-service-pool create profile

This command configures a profile for an ingress per port service pool buffer.

Default `none`
Format `bst ingress port-service-pool create profile` *`number value`*
Mode Global Config

Parameter	Description
number	The profile number.
value	The threshold value, as a percentage, for the given profile number.

4.23.0.17.1 no bst ingress port-service-pool create profile

This command removes the specified profile from an ingress per port service pool.

Format `bst ingress port-service-pool create profile` *`number`*
Mode Global Config

4.23.0.18 bst ingress service-pool attach profile

This command attaches the ingress port-service-pool resource type with a previously configured profile.

Format `bst ingress service-pool attach profile` *`number`*
Mode Global Config

Parameter	Description
number	The profile number to which to attach the service pool resource.

4.23.0.18.1 no bst ingress service-pool attach profile

This command detaches the resource type ingress port-service-pool from a previously configured profile.

Format `no bst ingress service-pool attach profile`
Mode Global Config

4.23.0.19 bst ingress-service-pool threshold

This command configures the threshold value for the entire ingress service pool.

Format `bst ingress-service-pool threshold` *`percentage`*
Mode Global Config

Parameter	Description
percentage	The threshold value percentage.

4.23.0.19.1 no bst ingress-service-pool threshold

This command removes the threshold value for the entire ingress service pool.

Format `no bst ingress-service-pool threshold`
Mode Global Config

4.23.0.20 bst logging

This command enables BST logging events. Threshold branch events are sent to system logging apart from storing in application buffer. Threshold branch events are stored in a circular buffer and are displayed with the `show bst events` command. These threshold branch events can also be logged into the system log buffer with this command. The logs can be seen with the `show logging buffered` command.

Format `bst logging`
Mode Global Config

4.23.0.20.1 no bst logging

This command stops writing the threshold branch events to the system log buffer.

Format `no bst logging`
Mode Global Config

4.23.0.21 show bst device

This command displays device-level MMU buffer statistics, including the device level limits and thresholds.

Format `show bst device`
Mode Privileged EXEC

Example:

```
(Routing) #show bst device

Limit of Device buffer..................... 65535
Threshold configured (in %)..................... 10
```

4.23.0.22 show bst egress cpu-queue

This command displays the configuration associated with the CPU queue size and the configured CPU queue threshold.

Format `show bst egress cpu-queue` *`number`*
Mode Privileged EXEC

Example:

```
(Routing) #show bst egress cpu-queue 1

Limit of CPU Queue buffer...................... 45
Threshold configured (in %)..................... 12
```

4.23.0.23 show bst egress port

This command displays the configuration associated with the egress unicast and multicast limits and queue number threshold.

Format `show bst egress port` *`number`* `{uc-queue | mc-queue }` *`number`*
Mode Privileged EXEC

Example:

```
(Routing) (Interface 0/1)#show bst egress port 0/1 uc-queue 0

Port      Size     Threshold
------    ----      ----------
0/1       47336    21
```

4.23.0.24 show bst egress rqe-queue

This command displays the size limits associated with the egress replication queue and threshold for either a specific queue or all queues.

Format `show bst egress rqe-queue { number | all }`

Mode Privileged EXEC

Example:

```
(Routing) (Config)#show bst egress rqe-queue all

Queue          Size        Threshold
------         ------      ----------
0              47336
1              47336       20
2              47336
3              47336
4              47336
5              47336
6              47336
7              47336
8              47336
9              47336
10             47336
```

4.23.0.25 show bst egress service-pool

This command displays the egress service pool configuration, including unicast shared limits, multicast shared limits, and configured thresholds.

Format `show bst egress service-pool`

Mode Privileged EXEC

Example:

```
(Routing) #show bst egress service-pool

Size of egress service pool UC shared buffer... 47336
Size of egress service pool MC shared buffer... 47336
```

4.23.0.26 show bst events

This command displays threshold breach events. A threshold breach event occurs when the buffer limit for a particular resource type goes above the configured threshold value. A maximum of 500 threshold breach events are shown, when a new event occurs, the old ones are replaced by the new ones. The oldest entry is replaced when a new entry is entered. The events can be cleared by the command `clear bst events`.

Format `show bst events`

Mode Privileged EXEC

4.23.0.27 show bst ingress port pg

This command displays the port and port group configuration; both the limit and configured threshold are displayed.

Format `show bst ingress port` *`port-number`* `pg` *`pg-number`*

Mode Privileged EXEC

Example:

```
(Routing) #show bst ingress port 0/1 pg 0

              PG Shared
Port         Size         Threshold
------       -----        ----------

0/1          61094        23
```

4.23.0.28 show bst ingress port service-pool

This command display the configuration associated with the port-service-pool resource for a specific port number. Both the size and configured threshold are displayed.

Format `show bst ingress port` *`number`* `service-pool`

Mode Privileged EXEC

Example:

```
(Routing) #show bst ingress port 0/1 service-pool

Port       Size         Threshold
------     ------       ---------
0/1        59869        13
```

4.23.0.29 show bst ingress service-pool

This command displays the ingress service pool configuration, including the ingress service-pool limits and the configured threshold.

Format `show bst ingress service-pool`

Mode Privileged EXEC

Example:

```
(Routing) #show bst ingress service-pool
Size of ingress service pool buffer..... 61094
```

4.23.0.30 show bst status

This command displays whether BST and BST logging are enabled or disabled globally.

Format `show bst status`

Mode Privileged EXEC

Example:

```
(Routing) #show bst status

BST..................................... Enabled.
BST event logging....................... Disabled.
```

4.23.0.31 show bst threshold

This command displays the BST threshold configuration. The port indicates the port associated with the resource. Some resources are not associated with a port (for example, DEV_GLOBAL). In such cases, the port column is left blank.

Format `show bst threshold`

Mode Privileged EXEC

Example:

```
(Routing) #show bst threshold

Stat type           Port   Resource   Profile-id   Threshold(%)
----------------    ----   --------   ----------   ------------
DEVICE                                              10
ISP                                                 25
ESP_UC_SHARED                                       20
ESP_MC_SHARED                                       19
ERQEQ                      Queue-1                  20
ECPUQ                      Queue-0    0             12
ECPUQ                      Queue-43   5             11
EMCQ                1      Queue-0    0             13
EMCQ                1      Queue-7    5             14
EPSP_MC_SHARED      1                 0             15
EPSP_UC_SHARED      1                 0             17
EUCQ                1      Queue-0    0             21
EUCQ                1      Queue-7    5             22
IPPG_SHARED         1      PG-0       0             23
IPSP                1                 0             23
EPSP_MC_SHARED      2                 5             16
EPSP_UC_SHARED      2                 5             18
IPPG_SHARED         2      PG-7       5             24
IPSP                2                 5             24
```

4.23.0.32 show bst threshold profiles

Some resource thresholds are set via profile configurations. For these resources, up to six profiles can be created. This command displays all such profiles. The first column indicates the resource. Each of the next six columns shows the associated thresholds for that particular profile number.

Format `show bst threshold profiles`

Mode Privileged EXEC

Example:

```
(Routing) #show bst threshold profiles

Threshold(%) per profile id
                  ----------------------------
```

```
Stat type           0   1   2   3   4   5
----------------  --- --- --- --- --- ---
IPPG_SHARED       23                  24
IPSP              23                  24
ECPUQ             12                  11
EMCQ              13                  14
EUCQ              21                  22
EPSP_UC_SHARED    17                  18
EPSP_MC_SHARED    15                  16
```

4.23.0.33 show mmu config device

This command displays the MMU buffer statistics configuration, including the number of service pools configured, the number of operational priority groups, and other device-level MMU information.

Format `show mmu config device`

Mode Privileged EXEC

Example:

```
(Routing) #show mmu config device

Number of Cells in the Device.................. 65535
Cell Size in the Device........................ 208
Number of Priority Groups Supported............ 8
Number of Service Pools Supported.............. 4
Number of Public Pools Supported............... 1
Number of UC queues Supported.................. 2960
Number of MC queues Supported.................. 1040
Number of CPU queues Supported................. 44
Number of RQE queues Supported................. 11
Number of UC queue groups Supported............ 8
Number of MC queue groups Supported............ 8
Number of Queue groups Supported.............. 128
```

4.23.0.34 show mmu config port

This command lists the MMU configuration settings for a specific port or all ports, including the queues, queue groups associated with the port, and the port to queue mappings.

Format `show mmu config port {`*`port`* `| all }`

Mode Privileged EXEC

4.23.0.35 clear bst events

This command clears the breach event logs.

Format `clear bst events`

Mode Privileged EXEC

4.24 Statistics Application Commands

The statistics application gives you the ability to query for statistics on port utilization, flow-based and packet reception on programmable time slots. The statistics application collects the statistics at a configurable time range. You can specify the port number(s) or a range of ports for statistics to be displayed. The configured time range applies to all ports. Detailed statistics are collected between a specified time range in date and time format. You can define the time range as having an absolute time entry and/or a periodic time. For example, you can specify the statistics to be collected and displayed between 9:00 12 NOV 2011 (START) and 21:00 12 NOV 2012 (END) or schedule it on every Mon, Wed, and Fri 9:00 (START) to 21:00 (END).

You can receive the statistics in the following ways:

- User requests through the CLI for a set of counters.
- Configuring the device to display statistics using syslog or email alert. The syslog or email alert messages are sent by the statistics application at END time.

You can configure the device to display statistics on the console. The collected statistics are presented on the console at END time.

4.24.0.1 stats group (Global Config)

This command creates a new group with the specified id or name and configures the time range and the reporting mechanism for that group.

Format `stats group` *`group {id | name}`* `timerange` *`time range name`* `reporting` *`list of reporting methods`*

Mode Global Config

Parameter	Description
group ID, name	Name of the group of statistics or its identifier to apply on the interface. The range is: 1. received 2. received-errors 3. transmitted 4. transmitted-errors 5. received-transmitted 6. port-utilization 7. congestion The default is None.
time range name	Name of the time range for the group or the flow-based rule. The range is 1 to 31 alphanumeric characters. The default is None.
list of reporting methods	Report the statistics to the configured method. The range is: **0**. none 1. console 2. syslog 3. e-mail The default is None.

Example: The following shows examples of the command.

```
(Routing) (Config)# stats group received timerange test reporting console email syslog

(Routing) (Config)# stats group received-errors timerange test reporting email syslog
```

```
(Routing) (Config)# stats group received-transmitted timerange test reporting none
```

4.24.0.1.1 no stats group

This command deletes the configured group.

Format `no stats group group {id | name}`

Mode Global Config

Example: The following shows examples of the command.

```
(Routing) (Config)# no stats group received
(Routing) (Config)# no stats group received-errors
(Routing) (Config)# no stats group received-transmitted
```

4.24.0.2 stats flow-based (Global Config)

This command configures flow based statistics rules for the given parameters over the specified time range. Only an IPv4 address is allowed as source and destination IP address.

Format `stats flow-based rule-id timerange time range name [{srcip ip-address} {dstip ip-address} {srcmac mac-address} {dstmac mac-address} {srctcpport portid} {dsttcpport portid} {srcudpport portid} {dstudpport portid}]`

Mode Global Config

Parameter	Description
rule ID	The flow-based rule ID. The range is 1 to 16. The default is None.
time range name	Name of the time range for the group or the flow-based rule. The range is 1 to 31 alphanumeric characters. The default is None.
srcip ip-address	Configure the source IP address of the rule.
dstip ip-address	Configure the destination IP address of the rule.
srcmac mac-address	Configure the source MAC address of the rule
dstmac mac-address	Configure the destination MAC address of the rule.
srctcpport portid	Configure the source TCP port for the rule.
dsttcpport portid	Configure the destination TCP port for the rule.
srcudpport portid	Configure the source UDP port for the rule.
dstudpport portid	Configure the destination UDP port for the rule.

Example: The following shows examples of the command.

```
(Routing) (Config)# stats flow-based 1 timerange test srcip 1.1.1.1 dstip 2.2.2.2 srcmac 1234 dstmac
1234 srctcpport 123 dsttcpport 123 srcudpport 123 dstudpport 123

(Routing) (Config)#stats flow-based 2 timerange test srcip 1.1.1.1 dstip 2.2.2.2 srctcpport 123
dsttcpport 123 srcudpport 123 dstudpport 123
```

4.24.0.2.1 no stats flow-based

This command deletes flow-based statistics.

Format `stats flow-based` *`rule-id`*
Mode Global Config

Example: The following shows examples of the command.

```
(Routing) (Config)# no stats flow-based 1
(Routing) (Config)# no stats flow-based 2
```

4.24.0.3 stats flow-based reporting

This command configures the reporting mechanism for all the flow-based rules configured on the system. There is no per flow-based rule reporting mechanism. Setting the reporting method as **none** resets all the reporting methods.

Format `stats flow-based reporting` *`list of reporting methods`*
Mode Global Config

Example: The following shows examples of the command.

```
(Routing) (Config)# stats flow-based reporting console email syslog
(Routing) (Config)# stats flow-based reporting email syslog
(Routing) (Config)# stats flow-based reporting none
```

4.24.0.4 stats group (Interface Config)

This command applies the group specified on an interface or interface-range.

Format `stats group {`*`group-id`* `|` *`name`*`}`
Mode Interface Config

Parameter	Description
group id, name	Specify the ID or name of the group. The ID and name associations are as follows: 1. received 2. received-errors 3. transmitted 4. transmitted-errors 5. received-transmitted 6. port-utilization 7. congestion The default is None.

Example: The following shows examples of the command.

```
(Routing) (Interface 0/1-0/10)# stats group 1
(Routing) (Interface 0/1-0/10)# stats group 2
```

4.24.0.4.1 no stats group

This command deletes the interface or interface-range from the group specified.

Format `no stats group {`*`group-id`* `|` *`name`*`}`

Mode Interface Config

Example: The following shows examples of the command.

```
(Routing) (Interface 0/1-0/10)# no stats group 1
(Routing) (Interface 0/1-0/10)# no stats group 2
```

4.24.0.5 stats flow-based (Interface Config)

This command applies the flow-based rule specified by the id on an interface or interface-range.

Format `stats flow-based` *`rule-id`*

Mode Interface Config

Parameter	Description
rule-id	The flow-based rule ID. The range is 1 to 16. The default is None.

Example: The following shows examples of the command.

```
(Routing) (Interface 0/1-0/10)# stats flow-based 1
(Routing) (Interface 0/1-0/10)# stats flow-based 2
```

4.24.0.5.1 no stats flow-based

This command deletes the interface or interface-range from the flow-based rule specified.

Format `no stats flow-based` *`rule-id`*

Mode Interface Config

4.24.0.6 show stats group

This command displays the configured time range and the interface list for the group specified and shows collected statistics for the specified time-range name on the interface list after the time-range expiry.

Format `show stats group {`*`group-id`* `|` *`name`*`}`

Mode Privileged EXEC

Parameter	Description
group id, name	Specify the ID or name of the group. The ID and name associations are as follows: 1. received 2. received-errors 3. transmitted 4. transmitted-errors 5. received-transmitted 6. port-utilization 7. congestion The default is None.

Example: The following shows example CLI display output for the command.

```
(Routing) #show stats group received

Group: received
Time Range: test
Interface List
-----------------
0/2, 0/4, lag 1

Counter ID                 Interface  Counter Value
-------------------------  ---------  ------------
Rx Total                   0/2        951600
Rx Total                   0/4        304512
Rx Total                   lag 1      0
Rx 64                      0/2        0
Rx 64                      0/4        4758
Rx 64                      lag 1      0
Rx 65to128                 0/2        0
Rx 65to128                 0/4        0
Rx 65to128                 lag 1      0
Rx 128to255                0/2        4758
Rx 128to255                0/4        0
Rx 128to255                lag 1      0
Rx 256to511                0/2        0
```

Example: The following shows example CLI display output for the command.

```
(Routing) #show stats group port-utilization

Group: port-utilization
Time Range: test
Interface List
--------------
0/2, 0/4, lag 1
Interface  Utilization (%)
---------  ---------------
0/2        0
0/4        0
lag 1      0
```

4.24.0.7 show stats flow-based

This command displays the configured time range, flow-based rule parameters and the interface list for the flow specified.

Format `show stats flow-based {`*`rule-id`* `| all}`

Mode Privileged EXEC

Parameter	Description
rule-id	The flow-based rule ID. The range is 1 to 16. The default is None.

Example: The following shows example CLI display output for the command.

```
(Routing) #show stats flow-based all

Flow based rule Id.............................. 1
```

```
Time Range..................................... test
Source IP...................................... 1.1.1.1
Source MAC..................................... 1234
Source TCP Port................................ 123
Source UDP Port................................ 123
Destination IP................................. 2.2.2.2
Destination MAC................................ 1234
Destination TCP Port........................... 123
Destination UDP Port........................... 123
Interface List
--------------
0/1 - 0/2

Interface  Hit Count
---------  ---------
0/1        100
0/2        0

Flow based rule Id............................. 2
Time Range..................................... test
Source IP...................................... 1.1.1.1
Source TCP Port................................ 123
Source UDP Port................................ 123
Destination IP................................. 2.2.2.2
Destination TCP Port........................... 123
Destination UDP Port........................... 123

Interface List
--------------
0/1 - 0/2

Interface  Hit Count
---------  ---------
0/1        100
0/2        0
```

Example: The following shows example CLI display output for the command.

```
(Routing) #show stats flow-based 2

Flow based rule Id............................. 2
Time Range..................................... test
Source IP...................................... 1.1.1.1
Source TCP Port................................ 123
Source UDP Port................................ 123
Destination IP................................. 2.2.2.2
Destination TCP Port........................... 123
Destination UDP Port........................... 123
Interface List
--------------
0/1 - 0/2

Interface  Hit Count
---------  ---------
0/1        100
0/2        0
```

4.25 In-Service Software Upgrade

The in-service software upgrade (ISSU) feature allows users to upgrade the switch software without interrupting data forwarding through the switch.

This feature is mainly targeted for top-of-rack (TOR) switches in data center Clos topologies. The goal of ISSU is to maintain Ethernet data connectivity with the servers attached to TOR switches while the TOR switch software is being upgraded. A software upgrade that requires a reboot or a kernel upgrade is not supported via ISSU.

During the ISSU process, management to the switch is disrupted. After the upgrade, users must log on to the switch again and re-authenticate to resume any switch management session.

The ISSU feature is available only on x86 platforms. As of the current EFOS release, the following features support ISSU:.

- SIM
- NIM
- L2 FDB
- DoS
- DiffServ/ACL
- MPLS
- DOT1X
- Open API Clients
- ARP
- Routing Interfaces
- RTO
- RTO6
- NDP Cache
- BGP
- VRF

The 802.1Q, DOT3AD, and DHCP client features have limited support for ISSU.

Any feature not listed above is ISSU unaware. This means that the feature does not distinguish between an ISSU restart and a normal restart. A feature that is not ISSU-aware tends to initialize afresh without the knowledge of previously active instance of the same and can cause traffic disruption during initialization.

4.25.0.1 show issu status

This command displays the current ISSU status summary.

Format	`show issu status`
Mode	Privileged EXEC

The following shows an example of the command output when ISSU succeeds:

```
(localhost) #show  issu status

Last reset reason.............................. In Service Software Upgrade
Current state.................................. ISSU completed, H/W reconciliation done
Time elapsed since ISSU initiation.............. 2 minutes 9 seconds
```

The following shows an example of the command output when ISSU fails:

```
(localhost) #show  issu status

Last reset reason.............................. In Service Software Upgrade
Current state.................................. ISSU failed
Time elapsed since ISSU initiation.............. 1 minutes 30 seconds
```

4.25.0.2 show issu status detail

This command displays ISSU event logs in chronological order.

Format `show issu status detail`

Mode Privileged EXEC

The following shows an example of the command output when ISSU succeeds :

```
(localhost) #show  issu status detail

Timestamp            State                                                    Time elapsed
-------------------- ------------------------------------------------------------ ------------
May 30 12:07:01 2017 ISSU initiated, storing application data                 0m 0s
May 30 12:07:02 2017 Application data stored                                  0m 1s
May 30 12:07:06 2017 Stopping efos                                            0m 0s
May 30 12:07:20 2017 Starting efos                                            0m 0s
May 30 12:07:27 2017 Application data restoration initiated                   0m 0s
May 30 12:08:02 2017 Application data restored                                0m 35s
May 30 12:08:02 2017 ISSU completed, hardware configuration done              0m 15s
```

The following shows an example of the command output when ISSU fails :

```
(localhost) #show  issu status detail

Timestamp            State                                                    Time elapsed
-------------------- ------------------------------------------------------------ ------------
May 30 09:06:01 2017 ISSU initiated, storing application data                 0m 0s
May 30 09:06:02 2017 Application data stored                                  0m 1s
May 30 09:06:06 2017 Stopping efos                                            0m 0s
May 30 09:06:20 2017 Starting efos                                            0m 0s
May 30 09:07:27 2017 Application data restoration initiated                   0m 0s
May 30 09:07:02 2017 ISSU failed                                              0m 15s

ISSU failure reason = Application data corrupted
```

4.26 Port and Feature Licensing Commands

Port licensing allows enabling a block of ports in a platform which already supports a higher number of ports but, by default, they are disabled. A valid license file must be purchased and installed in the system to enable such ports.

Feature licensing allows a disabled license feature to be enabled once a valid feature license file is installed.

For example, the BCM56870 IX8-B ODM platform has 48 x 25G + 8 x 100G ports. But only 16 x 25G + 2 x 100G ports are enabled by default. An additional downloadable software license is needed to enable multiples of 8 x 25G + 2 x 100G port blocks and the BroadView™ feature.

4.26.0.1 license clear

Use this command to clear/delete all licenses or a specific license stored at a particular index in persistent storage.

Format `license clear {`*`index`* `| all}`
Mode Privileged Exec

Example: The following shows an example of the command.

```
(localhost) #license clear ?

<1-16>                  Enter license file number/index
all                     Remove all license files

(dhcp-10-130-84-117) #license clear 8

Are you sure you want to remove license file(s)? (y/n) y


License file with index 8 is removed.


(dhcp-10-130-84-117) #license clear all

Are you sure you want to remove license file(s)? (y/n) y


All license files are removed.
```

4.26.0.2 debug license

Use this command to enable license debugging.

Format `debug license`
Mode Privileged Exec

Example: The following shows an example of the command.

```
(localhost) #debug license
```

4.26.0.2.1 no debug license

Use this command to disable license debugging.

Format `no debug license`
Mode Privileged Exec

Example: The following shows an example of the command.

```
(localhost) #no debug license
```

4.26.0.3 show license file

Use this command to display details of license file contents such as serial number, model, features, ports, license key, and so on.

Format `show license file` *`index`*
Mode Privileged Exec

Example: The following shows an example of the command.

```
(localhost) #show license file ?

<index>                 Enter license file number/index


(localhost) #show  license file 1

License Index.................................. 1
License File Version........................... 1.0
License Key.................................... 102D-V79T-0001-104F
Serial Number.................................. QTFCU38290010
Model.......................................... IX8-B
Description.................................... Instru license
Downlink Ports................................. 8
Uplink Ports................................... 2
Features....................................... BROADVIEW
```

4.26.0.4 show license

Use this command to display the summary of all license files and detail status of a specific license file. The summary status is displayed in tabular format.

Format `show license [`*`index`*`]`
Mode Privileged Exec

Example: The following shows an example of the command.

```
(localhost) #show license ?
<cr>                    Press enter to execute the command.
|                       Output filter options.
<index>                 Enter license file number/index
features                Display License features.
file                    Shows license file contents
```

```
(localhost) #show  license

Reboot needed..................................... Yes
Number of active licenses......................... 2
Total Downlink Ports enabled...................... 8
Total Uplink Ports enabled........................ 2


License Index  License Type              Status
-------------- ------------------------- ----------------------------------
1              Port and Feature          License applied
2              Feature                   License applied
6              Port                      License valid but not applied



(localhost) #show  license 2

License Index..................................... 2
License Type...................................... Feature
License Status.................................... License applied
Status Details.................................... Reboot required to apply license file with index 6
```

4.26.0.5 show license features

Use the `show license features` command to display the licensable capabilities on the switch, including their status (such as, Enabled/Disabled), and corresponding license index. If the `License Index` field shows a valid index, but the feature status is shown as Disabled, the user is expected to check the license status using the `show license [index]` command.

Format `show license features`

Mode Privileged Exec

Example: The following shows an example of the command.

```
(localhost) #show license features

Feature           Status    License Index
----------------- --------- --------------
BROADVIEW         Enabled   2
```

Chapter 5: Switching Commands

This section describes the switching commands available in the EFOS CLI.

NOTE: The commands in this chapter are in one of three functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Clear commands clear some or all of the settings to factory defaults.

5.1 Port Configuration Commands

This section describes the commands you use to view and configure port settings.

5.1.0.1 interface

This command gives you access to the Interface Config mode, which allows you to enable or modify the operation of an interface (port). You can also specify a range of ports to configure at the same time by specifying the starting *slot/port* and ending *slot/port*, separated by a hyphen.

Format `interface {slot/port | slot/port(startrange)-slot/port(endrange)}`

Mode Global Config

Example: The following example enters Interface Config mode for port 0/1:

```
(Routing) #configure
(Routing) (config)#interface 0/1
(Routing) (interface 0/1)#
```

Example: The following example enters Interface Config mode for ports 0/1 through 0/4:

```
(Routing)#configure
(Routing) (config)#interface 0/1-0/4
(Routing) (interface 0/1-0/4)#
```

5.1.0.2 auto-negotiate

This command enables automatic negotiation on a port or range of ports.

Default enabled

Format `auto-negotiate`

Mode Interface Config

5.1.0.2.1 no auto-negotiate

This command disables automatic negotiation on a port.

NOTE: Automatic sensing is disabled when automatic negotiation is disabled.

Format `no auto-negotiate`

Mode Interface Config

5.1.0.3 auto-negotiate all

This command enables automatic negotiation on all ports.

Default enabled

Format `auto-negotiate all`

Mode Global Config

5.1.0.3.1 no auto-negotiate all

This command disables automatic negotiation on all ports.

Format `no auto-negotiate all`

Mode Global Config

5.1.0.4 description

Use this command to create an alpha-numeric description of an interface or range of interfaces.

Format `description` *`description`*

Mode Interface Config

5.1.0.5 fec

Use this command to enable forward error correction (FEC) for an interface in adherence with IEEE requirements (IEEE 802.3bj -CL 91). This command is available only on interfaces operating at 100G, 50G and 25G speeds. If you change the speed of an interface to a speed at which FEC is not supported, FEC is automatically disabled on the interface. When the interface returns to the speed that supports FEC, EFOS retains the original FEC configuration and re-applies it on the interface.

Format `fec {100G | 50G | 25G}`

Mode Interface Config

5.1.0.5.1 no fec

Use this command to disable FEC on an interface.

Format `no fec`

Mode Interface Config

5.1.0.6 media-type

Use this command to change between fiber and copper mode on the Combo port.

- Combo Port: A port or an interface that can operate in either copper or in fiber mode.
- Copper and Fiber port: A port that uses copper a medium for communication (for example, RJ45 ports). A fiber port uses the fiber optics as a medium for communication (for example, example SFP ports).

Default	Auto-select, SFP preferred
Format	`media-type {auto-select | rj45 | sfp }`
Mode	Interface Config

The following modes are supported by the `media-type` command.

- Auto-select, SFP preferred: The medium is selected automatically based on the physical medium presence. However, when both the fiber and copper links are connected, the fiber link takes precedence and the fiber link is up.
- Auto-select, RJ45 preferred: The medium is selected automatically based on the physical medium presence. However, when both the fiber and copper links are connected, the copper link takes precedence and the copper link is up.
- SFP: Only the fiber medium works. The copper medium is always down.
- RJ45: Only the copper medium works. The fiber medium is always down.

5.1.0.6.1 no media-type

Use this command to revert the `media-type` configuration and configure the default value on the interface.

Format	`no media-type`
Mode	Interface Config

5.1.0.7 mtu

Use the `mtu` command to set the maximum transmission unit (MTU) size, in bytes, for frames that ingress or egress the interface. You can use the `mtu` command to configure jumbo frame support for physical and port-channel (LAG) interfaces. For the standard EFOS implementation, the MTU size is a valid integer between 1504–12270 for tagged packets and a valid integer between 1500–12270 for untagged packets.

NOTE: To receive and process packets, the Ethernet MTU must include any extra bytes that Layer-2 headers might require. To configure the IP MTU size, which is the maximum size of the IP packet (IP Header + IP payload), see Section 7.2.0.18, ip mtu.

Default	1500 (untagged)
Format	`mtu` *`1500–12270`*
Mode	Interface Config

5.1.0.7.1 no mtu

This command sets the default MTU size (in bytes) for the interface.

Format	`no mtu`
Mode	Interface Config

5.1.0.8 shutdown

This command disables a port or range of ports.

NOTE: You can use the `shutdown` command on physical and port-channel (LAG) interfaces, but not on VLAN routing interfaces.

Default	enabled
Format	`shutdown`
Mode	Interface Config

5.1.0.8.1 no shutdown

This command enables a port.

Format	`no shutdown`
Mode	Interface Config

5.1.0.9 shutdown all

This command disables all ports.

NOTE: You can use the `shutdown all` command on physical and port-channel (LAG) interfaces, but not on VLAN routing interfaces.

Default	enabled
Format	`shutdown all`
Mode	Global Config

5.1.0.9.1 no shutdown all

This command enables all ports.

Format	`no shutdown all`
Mode	Global Config

5.1.0.10 speed

Use this command to enable or disable auto-negotiation and set the speed that will be advertised by that port. The duplex parameter allows you to set the advertised speed for both half as well as full duplex mode.

Use the `auto` keyword to enable auto-negotiation on the port. Use the command without the `auto` keyword to ensure auto-negotiation is disabled and to set the port speed and mode according to the command values. If auto-negotiation is disabled, the speed and duplex mode must be set.

Default	Auto-negotiation is enabled.

Format	`speed auto {10|100|1000|2.5G|10G|20G|25G|40G|50G|100G} [10|100|1000|2.5G|10G|20G|25G|40G|50G|100G] [half-duplex|full-duplex]`
	
	`speed {10|100|1000|2.5G|10G|20G|25G|40G|50G|100G} {half-duplex|full-duplex}`

Mode	Interface Config

5.1.0.11 speed all

This command sets the speed and duplex setting for all interfaces if auto-negotiation is disabled. If auto-negotiation is enabled, an error message is returned. Use the `no auto-negotiate` command to disable.'

Default Auto-negotiation is enabled. Adv. is 10h, 10f, 100h, 100f, 1000f.

Format `speed all {100 | 10} {half-duplex | full-duplex}`

Mode Global Config

5.1.0.12 show interface fec

Use this command to display the FEC status for the specified interface or for all interfaces, if no interface is specified.

Format `show interface [slot/port] fec`

Mode Privileged EXEC

The following information is displayed for the command.

Term	Definition
Interface	The interface associated with the rest of the information in the row.
Configured FEC Status	The FEC status for the interface.

Example: The following command shows the command output:

```
(Switching) (Config)#show interface 0/85 fec

Interface     Configured FEC Status
------------------------------------
0/85               fec 100G

(Switching) (Config)#show interface fec

Interface     Configured FEC Status
------------------------------------
0/65               fec 25G
0/66               fec 25G
0/67               fec 25G
0/68               fec 25G
0/69               fec 25G
0/70               fec 25G
0/71               fec 25G
```

5.1.0.13 show interface media-type

Use this command to display the media-type configuration of the interface.

Format `show interface media-type`

Mode Privileged EXEC

The following information is displayed for the command.

Term	Definition
Port	The slot/port.
Configured Media Type	The media type for the interface. auto-select—The media type is automatically selected. The preferred media type is displayed. RJ45—RJ45 SFP—SFP
Active	Displays the current operational state of the combo port.

Example: The following command shows the command output:

```
(Routing) #show interface media-type

Port       Configured Media Type         Active
---------  ----------------------------  ------
0/21       SFP                           RJ45
0/22       auto-select, SFP preferred    Down
0/23       auto-select, SFP preferred    RJ45
0/24       auto-select, SFP preferred    Down
```

5.1.0.14 show port

This command displays port information.

Format `show port {`*`intf-range`* `| all}`

Mode Privileged EXEC

Parameter	Definition
Interface	slot/port
Type	If not blank, this field indicates that this port is a special type of port. The possible values are: ■ **Mirror** — this port is a monitoring port. ■ **PC Mbr**— this port is a member of a port-channel (LAG). ■ **Probe** — this port is a probe port.
Admin Mode	The Port control administration state. The port must be enabled in order for it to be allowed into the network. May be enabled or disabled. The factory default is enabled.
Physical Mode	The desired port speed and duplex mode. If auto-negotiation support is selected, then the duplex mode and speed is set from the auto-negotiation process. Note that the maximum capability of the port (full duplex -100M) is advertised. Otherwise, this object determines the port's duplex mode and transmission rate. The factory default is Auto.
Physical Status	The port speed and duplex mode.
Link Status	The Link is up or down.
Link Trap	This object determines whether or not to send a trap when link status changes. The factory default is enabled.
LACP Mode	LACP is enabled or disabled on this port.

Example: The following command shows an example of the command output for all ports.

```
(Routing) #show port all

                Admin     Physical   Physical   Link   Link    LACP   Actor
Intf      Type  Mode      Mode       Status     Status Trap    Mode   Timeout
--------- ------ --------- ---------- ---------- ------ ------- ------ --------
```

```
0/1               Enable    Auto       100 Full   Up     Enable  Enable long
0/2               Enable    Auto       100 Full   Up     Enable  Enable long
0/3               Enable    Auto                  Down   Enable  Enable long
0/4               Enable    Auto       100 Full   Up     Enable  Enable long
0/5               Enable    Auto       100 Full   Up     Enable  Enable long
0/6               Enable    Auto       100 Full   Up     Enable  Enable long
0/7               Enable    Auto       100 Full   Up     Enable  Enable long
0/8               Enable    Auto       100 Full   Up     Enable  Enable long
1/1               Enable                          Down   Disable N/A    N/A
1/2               Enable                          Down   Disable N/A    N/A
1/3               Enable                          Down   Disable N/A    N/A
1/4               Enable                          Down   Disable N/A    N/A
1/5               Enable                          Down   Disable N/A    N/A
1/6               Enable                          Down   Disable N/A    N/A
```

Example: The following command shows an example of the command output for a range of ports.

```
(Routing) #show port 0/1-1/6

                  Admin     Physical   Physical   Link   Link    LACP   Actor
Intf      Type    Mode      Mode       Status     Status Trap    Mode   Timeout
--------- ------ --------- ---------- ---------- ------ ------- ------ --------
0/1               Enable    Auto       100 Full   Up     Enable  Enable long
0/2               Enable    Auto       100 Full   Up     Enable  Enable long
0/3               Enable    Auto                  Down   Enable  Enable long
0/4               Enable    Auto       100 Full   Up     Enable  Enable long
0/5               Enable    Auto       100 Full   Up     Enable  Enable long
0/6               Enable    Auto       100 Full   Up     Enable  Enable long
0/7               Enable    Auto       100 Full   Up     Enable  Enable long
0/8               Enable    Auto       100 Full   Up     Enable  Enable long
1/1               Enable                          Down   Disable N/A    N/A
1/2               Enable                          Down   Disable N/A    N/A
1/3               Enable                          Down   Disable N/A    N/A
1/4               Enable                          Down   Disable N/A    N/A
1/5               Enable                          Down   Disable N/A    N/A
1/6               Enable                          Down   Disable N/A    N/A
```

5.1.0.15 show port description

This command displays the interface description.

Format `show port description {`*`slot/port`* | *`lag lag-id`*`}`

Mode Privileged EXEC

Parameter	Definition
Interface	The slot/port or LAG with the information to view.
ifIndex	The interface index number associated with the port.
Description	The alpha-numeric description of the interface created by the Section 5.1.0.4, description command.
MAC address	The MAC address of the port. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Bit Offset Val	The bit offset value.

Example: The following shows example CLI display output for the command.

```
(Switching) #show port description 0/1
```

```
Interface..........0/1
ifIndex............1
Description.........
MAC address.........00:10:18:82:0C:10
Bit Offset Val......1
```

5.1.0.16 hardware profile portmode

Use the `hardware profile portmode` command to configure a 40G QSFP port in either 4x10G mode or 1x40G mode or a 100G QSFP port in either 1x100G, 2x50G, or 4x25G mode.

This command can only be executed on interfaces that support the expandable ports feature. Entering the command on any other type of interface will give an error.

NOTE: This command does not operate in interface range mode.

Default The default mode for QSFP ports is platform-specific.

Format `hardware profile portmode` *mode*

Mode Interface Config

Parameter	Definition
mode	The available modes depend on the platform. Possible modes are: ■ 1x40g: Configure the port as a single 40G port using four lanes. ■ 4x10g: Configure the port as four 10G ports, each on a separate lane. This mode requires the use of a suitable 4x10G to 1x40G pigtail cable. ■ 1x100g: Configure the port as a single 100G port using four lanes. The 100G ports may be reconfigured as 40G ports using the `interface speed` command. ■ 2x50g: Configure the port as two 50G ports, each using two lanes. This mode requires the use of a suitable 1x100G to 2x50G pigtail cable ■ 4x25g: Configure the port as a four 25G ports, each on a separate lane. This mode requires the use of a suitable 4x25G to 1x100G pigtail cable. The 4x25G ports may be reconfigured as 4x10G ports with the `interface speed` command.

5.1.0.16.1 no hardware profile portmode

Use the no form of the `hardware profile portmode` command to return the port to the default mode.

Format `no hardware profile portmode`

Mode Interface Config

5.1.0.17 show interfaces hardware profile

Use the `show interfaces hardware profile` command in Privileged EXEC mode to display the hardware profile information for the ports that support the expandable feature. The command displays the 40G interface and the corresponding 10G interfaces or the 100G interface and the corresponding 25G or 50G interfaces. Because any hardware profile configuration is only effective with the next boot of the switch, the configured mode may be different than the operational mode of the interface. Therefore, this command also displays the configured mode and the operational mode of the interface.

The user can optionally specify an interface or all expandable interfaces to display.

Format `show interfaces hardware profile [`*`interface`*`]`

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

NOTE: The port mappings can vary from platform to platform. This example is only for illustration, and may not represent the actual port mappings on all platforms.

```
(Routing) #show interfaces hardware profile
                              Configured  Oper
40G Interface  10G Interfaces  Mode        Mode
-------------  -------------- ----------  -------
0/1           0/17-20         1x40G       4x10G
0/2           0/21-24        1x40G       1x40G

(Routing) #show interfaces hardware profile 0/1
                              Configured  Oper
40G Interface  10G Interfaces  Mode        Mode
-------------  --------------  ----------  -------
0/1              0/17-20       1x40G       4x10G
```

For platforms that support expandable ports (high density ports that can be split into multiple lane modes), additional information is displayed in the output.

```
(Routing) #show interfaces hardware profile

100G/40G       Configured  Operating   Expandable  Expanded
Interface      Mode        Mode        Option(s)   Interfaces
-------------------------------------------------------------
0/81           1x40G       1x40G       4x10G       0/93-96
0/82           1x40G       1x40G       4x10G       0/97-100
0/83           1x40G       1x40G       4x10G       0/101-104
0/84           1x40G       1x40G       4x10G       0/105-108
0/85           1x100G      1x100G      4x25G       0/109-112
                                       2x50G       0/125-126
0/86           1x100G      1x100G      4x25G       0/113-116
                                       2x50G       0/127-128
0/87           1x100G      1x100G      4x25G       0/117-120
                                       2x50G       0/129-130
0/88           1x100G      1x100G      4x25G       0/121-124
                                       2x50G       0/131-132
(Routing) #show interfaces hardware profile 0/85

100G/40G       Configured  Operating   Expandable  Expanded
Interface      Mode        Mode        Option(s)   Interfaces
-------------------------------------------------------------
0/85           4x25G       4x25G       4x25G       0/109-112
                                       2x50G       0/125-126
```

5.2 Spanning Tree Protocol Commands

This section describes the commands you use to configure Spanning Tree Protocol (STP). STP helps prevent network loops, duplicate messages, and network instability.

NOTE: Note the following:

- STP is enabled on the switch and on all ports and LAGs by default.
- If STP is disabled, the system does not forward BPDU messages.

5.2.0.1 spanning-tree

This command sets the spanning-tree operational mode to enabled.

Default	enabled
Format	`spanning-tree`
Mode	Global Config

5.2.0.1.1 no spanning-tree

This command sets the spanning-tree operational mode to disabled. While disabled, the spanning-tree configuration is retained and can be changed, but is not activated.

Format	`no spanning-tree`
Mode	Global Config

5.2.0.2 spanning-tree auto-edge

Use this command to allow the interface to become an edge port if it does not receive any BPDUs within a given amount of time.

Default	Enabled
Format	`spanning-tree auto-edge`
Mode	Interface Config

5.2.0.2.1 no spanning-tree auto-edge

This command resets the auto-edge status of the port to the default value.

Format	`no spanning-tree auto-edge`
Mode	Interface Config

5.2.0.3 spanning-tree backbonefast

Use this command to enable the detection of indirect link failures and accelerate spanning tree convergence on PVSTP configured switches.

Backbonefast accelerates finding an alternate path when an indirect link to the root port goes down.

Backbonefast can be configured even if the switch is configured for MST(RSTP) or PVST mode. It only has an effect when the switch is configured for the PVST mode.

If a backbonefast-enabled switch receives an inferior BPDU from its designated switch on a root or blocked port, it sets the maximum aging time on the interfaces on which it received the inferior BPDU if there are alternate paths to the designated switch. This allows a blocked port to immediately move to the listening state where the port can be transitioned to the forwarding state in the normal manner.

On receipt of an inferior BPDU from a designated bridge, backbonefast enabled switches send a Root Link Query (RLQ) request to all non-designated ports except the port from which it received the inferior BPDU. This check validates that the switch can receive packets from the root on ports where it expects to receive BPDUs. The port from which the original inferior BPDU was received is excluded because it has already encountered a failure. Designated ports are excluded as they do not lead to the root.

On receipt of an RLQ response, if the answer is negative, the receiving port has lost connection to the root and its BPDU is immediately aged out. If all nondesignated ports have already received a negative answer, the whole bridge has lost the root and can start the STP calculation from scratch.

If the answer confirms the switch can access the root bridge on a port, it can immediately age out the port on which it initially received the inferior BPDU.

A bridge that sends an RLQ puts its bridge ID in the PDU. This ensures that it does not flood the response on designated ports.

A bridge that receives an RLQ and has connectivity to the root forwards the query toward the root through its root port.

A bridge that receives a RLQ request and does not have connectivity to the root (switch bridge ID is different from the root bridge ID in the query) or is the root bridge immediately answers the query with its root bridge ID.

RLQ responses are flooded on designated ports.

Default	NA
Format	`spanning-tree backbonefast`
Mode	Global Config

5.2.0.3.1 no spanning-tree backbonefast

This command disables backbonefast.

NOTE: Per VLAN Rapid Spanning Tree Protocol (PVRSTP) embeds support for FastBackbone and FastUplink. Even if FastUplink and FastBackbone are configured, they are effective only in PVSTP mode.

Format	`no spanning-tree backbonefast`
Mode	Global Config

5.2.0.4 spanning-tree cost

Use this command to configure the external path cost for port used by a MST instance. When the `auto` keyword is used, the path cost from the port to the root bridge is automatically determined by the speed of the interface. To configure the cost manually, specify a *`cost`* value from 1–200000000.

Default	auto
Format	`spanning-tree cost {`*`cost`* `| auto}`
Mode	Interface Config

5.2.0.4.1 no spanning-tree cost

This command resets the auto-edge status of the port to the default value.

Format	`no spanning-tree auto-edge`
Mode	Interface Config

5.2.0.5 spanning-tree bpdufilter

Use this command to enable BPDU Filter on an interface or range of interfaces.

Default	disabled
Format	`spanning-tree bpdufilter`
Mode	Interface Config

5.2.0.5.1 no spanning-tree bpdufilter

Use this command to disable BPDU Filter on the interface or range of interfaces.

Default	disabled
Format	`no spanning-tree bpdufilter`
Mode	Interface Config

5.2.0.6 spanning-tree bpdufilter default

Use this command to enable BPDU Filter on all the edge port interfaces.

Default	disabled
Format	`spanning-tree bpdufilter`
Mode	Global Config

5.2.0.6.1 no spanning-tree bpdufilter default

Use this command to disable BPDU Filter on all the edge port interfaces.

Default	disabled
Format	`no spanning-tree bpdufilter default`
Mode	Global Config

5.2.0.7 spanning-tree bpduflood

Use this command to enable BPDU Flood on an interface or range of interfaces.

Default disabled
Format `spanning-tree bpduflood`
Mode Interface Config

5.2.0.7.1 no spanning-tree bpduflood

Use this command to disable BPDU Flood on the interface or range of interfaces.

Default disabled
Format `no spanning-tree bpduflood`
Mode Interface Config

5.2.0.8 spanning-tree bpduguard

Use this command to enable BPDU Guard on the switch.

Default disabled
Format `spanning-tree bpduguard`
Mode Global Config

5.2.0.8.1 no spanning-tree bpduguard

Use this command to disable BPDU Guard on the switch.

Default disabled
Format `no spanning-tree bpduguard`
Mode Global Config

5.2.0.9 spanning-tree bpdumigrationcheck

Use this command to force a transmission of rapid spanning tree (RSTP) and multiple spanning tree (MSTP) BPDUs. Use the *`slot/port`* parameter to transmit a BPDU from a specified interface, or use the `all` keyword to transmit BPDUs from all interfaces. This command forces the BPDU transmission when you execute it, so the command does not change the system configuration or have a “no” version.

Format `spanning-tree bpdumigrationcheck {`*`slot/port`* `| all}`
Mode Global Config

5.2.0.10 spanning-tree configuration name

This command sets the Configuration Identifier Name for use in identifying the configuration that this switch is currently using. The `name` is a string of up to 32 characters.

Default base MAC address in hexadecimal notation
Format `spanning-tree configuration name` *`name`*
Mode Global Config

5.2.0.10.1 no spanning-tree configuration name

This command resets the Configuration Identifier Name to its default.

Format `no spanning-tree configuration name`
Mode Global Config

5.2.0.11 spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using. The Configuration Identifier Revision Level is a number in the range of 0 to 65535.

Default 0
Format `spanning-tree configuration revision` *`0-65535`*
Mode Global Config

5.2.0.11.1 no spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using to the default value.

Format `no spanning-tree configuration revision`
Mode Global Config

5.2.0.12 spanning-tree edgeport

This command specifies that an interface (or range of interfaces) is an Edge Port within the common and internal spanning tree. This allows this port to transition to Forwarding State without delay.

Format `spanning-tree edgeport`
Mode Interface Config

5.2.0.12.1 no spanning-tree edgeport

This command specifies that this port is not an Edge Port within the common and internal spanning tree.

Format `no spanning-tree edgeport`
Mode Interface Config

5.2.0.13 spanning-tree forward-time

This command sets the Bridge Forward Delay parameter to a new value for the common and internal spanning tree. The forward-time value is in seconds within a range of 4 to 30, with the value being greater than or equal to “(Bridge Max Age / 2) + 1”.

Default 15
Format `spanning-tree forward-time` *`4-30`*
Mode Global Config

5.2.0.13.1 no spanning-tree forward-time

This command sets the Bridge Forward Delay parameter for the common and internal spanning tree to the default value.

Format `no spanning-tree forward-time`
Mode Global Config

5.2.0.14 spanning-tree guard

This command selects whether loop guard or root guard is enabled on an interface or range of interfaces. If neither is enabled, then the port operates in accordance with the multiple spanning tree protocol.

Default none
Format `spanning-tree guard {none | root | loop}`
Mode Interface Config

5.2.0.14.1 no spanning-tree guard

This command disables loop guard or root guard on the interface.

Format `no spanning-tree guard`
Mode Interface Config

5.2.0.15 spanning-tree max-age

This command sets the Bridge Max Age parameter to a new value for the common and internal spanning tree. The max-age value is in seconds within a range of 6 to 40, with the value being less than or equal to *2 x (Bridge Forward Delay - 1)*.

Default 20
Format `spanning-tree max-age` *`6-40`*
Mode Global Config

5.2.0.15.1 no spanning-tree max-age

This command sets the Bridge Max Age parameter for the common and internal spanning tree to the default value.

Format `no spanning-tree max-age`
Mode Global Config

5.2.0.16 spanning-tree max-hops

This command sets the MSTP Max Hops parameter to a new value for the common and internal spanning tree. The max-hops value is a range from 1 to 127.

Default 20
Format `spanning-tree max-hops` *`1-127`*
Mode Global Config

5.2.0.16.1 no spanning-tree max-hops

This command sets the Bridge Max Hops parameter for the common and internal spanning tree to the default value.

Format	`no spanning-tree max-hops`
Mode	Global Config

5.2.0.17 spanning-tree mode

This command configures global spanning tree mode per VLAN spanning tree, Rapid-PVST, MST, RSTP or STP. Only one of MSTP (RSTP), PVST or RPVST can be enabled on a switch.

When PVSTP or rapid PVSTP (PVRSTP) is enabled, MSTP/RSTP/STP is operationally disabled. To reenable MSTP/RSTP/STP, disable PVSTP/RVPVSTP. By default, EFOS has MSTP enabled. In PVSTP or PVRSTP mode, BPDUs contain per-VLAN information instead of the common spanning-tree information (MST/RSTP).

PVSTP maintains independent spanning tree information about each configured VLAN. PVSTP uses IEEE 802.1Q trunking and allows a trunked VLAN to maintain blocked or forwarding state per port on a per-VLAN basis. This allows a trunk port to be forwarded on some VLANs and blocked on other VLANs.

PVRSTP is based on the IEEE 8012.1w standard. It supports fast convergence IEEE 802.1D. RVPVSTP is compatible with IEEE 802.1D spanning tree. PVRSTP sends BPDUs on all ports, instead of only the root bridge sending BPDUs, and supports the discarding, learning, and forwarding states.

When the mode is changed to PVRSTP, version 0 STP BPDUs are no longer transmitted and version 2 PVRSTP BPDUs that carry per-VLAN information are transmitted on the VLANs enabled for spanning-tree. If a version 0 BPDU is seen, RVPVSTP reverts to sending version 0 BPDUs.

Per VLAN Rapid Spanning Tree Protocol (PVRSTP) embeds support for PVSTP FastBackbone and FastUplink. There is no provision to enable or disable these features in PVRSTP.

Default	MST
Format	`spanning-tree mode {mst | pvst | rapid-pvst | stp | rstp }`
Mode	Global Config

5.2.0.17.1 no spanning-tree mode

This command globally configures the switch to the default EFOS spanning-tree mode, MSTP.

Format	`no spanning-tree mode`
Mode	Global Configuration

5.2.0.18 spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance or in the common and internal spanning tree. If you specify an `mstid` parameter that corresponds to an existing multiple spanning tree instance, the configurations are done for that multiple spanning tree instance. If you specify 0 (defined as the default CIST ID) as the `mstid`, the configurations are done for the common and internal spanning tree instance.

If you specify the **cost** option, the command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the `mstid` parameter. You can set the path cost as a number in the range of 1 to 200000000 or **auto**. If you select **auto** the path cost value is set based on Link Speed.

If you specify the **port-priority** option, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the `mstid` parameter. The port-priority value is a number in the range of 0 to 240 in increments of 16.

Default
- cost—auto
- port-priority—128

Format `spanning-tree mst` ***mstid*** `{{cost` ***1-200000000*** `| auto} | port-priority` ***0-240***`}`

Mode Interface Config

5.2.0.18.1 no spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance, or in the common and internal spanning tree to the respective default values. If you specify an `mstid` parameter that corresponds to an existing multiple spanning tree instance, you are configuring that multiple spanning tree instance. If you specify 0 (defined as the default CIST ID) as the `mstid`, you are configuring the common and internal spanning tree instance.

If the you specify **cost**, this command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the `mstid` parameter, to the default value, i.e., a path cost value based on the Link Speed.

If you specify **port-priority**, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the `mstid` parameter, to the default value.

Format `no spanning-tree mst` ***mstid*** `{cost | port-priority}`

Mode Interface Config

5.2.0.19 spanning-tree mst instance

This command adds a multiple spanning tree instance to the switch. The parameter `mstid` is a number within a range of 1 to 4094, that corresponds to the new instance ID to be added. The maximum number of multiple instances supported by the switch is 4.

Default none

Format `spanning-tree mst instance` ***mstid***

Mode Global Config

5.2.0.19.1 no spanning-tree mst instance

This command removes a multiple spanning tree instance from the switch and reallocates all VLANs allocated to the deleted instance to the common and internal spanning tree. The parameter `mstid` is a number that corresponds to the desired existing multiple spanning tree instance to be removed.

Format `no spanning-tree mst instance` ***mstid***

Mode Global Config

5.2.0.20 spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance. The parameter `mstid` is a number that corresponds to the desired existing multiple spanning tree instance. The priority value is a number within a range of 0 to 61440 in increments of 4096.

If you specify 0 (defined as the default CIST ID) as the `mstid`, this command sets the Bridge Priority parameter to a new value for the common and internal spanning tree. The bridge priority value is a number within a range of 0 to 61440. The twelve least significant bits are masked according to the 802.1s specification. This causes the priority to be rounded down to the next lower valid priority.

Default 32768

Format `spanning-tree mst priority` ***mstid 0-61440***

Mode Global Config

5.2.0.20.1 no spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance to the default value. The parameter `mstid` is a number that corresponds to the desired existing multiple spanning tree instance.

If 0 (defined as the default CIST ID) is passed as the `mstid`, this command sets the Bridge Priority parameter for the common and internal spanning tree to the default value.

Format `no spanning-tree mst priority` ***mstid***

Mode Global Config

5.2.0.21 spanning-tree mst vlan

This command adds an association between a multiple spanning tree instance and one or more VLANs so that the VLAN(s) are no longer associated with the common and internal spanning tree. The parameter `mstid` is a number that corresponds to the desired existing multiple spanning tree instance. The `vlanid` can be specified as a single VLAN, a list, or a range of values. To specify a list of VLANs, enter a list of VLAN IDs, each separated by a comma with no spaces in between. To specify a range of VLANs, separate the beginning and ending VLAN ID with a dash (-). The VLAN IDs may or may not exist in the system.

Format `spanning-tree mst vlan` ***mstid vlanid***

Mode Global Config

5.2.0.21.1 no spanning-tree mst vlan

This command removes an association between a multiple spanning tree instance and one or more VLANs so that the VLAN(s) are again associated with the common and internal spanning tree.

Format `no spanning-tree mst vlan` ***mstid vlanid***

Mode Global Config

5.2.0.22 spanning-tree port mode

This command sets the Administrative Switch Port State for this port to enabled.

Default enabled

Format `spanning-tree port mode`

Mode Interface Config

5.2.0.22.1 no spanning-tree port mode

This command sets the Administrative Switch Port State for this port to disabled.

Format `no spanning-tree port mode`

Mode Interface Config

5.2.0.23 spanning-tree port mode all

This command sets the Administrative Switch Port State for all ports to enabled.

Default enabled

Format `spanning-tree port mode all`

Mode Global Config

5.2.0.23.1 no spanning-tree port mode all

This command sets the Administrative Switch Port State for all ports to disabled.

Format `no spanning-tree port mode all`

Mode Global Config

5.2.0.24 spanning-tree port-priority

Use this command to change the priority value of the port to allow the operator to select the relative importance of the port in the forwarding process. Set this value to a lower number to prefer a port for forwarding of frames.

All LAN ports have 128 as priority value by default. PVSTP/PVRSTP puts the LAN port with the lowest LAN port number in the forwarding state and blocks other LAN ports.

The application uses the port priority value when the LAN port is configured as an edge port.

Default enabled

Format `spanning-tree port-priority` *`0-240`*

Mode Interface Config

5.2.0.25 spanning-tree transmit

This command sets the Bridge Transmit Hold Count parameter. The valid hold count range is 1–10.

Default `6`

Format `spanning-tree transmit` *`hold-count`*

Mode Global Config

Parameter	Description
hold-count	The Bridge Tx hold-count parameter. The value in an integer between 1 and 10.

5.2.0.26 spanning-tree tcnguard

Use this command to enable TCN guard on the interface. When enabled, TCN Guard restricts the interface from propagating any topology change information received through that interface.

Default	Enabled
Format	`spanning-tree tcnguard`
Mode	Interface Config

5.2.0.26.1 no spanning-tree tcnguard

This command resets the TCN guard status of the port to the default value.

Format	`no spanning-tree tcnguard`
Mode	Interface Config

5.2.0.27 spanning-tree uplinkfast

This command configures the rate at which gratuitous frames are sent (in packets per second) after switchover to an alternate port on PVSTP configured switches and enables uplinkfast on PVSTP switches. The range is 0-32000; the default is 150. This command has the effect of accelerating spanning-tree convergence after switchover to an alternate port.

Uplinkfast can be configured even if the switch is configured for MST(RSTP) mode, but it only has an effect when the switch is configured for PVST mode. Enabling FastUplink increases the priority by 3000. Path costs less than 3000 have an additional 3000 added when uplinkfast is enabled. This reduces the probability that the switch will become the root switch.

Uplinkfast immediately changes to an alternate root port on detecting a root port failure and changes the new root port directly to the forwarding state. A TCN is sent for this event.

After a switchover to an alternate port (new root port), uplinkfast multicasts a gratuitous frame on the new root port on behalf of each attached machine so that the rest of the network knows to use the secondary link to reach that machine.

PVRSTP embeds support for backbonefast and uplinkfast. There is no provision to enable or disable these features in PVRSTP configured switches.

Default	`150`
Format	`spanning-tree uplinkfast [max-update-rate` *`packets`*`]`
Mode	Global Config

5.2.0.27.1 no spanning-tree uplinkfast

This command disables uplinkfast on PVSTP configured switches. All switch priorities and path costs that have not been modified from their default values are set to their default values.

Format	`no spanning-tree uplinkfast [max-update-rate]`
Mode	Global Config

5.2.0.28 spanning-tree vlan

Use this command to enable/disable spanning tree on a VLAN.

Default None
Format spanning-tree vlan *vlan-list*
Mode Global Config

Parameter	Description
vlan-list	The VLANs to which to apply this command.

5.2.0.29 spanning-tree vlan cost

Use this command to set the path cost for a port in a VLAN. The valid values are in the range of 1 to 200000000 or auto. If auto is selected, the path cost value is set based on the link speed.

Default None
Format spanning-tree vlan *vlan-id* cost {auto |*1-200000000*}
Mode Interface Config

5.2.0.30 spanning-tree vlan forward-time

Use this command to configure the spanning tree forward delay time for a VLAN or a set of VLANs. The default is 15 seconds.

Set this value to a lower number to accelerate the transition to forwarding. The network operator should take into account the end-to-end BPDU propagation delay, the maximum frame lifetime, the maximum transmission halt delay, and the message age overestimate values specific to their network when configuring this parameter.

Default 15 seconds
Format spanning-tree vlan *vlan-list* forward-time *4-30*
Mode Global Config

Parameter	Description
vlan-list	The VLANs to which to apply this command.
forward-time	The spanning tree forward delay time. The range is 4-30 seconds.

5.2.0.31 spanning-tree vlan hello-time

Use this command to configure the spanning tree hello time for a specified VLAN or a range of VLANs. The default is 2 seconds. Set this value to a lower number to accelerate the discovery of topology changes.

Default 2 seconds
Format spanning-tree vlan *vlan-list* hello-time *1-10*
Mode Global Config

Parameter	Description
vlan-list	The VLANs to which to apply this command.
hello-time	The spanning tree forward hello time. The range is 1-10 seconds.

5.2.0.32 spanning-tree vlan max-age

Use this command to configure the spanning tree maximum age time for a set of VLANs. The default is 20 seconds.

Set this value to a lower number to accelerate the discovery of topology changes. The network operator must take into account the end-to-end BPDU propagation delay and message age overestimate for their specific topology when configuring this value.

The default setting of 20 seconds is suitable for a network of diameter 7, lost message value of 3, transit delay of 1, hello interval of 2 seconds, overestimate per bridge of 1 second, and a BPDU delay of 1 second. For a network of diameter 4, a setting of 16 seconds is appropriate if all other timers remain at their default values.

Default `20 seconds`

Format `spanning-tree vlan` ***`vlan-list`*** `max-age` ***`6-40`***

Mode Global Config

Parameter	Description
vlan-list	The VLANs to which to apply this command.
hello-time	The spanning tree forward hello time. The range is 1-10 seconds.

5.2.0.33 spanning-tree vlan port-priority

Use this command to change the VLAN port priority value of the VLAN port to allow the operator to select the relative importance of the VLAN port in the forwarding selection process when the port is configured as a point-to-point link type. Set this value to a lower number to prefer a port for forwarding of frames.

Default `None`

Format `spanning-tree vlan` ***`vlan-id`*** `port-priority` ***`priority`***

Mode Interface Config

Parameter	Description
vlan-list	The VLANs to which to apply this command.
priority	The VLAN port priority. The range is 0-255.

5.2.0.34 spanning-tree vlan root

Use this command to configure the switch to become the root bridge or standby root bridge by modifying the bridge priority from the default value of 32768 to a lower value calculated to ensure the bridge is the root (or standby) bridge.

The logic takes care of setting the bridge priority to a value lower (primary) or next lower (secondary) than the lowest bridge priority for the specified VLAN or a range of VLANs.

Default 32768

Format spanning-tree vlan *vlan-list* root {primary|secondary}

Mode Global Config

Parameter	Description
vlan-list	The VLANs to which to apply this command.

5.2.0.35 spanning-tree vlan priority

Use this command to configure the bridge priority of a VLAN. The default value is 32768.

If the value configured is not among the specified values, it will be rounded off to the nearest valid value.

Default 32768

Format spanning-tree vlan *vlan-list* priority *priority*

Mode Global Config

Parameter	Description
vlan-list	The VLANs to which to apply this command.
priority	The VLAN bridge priority. Valid values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.

5.2.0.36 show spanning-tree

This command displays spanning tree settings for the common and internal spanning tree. The following details are displayed.

Format show spanning-tree

Mode
- Privileged EXEC
- User EXEC

Parameter	Definition
Bridge Priority	Specifies the bridge priority for the Common and Internal Spanning tree (CST). The value lies between 0 and 61440. It is displayed in multiples of 4096.
Bridge Identifier	The bridge identifier for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
Time Since Topology Change	Time in seconds.
Topology Change Count	Number of times changed.
Topology Change	Boolean value of the Topology Change parameter for the switch indicating if a topology change is in progress on any port assigned to the common and internal spanning tree.
Designated Root	The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.
Root Path Cost	Value of the Root Path Cost parameter for the common and internal spanning tree.

Parameter	Definition
Root Port Identifier	Identifier of the port to access the Designated Root for the CST
Root Port Max Age	Derived value.
Root Port Bridge Forward Delay	Derived value.
Hello Time	Configured value of the parameter for the CST.
Bridge Hold Time	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).
Bridge Max Hops	Bridge max-hops count for the device.
CST Regional Root	Bridge Identifier of the CST Regional Root. It is made up using the bridge priority and the base MAC address of the bridge.
Regional Root Path Cost	Path Cost to the CST Regional Root.
Associated FIDs	List of forwarding database identifiers currently associated with this instance.
Associated VLANs	List of VLAN IDs currently associated with this instance.

5.2.0.37 show spanning-tree active

Use this command to display the spanning tree values on active ports for the modes (xSTP and PV(R)STP).

Format `show spanning-tree active`

Mode
- Privileged EXEC
- User EXEC

Example: Example 1

```
(Routing)#show spanning-tree active

Spanning Tree: Enabled (BPDU Flooding: Disabled) Portfast BPDU Filtering: Disabled
Mode: rstp
CST Regional Root:        80:00:00:01:85:48:F0:0F
Regional Root Path Cost:  0


###### MST 0 Vlan Mapped:   3
ROOT ID
              Priority        32768
              Address         00:00:EE:EE:EE:EE
              This Switch is the Root.
              Hello Time: 2s Max Age: 20s Forward Delay: 15s
Interfaces

Name      State    Prio.Nbr  Cost      Sts           Role  RestrictedPort
--------- -------- --------- --------- ------------- ----- --------------
0/49      Enabled  128.49    2000      Forwarding    Desg  No
3/1       Enabled  96.66     5000      Forwarding    Desg  No
3/2       Enabled  96.67     5000      Forwarding    Desg  No
3/10      Enabled  96.75     0         Forwarding    Desg  No
```

Example: Example 2

```
(Routing)#show spanning-tree active

Spanning-tree enabled protocol rpvst
```

```
VLAN    1
 RootID    Priority        32769
           Address         00:00:EE:EE:EE:EE
           Cost            0
           Port            This switch is the root
           Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
 BridgeID  Priority        32769 (priority 32768 sys-id-ext 1)
           Address         00:00:EE:EE:EE:EE
           Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 300 sec

Interface State     Prio.Nbr  Cost    Status        Role
--------- --------- --------- ------- ------------- -----------
0/49      Enabled   128.49    2000    Forwarding    Designated
3/1       Enabled   128.66    5000    Forwarding    Designated
3/2       Enabled   128.67    5000    Forwarding    Designated
3/10      Enabled   128.75    0       Forwarding    Designated
VLAN    3
 RootID    Priority        32771
           Address         00:00:EE:EE:EE:EE
           Cost            0
           Port            This switch is the root
           Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
 BridgeID  Priority        32771 (priority 32768 sys-id-ext 3)
           Address         00:00:EE:EE:EE:EE
           Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 300 sec

Interface State     Prio.Nbr  Cost    Status        Role
--------- --------- --------- ------- ------------- -----------
3/1       Enabled   128.66    5000    Forwarding    Designated
3/2       Enabled   128.67    5000    Forwarding    Designated
3/10      Enabled   128.75    0       Forwarding    Designated
```

Example: Example 3

```
(Routing)#show spanning-tree active

Spanning-tree enabled protocol rpvst

VLAN    1
 RootID    Priority        32769
           Address         00:00:EE:EE:EE:EE
           Cost            0
           Port            10(3/10   )
           Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
 BridgeID  Priority        32769 (priority 32768 sys-id-ext 1)
           Address         00:00:EE:EE:EE:EE
           Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 300 sec

Interface State     Prio.Nbr  Cost    Status        Role
--------- --------- --------- ------- ------------- -----------
0/49      Enabled   128.49    2000    Discarding    Alternate
3/1       Enabled   128.66    5000    Forwarding    Disabled
3/2       Enabled   128.67    5000    Forwarding    Disabled
3/10      Enabled   128.75    0       Forwarding    Root
```

```
VLAN    3
 RootID    Priority        32771
           Address         00:00:EE:EE:EE:EE
           Cost            0
           Port            10(3/10   )
           Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
 BridgeID  Priority        32771 (priority 32768 sys-id-ext 3)
           Address         00:00:EE:EE:EE:EE
           Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 300 sec

Interface State     Prio.Nbr  Cost    Status        Role
--------- --------- --------- ------- ------------- -----------
3/1       Enabled   128.66    5000    Forwarding    Disabled
3/2       Enabled   128.67    5000    Forwarding    Disabled
3/10      Enabled   128.75    0       Forwarding    Root
```

5.2.0.38 show spanning-tree backbonefast

This command displays spanning tree information for backbonefast.

Format `show spanning-tree backbonefast`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Transitions via Backbonefast	The number of backbonefast transitions.
Inferior BPDUs received (all VLANs)	The number of inferior BPDUs received on all VLANs.
RLQ request PDUs received (all VLANs)	The number of root link query (RLQ) requests PDUs received on all VLANs.
RLQ response PDUs received (all VLANs)	The number of RLQ response PDUs received on all VLANs.
RLQ request PDUs sent (all VLANs)	The number of RLQ request PDUs sent on all VLANs.
RLQ response PDUs sent (all VLANs)	The number of RLQ response PDUs sent on all VLANs.

Example: The following shows example output from the command.

```
(Routing)#show spanning-tree backbonefast

Backbonefast Statistics
-----------------------
Transitions via Backbonefast (all VLANs)          : 0
Inferior BPDUs received (all VLANs)               : 0
RLQ request PDUs received (all VLANs)             : 0
RLQ response PDUs received (all VLANs)            : 0
RLQ request PDUs sent (all VLANs)                 : 0
RLQ response PDUs sent (all VLANs)                : 0
```

5.2.0.39 show spanning-tree brief

This command displays spanning tree settings for the bridge. The following information appears.

Format `show spanning-tree brief`

Mode
- Privileged EXEC
- User EXEC

Parameter	Definition
Bridge Priority	Configured value.
Bridge Identifier	The bridge identifier for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.
Bridge Max Age	Configured value.
Bridge Max Hops	Bridge max-hops count for the device.
Bridge Hello Time	Configured value.
Bridge Forward Delay	Configured value.
Bridge Hold Time	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).

5.2.0.40 show spanning-tree interface

This command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The `{slot/port | lag lag-id}` is the desired switch port or LAG to view. The following details are displayed on execution of the command.

Format `show spanning-tree interface {slot/port | lag lag-id}`

Mode
- Privileged EXEC
- User EXEC

Parameter	Definition
Hello Time	Admin hello time for this port.
Port Mode	Enabled or disabled.
BPDU Guard Effect	Enabled or disabled.
Root Guard	Enabled or disabled.
Loop Guard	Enabled or disabled.
TCN Guard	Enable or disable the propagation of received topology change notifications and topology changes to other ports.
BPDU Filter Mode	Enabled or disabled.
BPDU Flood Mode	Enabled or disabled.
Auto Edge	To enable or disable the feature that causes a port that has not seen a BPDU for **edge delay** time, to become an edge port and transition to forwarding faster.
Port Up Time Since Counters Last Cleared	Time since port was reset, displayed in days, hours, minutes, and seconds.
STP BPDUs Transmitted	Spanning Tree Protocol Bridge Protocol Data Units sent.
STP BPDUs Received	Spanning Tree Protocol Bridge Protocol Data Units received.
RSTP BPDUs Transmitted	Rapid Spanning Tree Protocol Bridge Protocol Data Units sent.
RSTP BPDUs Received	Rapid Spanning Tree Protocol Bridge Protocol Data Units received.
MSTP BPDUs Transmitted	Multiple Spanning Tree Protocol Bridge Protocol Data Units sent.
MSTP BPDUs Received	Multiple Spanning Tree Protocol Bridge Protocol Data Units received.

5.2.0.41 show spanning-tree mst detailed

This command displays the detailed settings for an MST instance.

Format `show spanning-tree mst detailed` *`mstid`*

Mode
- Privileged EXEC
- User EXEC

Parameter	Description
mstid	A multiple spanning tree instance identifier. The value is 0–4094.

5.2.0.42 show spanning-tree mst port detailed

This command displays the detailed settings and parameters for a specific switch port within a particular multiple spanning tree instance. The parameter `mstid` is a number that corresponds to the desired existing multiple spanning tree instance. The {*`slot/port`* | *`lag lag-id`*} is the desired switch port or LAG.

Format `show spanning-tree mst port detailed` *`mstid`* {*`slot/port`* | *`lag lag-id`*}

Mode
- Privileged EXEC
- User EXEC

Parameter	Definition
MST Instance ID	The ID of the existing MST instance.
Port Identifier	The port identifier for the specified port within the selected MST instance. It is made up from the port priority and the interface number of the port.
Port Priority	The priority for a particular port within the selected MST instance. The port priority is displayed in multiples of 16.
Port Forwarding State	Current spanning tree state of this port.
Port Role	Each enabled MST Bridge Port receives a Port Role for each spanning tree. The port role is one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port or Disabled Port
Auto-Calculate Port Path Cost	Indicates whether auto calculation for port path cost is enabled.
Port Path Cost	Configured value of the Internal Port Path Cost parameter.
Designated Root	The Identifier of the designated root for this port.
Root Path Cost	The path cost to get to the root bridge for this instance. The root path cost is zero if the bridge is the root bridge for that instance.
Designated Bridge	Bridge Identifier of the bridge with the Designated Port.
Designated Port Identifier	Port on the Designated Bridge that offers the lowest cost to the LAN.
Loop Inconsistent State	The current loop inconsistent state of this port in this MST instance. When in loop inconsistent state, the port has failed to receive BPDUs while configured with loop guard enabled. Loop inconsistent state maintains the port in a blocking state until a subsequent BPDU is received.
Transitions Into Loop Inconsistent State	The number of times this interface has transitioned into loop inconsistent state.
Transitions Out of Loop Inconsistent State	The number of times this interface has transitioned out of loop inconsistent state.

If you specify 0 (defined as the default CIST ID) as the `mstid`, this command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The *`slot/port`* is the desired switch port. In this case, the following are displayed.

Parameter	Definition
Port Identifier	The port identifier for this port within the CST.
Port Priority	The priority of the port within the CST.
Port Forwarding State	The forwarding state of the port within the CST.
Port Role	The role of the specified interface within the CST.
Auto-Calculate Port Path Cost	Indicates whether auto calculation for port path cost is enabled or not (disabled).
Port Path Cost	The configured path cost for the specified interface.
Auto-Calculate External Port Path Cost	Indicates whether auto calculation for external port path cost is enabled.
External Port Path Cost	The cost to get to the root bridge of the CIST across the boundary of the region. This means that if the port is a boundary port for an MSTP region, then the external path cost is used.
Designated Root	Identifier of the designated root for this port within the CST.
Root Path Cost	The root path cost to the LAN by the port.
Designated Bridge	The bridge containing the designated port.
Designated Port Identifier	Port on the Designated Bridge that offers the lowest cost to the LAN.
Topology Change Acknowledgement	Value of flag in next Configuration Bridge Protocol Data Unit (BPDU) transmission indicating if a topology change is in progress for this port.
Hello Time	The hello time in use for this port.
Edge Port	The configured value indicating if this port is an edge port.
Edge Port Status	The derived value of the edge port status. True if operating as an edge port; false otherwise.
Point To Point MAC Status	Derived value indicating if this port is part of a point to point link.
CST Regional Root	The regional root identifier in use for this port.
CST Internal Root Path Cost	The internal root path cost to the LAN by the designated external port.
Loop Inconsistent State	The current loop inconsistent state of this port in this MST instance. When in loop inconsistent state, the port has failed to receive BPDUs while configured with loop guard enabled. Loop inconsistent state maintains the port in a blocking state until a subsequent BPDU is received.
Transitions Into Loop Inconsistent State	The number of times this interface has transitioned into loop inconsistent state.
Transitions Out of Loop Inconsistent State	The number of times this interface has transitioned out of loop inconsistent state.

5.2.0.43 show spanning-tree mst port summary

This command displays the settings of one or all ports within the specified multiple spanning tree instance. The parameter `mstid` indicates a particular MST instance. The parameter `{`*`slot/port`* `|` *`lag lag-id`* `| all}` indicates the desired switch port, LAG, or all ports.

If you specify 0 (defined as the default CIST ID) as the `mstid`, the status summary displays for one or all ports within the common and internal spanning tree.

Format `show spanning-tree mst port summary` *`mstid`* `{`*`slot/port`* `|` *`lag lag-id`* `| all}`

Mode
- Privileged EXEC
- User EXEC

Parameter	Definition
MST Instance ID	The MST instance associated with this port.
Interface	*slot/port*
STP Mode	Indicates whether spanning tree is enabled or disabled on the port.
Type	Currently not used.
STP State	The forwarding state of the port in the specified spanning tree instance.
Port Role	The role of the specified port within the spanning tree.
Desc	Indicates whether the port is in loop inconsistent state or not. This field is blank if the loop guard feature is not available.

5.2.0.44 show spanning-tree mst port summary active

This command displays settings for the ports within the specified multiple spanning tree instance that are active links.

Format `show spanning-tree mst port summary` *`mstid`* `active`

Mode
- Privileged EXEC
- User EXEC

Parameter	Definition
MST Instance ID	The ID of the existing MST instance.
Interface	*slot/port*
STP Mode	Indicates whether spanning tree is enabled or disabled on the port.
Type	Currently not used.
STP State	The forwarding state of the port in the specified spanning tree instance.
Port Role	The role of the specified port within the spanning tree.
Desc	Indicates whether the port is in loop inconsistent state or not. This field is blank if the loop guard feature is not available.

5.2.0.45 show spanning-tree mst summary

This command displays summary information about all multiple spanning tree instances in the switch. On execution, the following details are displayed.

Format `show spanning-tree mst summary`

Mode
- Privileged EXEC
- User EXEC

Parameter	Definition
MST Instance ID List	List of multiple spanning trees IDs currently configured.
For each MSTID: ■ Associated FIDs ■ Associated VLANs	■ List of forwarding database identifiers associated with this instance. ■ List of VLAN IDs associated with this instance.

5.2.0.46 show spanning-tree summary

This command displays spanning tree settings and parameters for the switch. The following details are displayed on execution of the command.

Format `show spanning-tree summary`

Mode
- Privileged EXEC
- User EXEC

Parameter	Definition
Spanning Tree Adminmode	Enabled or disabled.
Spanning Tree Version	Version of 802.1 currently supported (IEEE 802.1s, IEEE 802.1w, or IEEE 802.1d) based upon the Force Protocol Version parameter.
BPDU Guard Mode	Enabled or disabled.
BPDU Filter Mode	Enabled or disabled.
Configuration Name	Identifier used to identify the configuration currently being used.
Configuration Revision Level	Identifier used to identify the configuration currently being used.
Configuration Digest Key	A generated Key used in the exchange of the BPDUs.
Configuration Format Selector	Specifies the version of the configuration format being used in the exchange of BPDUs. The default value is zero.
MST Instances	List of all multiple spanning tree instances configured on the switch.

5.2.0.47 show spanning-tree uplinkfast

This command displays spanning tree information for uplinkfast.

Format `show spanning-tree uplinkfast`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Uplinkfast transitions (all VLANs)	The number of uplinkfast transitions on all VLANs.
Proxy multicast addresses transmitted (all VLANs)	The number of proxy multicast addresses transmitted on all VLANs.

Example: The following shows example output from the command.

```
(Routing) #show spanning-tree uplinkfast

Uplinkfast is enabled.
BPDU update rate : 150 packets/sec

Uplinkfast Statistics
---------------------
Uplinkfast transitions (all VLANs)................. 0
Proxy multicast addresses transmitted (all VLANs).. 0
```

5.2.0.48 show spanning-tree vlan

This command displays spanning tree information per VLAN and also lists out the port roles and states along with port cost. The *vlan-list* parameter is a list of VLANs or VLAN-ranges separated by commas and with no embedded blank spaces. VLAN ranges are of the form “X-Y” where X and Y are valid VLAN identifiers and X< Y. The *vlanid* corresponds to an existing VLAN ID.

Format `show spanning-tree vlan {vlanid | vlan-list}`

Mode
- Privileged EXEC
- User EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) show spanning-tree vlan 1

VLAN    1
          Spanning-tree enabled protocol rpvst
          RootID    Priority        32769
           Address         00:0C:29:D3:80:EA
           Cost            0
           Port            This switch is the root
           Hello Time 2 Sec Max Age 15 sec Forward Delay 15 sec
 BridgeID  Priority        32769 (priority 32768 sys-id-ext 1)
           Address         00:0C:29:D3:80:EA
           Hello Time 2 Sec Max Age 15 sec Forward Delay 15 sec
           Aging Time 300
Interface  Role        Sts            Cost         Prio.Nbr
---------  ----------  -------------  ---------    --------
1/0/1      Designated  Forwarding     3000        128.1
1/0/2      Designated  Forwarding     3000        128.2
1/0/3      Disabled    Disabled       3000        128.3
1/0/4      Designated  Forwarding     3000        128.4
1/0/5      Designated  Forwarding     3000        128.5
1/0/6      Designated  Forwarding     3000        128.6
1/0/7      Designated  Forwarding     3000        128.7
1/0/8      Designated  Forwarding     3000        128.8
0/1/1      Disabled    Disabled       3000        128.1026
0/1/2      Disabled    Disabled       3000        128.1027
0/1/3      Disabled    Disabled       3000        128.1028
0/1/4      Disabled    Disabled       3000        128.1029
0/1/5      Disabled    Disabled       3000        128.1030
0/1/6      Disabled    Disabled       3000        128.1031
```

5.3 VLAN Commands

This section describes the commands you use to configure VLAN settings.

5.3.0.1 vlan database

This command gives you access to the VLAN Database mode, which allows you to configure VLAN characteristics.

Format `vlan database`

Mode Privileged EXEC

5.3.0.2 network mgmt_vlan

This command configures the Management VLAN ID.

Default 1

Format `network mgmt_vlan` *`1-4093`*

Mode Privileged EXEC

5.3.0.2.1 no network mgmt_vlan

This command sets the Management VLAN ID to the default.

Format `no network mgmt_vlan`

Mode Privileged EXEC

5.3.0.3 vlan

This command creates a new VLAN and assigns it an ID. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). VLAN range is 1-4093.

Format `vlan` *`1-4093`*

Mode VLAN Database

5.3.0.3.1 no vlan

This command deletes an existing VLAN. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). The VLAN range is 1-4093.

Format `no vlan 1-`*`4093`*

Mode VLAN Database

5.3.0.4 vlan acceptframe

This command sets the frame acceptance mode on an interface or range of interfaces. For VLAN Only mode, untagged frames or priority frames received on this interface are discarded. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. For admituntaggedonly mode, only untagged frames are accepted on this interface; tagged frames are discarded. With all options, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Default all

Format `vlan acceptframe {admituntaggedonly |vlanonly | all}`
Mode Interface Config

5.3.0.4.1 no vlan acceptframe

This command resets the frame acceptance mode for the interface or range of interfaces to the default value.

Format `no vlan acceptframe`
Mode Interface Config

5.3.0.5 vlan ingressfilter

This command enables ingress filtering on an interface or range of interfaces. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Default disabled
Format `vlan ingressfilter`
Mode Interface Config

5.3.0.5.1 no vlan ingressfilter

This command disables ingress filtering. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Format `no vlan ingressfilter`
Mode Interface Config

5.3.0.6 vlan internal allocation

Use this command to configure which VLAN IDs to use for port-based routing interfaces. When a port-based routing interface is created, an unused VLAN ID is assigned internally.

Format `vlan internal allocation {base vlan-id | policy ascending | policy decending}`
Mode Global Config

Parameter	Description
base *vlan-id*	The first VLAN ID to be assigned to a port-based routing interface.
policy ascending	VLAN IDs assigned to port-based routing interfaces start at the base and increase in value
policy descending	VLAN IDs assigned to port-based routing interfaces start at the base and decrease in value

5.3.0.7 vlan makestatic

This command changes a dynamically created VLAN to a static VLAN (one that is permanently configured and defined). The ID is a valid VLAN identification number. VLAN range is 1-4093.

Format `vlan makestatic *1-4093*`
Mode VLAN Database

5.3.0.8 vlan name

This command changes the name of a VLAN. The name is an alphanumeric string of up to 32 characters, and the ID is a valid VLAN identification number. ID range is 1-4093.

Default
- VLAN ID 1 - default
- other VLANS - blank string

Format `vlan name` *`1-4093 name`*

Mode VLAN Database

5.3.0.8.1 no vlan name

This command sets the name of a VLAN to a blank string.

Format `no vlan name` *`1-4093`*

Mode VLAN Database

5.3.0.9 vlan participation

This command configures the degree of participation for a specific interface or range of interfaces in a VLAN. The ID is a valid VLAN identification number, and the interface is a valid interface number.

Format `vlan participation {exclude | include | auto}` *`1-4093`*

Mode Interface Config

Participation options are:

Options	Definition
include	The interface is always a member of this VLAN. This is equivalent to registration fixed.
exclude	The interface is never a member of this VLAN. This is equivalent to registration forbidden.
auto	The interface is dynamically registered in this VLAN and will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

5.3.0.10 vlan participation all

This command configures the degree of participation for all interfaces in a VLAN. The ID is a valid VLAN identification number.

Format `vlan participation all {exclude | include | auto}` *`1-4093`*

Mode Global Config

You can use the following participation options:

Participation Options	Definition
include	The interface is always a member of this VLAN. This is equivalent to registration fixed.
exclude	The interface is never a member of this VLAN. This is equivalent to registration forbidden.
auto	The interface is dynamically registered in this VLAN. The interface will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

5.3.0.11 vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces.

Default all

Format `vlan port acceptframe all {vlanonly | all}`

Mode Global Config

The modes are defined as follows:

Mode	Definition
VLAN Only mode	Untagged frames or priority frames received on this interface are discarded.
Admit All mode	Untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port.

With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

5.3.0.11.1 no vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces to Admit All. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Format `no vlan port acceptframe all`

Mode Global Config

5.3.0.12 vlan port ingressfilter all

This command enables ingress filtering for all ports. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Default disabled

Format `vlan port ingressfilter all`

Mode Global Config

5.3.0.12.1 no vlan port ingressfilter all

This command disables ingress filtering for all ports. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Format `no vlan port ingressfilter all`

Mode Global Config

5.3.0.13 vlan port pvid all

This command changes the VLAN ID for all interface.

Default 1

Format `vlan port pvid all` *`1-4093`*

Mode Global Config

5.3.0.13.1 no vlan port pvid all

This command sets the VLAN ID for all interfaces to 1.

Format `no vlan port pvid all`

Mode Global Config

5.3.0.14 vlan port tagging all

This command configures the tagging behavior for all interfaces in a VLAN to enabled. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format `vlan port tagging all` *`1-4093`*

Mode Global Config

5.3.0.14.1 no vlan port tagging all

This command configures the tagging behavior for all interfaces in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format `no vlan port tagging all`

Mode Global Config

5.3.0.15 vlan pvid

This command changes the VLAN ID on an interface or range of interfaces.

Default 1

Format `vlan pvid` *`1-4093`*

Mode Interface Config
Interface Range Config

5.3.0.15.1 no vlan pvid

This command sets the VLAN ID on an interface or range of interfaces to 1.

Format `no vlan pvid`

Mode Interface Config

5.3.0.16 vlan stats

This command enables statistics collection on the VLAN list specified if the specified VLAN(s) are administratively created in the system.

Default enable

Format `vlan` *`vlan-list`* `stats`

Mode VLAN Database

Example: To enable statistics on VLANs 10, 20, and 30.

```
(Switching) (Vlan)# vlan 10,20,30 stats
```

5.3.0.16.1 no vlan stats

This command disables statistics collection on the VLAN list specified if the specified VLAN(s) are administratively created in the system.

Default enable

Format `no vlan vlan-list stats`

Mode VLAN Database

Example: To disable statistics on VLANs 10, 20 and 30.

```
(Switching) (Vlan)# no vlan 10,20,30 stats
```

5.3.0.17 vlan tagging

This command configures the tagging behavior for a specific interface or range of interfaces in a VLAN to enabled. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format `vlan tagging 1-4093`

Mode
- Interface Config

5.3.0.17.1 no vlan tagging

This command configures the tagging behavior for a specific interface or range of interfaces in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format `no vlan tagging 1-4093`

Mode
- Interface Config

5.3.0.18 show vlan

This command displays information about the configured private VLANs, including primary and secondary VLAN IDs, type (community, isolated, or primary) and the ports which belong to a private VLAN.

Format `show vlan {vlanid|private-vlan [type]}`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Primary	Primary VLAN identifier. The range of the VLAN ID is 1 to 4093.
Secondary	Secondary VLAN identifier.
Type	Secondary VLAN type (community, isolated, or primary).
Ports	Ports which are associated with a private VLAN.
VLAN ID	The VLAN identifier (VID) associated with each VLAN. The range of the VLAN ID is 1 to 4093.

Term	Definition
VLAN Name	A string associated with this VLAN as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of **Default**. This field is optional.
VLAN Type	Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is configured and permanently defined), or Dynamic. A dynamic VLAN can be created by GVRP registration or during the 802.1X authentication process (DOT1X) if a RADIUS-assigned VLAN does not exist on the switch.
Interface	The physical port, or LAG interface associated with the rest of the data in the row.
Current	The degree of participation of this port in this VLAN. The permissible values are: ■ **Include** - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard. ■ **Exclude** - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. ■ **Autodetect** - To allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.
Configured	The configured degree of participation of this port in this VLAN. The permissible values are: ■ **Include** - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard. ■ **Exclude** - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. ■ **Autodetect** - To allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.
Tagging	The tagging behavior for this port in this VLAN. ■ **Tagged** - Transmit traffic for this VLAN as tagged frames. ■ **Untagged** - Transmit traffic for this VLAN as untagged frames.

5.3.0.19 show vlan stats

This command displays the supported per-VLAN statistics for the VLAN(s) specified.

Format `show vlan [`*`vlan-id`* `|` *`vlan-list`*`] stats`

Mode Privileged EXEC

Example: To display statistics on VLAN 10.

```
(Switching) # show vlan 10 stats
VlanID..................................... 10
RxBytes.................................... 0
RxFrames................................... 0
RxDiscardBytes............................. 0
RxDiscardFrames............................ 0
TxBytes.................................... 0
TxFrames................................... 0
TxDiscardBytes............................. 0
TxDiscardFrames............................ 0
```

Example: To display statistics on VLAN 10, 20 and 30.

```
(Switching) # show vlan 10,20,30 stats
```

```
VlanID..................................... 10
RxBytes.................................... 0
RxFrames................................... 0
RxDiscardBytes............................. 0
RxDiscardFrames............................ 0
TxBytes.................................... 0
TxFrames................................... 0
TxDiscardBytes............................. 0
TxDiscardFrames............................ 0

VlanID..................................... 20
RxBytes.................................... 0
RxFrames................................... 0
RxDiscardBytes............................. 0
RxDiscardFrames............................ 0
TxBytes.................................... 0
TxFrames................................... 0
TxDiscardBytes............................. 0
TxDiscardFrames............................ 0

VlanID..................................... 30
RxBytes.................................... 0
RxFrames................................... 0
RxDiscardBytes............................. 0
RxDiscardFrames............................ 0
TxBytes.................................... 0
TxFrames................................... 0
TxDiscardBytes............................. 0
TxDiscardFrames............................ 0
```

Example: To display statistics on all available VLANs.

```
(Switching) # show vlan stats

VlanID..................................... 1
RxBytes.................................... 0
RxFrames................................... 0
RxDiscardBytes............................. 0
RxDiscardFrames............................ 0
TxBytes.................................... 0
TxFrames................................... 0
TxDiscardBytes............................. 0
TxDiscardFrames............................ 0

VlanID..................................... 10
RxBytes.................................... 0
RxFrames................................... 0
RxDiscardBytes............................. 0
RxDiscardFrames............................ 0
TxBytes.................................... 0
TxFrames................................... 0
TxDiscardBytes............................. 0
TxDiscardFrames............................ 0

VlanID..................................... 20
RxBytes.................................... 0
RxFrames................................... 0
RxDiscardBytes............................. 0
RxDiscardFrames............................ 0
```

```
TxBytes..................................... 0
TxFrames.................................... 0
TxDiscardBytes.............................. 0
TxDiscardFrames............................. 0

VlanID...................................... 30
RxBytes..................................... 0
RxFrames.................................... 0
RxDiscardBytes.............................. 0
RxDiscardFrames............................. 0
TxBytes..................................... 0
TxFrames.................................... 0
TxDiscardBytes.............................. 0
TxDiscardFrames............................. 0
```

5.3.0.20 show vlan internal usage

This command displays information about the VLAN ID allocation on the switch.

Format `show vlan internal usage`

Mode
- Privileged EXEC
- User EXEC

Parameter	Definition
Base VLAN ID	Identifies the base VLAN ID for Internal allocation of VLANs to the routing interface.
Allocation policy	Identifies whether the system allocates VLAN IDs in ascending or descending order.

5.3.0.21 show vlan brief

This command displays a list of all configured VLANs.

Format `show vlan brief`

Mode
- Privileged EXEC
- User EXEC

Parameter	Definition
VLAN ID	There is a VLAN Identifier (vlanid) associated with each VLAN. The range of the VLAN ID is 1-4093.
VLAN Name	A string associated with this VLAN as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of “Default.” This field is optional.
VLAN Type	Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is configured and permanently defined).

5.3.0.22 show vlan port

This command displays VLAN port information.

Format `show vlan port {`*`slot/port`* `| all}`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Interface	*slot/port* It is possible to set the parameters for all ports by using the selectors on the top line.
Port VLAN ID Configured	The VLAN ID that this port will assign to untagged frames or priority tagged frames received on this port. The value must be for an existing VLAN. The factory default is 1.
Port VLAN ID Current	The current VLAN ID that this port assigns to untagged frames or priority tagged frames received on this port. The factory default is 1.
Acceptable Frame Types	The types of frames that may be received on this port. The options are 'VLAN only' and 'Admit All'. When set to 'VLAN only', untagged frames or priority tagged frames received on this port are discarded. When set to 'Admit All', untagged frames or priority tagged frames received on this port are accepted and assigned the value of the Port VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance to the 802.1Q VLAN specification.
Ingress Filtering Configured	May be enabled or disabled. When enabled, the frame is discarded if this port is not a member of the VLAN with which this frame is associated. In a tagged frame, the VLAN is identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the Port VLAN ID specified for the port that received this frame. When disabled, all frames are forwarded in accordance with the 802.1Q VLAN bridge specification. The factory default is disabled.
Ingress Filtering Current	Shows the current ingress filtering configuration.
GVRP	May be enabled or disabled.
Default Priority	The 802.1p priority assigned to tagged packets arriving on the port.
Protected Port	Specifies if this is a protected port. If False, it is not a protected port; If true, it is.
Switchport mode	The current switchport mode for the port.
Operating parameters	The operating parameters for the port, including the VLAN, name, egress rule, and type.
Static configuration	The static configuration for the port, including the VLAN, name, and egress rule.
Forbidden VLANs	The forbidden VLAN configuration for the port, including the VLAN and name.

5.4 Private VLAN Commands

This section describes the commands you use for private VLANs. Private VLANs provides Layer 2 isolation between ports that share the same broadcast domain. In other words, it allows a VLAN broadcast domain to be partitioned into smaller point-to-multipoint subdomains. The ports participating in a private VLAN can be located anywhere in the Layer 2 network.

5.4.0.1 switchport private-vlan

This command defines a private-VLAN association for an isolated or community port or a mapping for a promiscuous port.

Format `switchport private-vlan {host-association primary-vlan-id secondary-vlan-id | mapping primary-vlan-id {add | remove} secondary-vlan-list | mapping trunk primary-vlan-id {secondary-vlan-list | add secondary-vlan-list | remove secondary-vlan-list} | trunk {native vlan vlan-id | allowed vlan vlan-list}} | association trunk primary-vlan-id secondary-vlan-id}`

Mode Interface Config

Parameter	Description
host-association	Defines the VLAN association for community or host ports.
mapping	Defines the private VLAN mapping for promiscuous ports.
mapping trunk	Maps the port to a primary VLAN and selected secondary VLANs.
primary-vlan-id	Primary VLAN ID of a private VLAN.
secondary-vlan-id	Secondary (isolated or community) VLAN ID of a private VLAN.
add	Associates the secondary VLAN with the primary one.
remove	Deletes the secondary VLANs from the primary VLAN association.
secondary-vlan-list	A list of secondary VLANs to be mapped to a primary VLAN.
trunk native vlan	Defines the VLAN association for untagged packets. If not configured, untagged packets are dropped.
trunk allowed vlan	Specifies the list of allowed normal VLANs on the trunk port.
association trunk	Associates a primary VLAN with a secondary (isolated only) VLAN. Multiple private VLAN pairs can be configured using this command.

5.4.0.1.1 no switchport private-vlan

This command removes the private-VLAN association or mapping from the port.

Format `no switchport private-vlan {host-association | mapping | mapping trunk {primary-vlan-id}| trunk allowed vlan-list | trunk native vlan vlan-id} association trunk primary-vlan-id secondary-vlan-id}`

Mode Interface Config

5.4.0.2 switchport mode private-vlan

This command configures a port as a promiscuous or host private VLAN port. Note that the properties of each mode can be configured even when the switch is not in that mode. However, they will only be applicable once the switch is in that particular mode.

Default `general`

Format `switchport mode private-vlan {host | promiscuous | trunk promiscuous | trunk secondary}`

Mode Interface Config

Parameter	Description
host	Configures an interface as a private VLAN host port. It can be either an isolated or community port depending on the secondary VLAN it is associated with.
promiscuous	Configures an interface as a private VLAN promiscuous port. The promiscuous ports are members of the primary VLAN.
trunk promiscuous	Configures an interface as a private VLAN promiscuous trunk port. These ports can carry traffic of several primary VLANs and normal VLANs. An endpoint connected to a promiscuous trunk port is allowed to communicate with all the endpoints within the private VLAN and also with other ports participating in normal VLANs. These ports carry the traffic of multiple primary VLANs towards the upstream router and regular VLANs. Promiscuous trunk ports are used when it is required to reduce the number of links connected to upstream devices while still being able to manage all the endpoints in a private VLAN—in addition to carrying traffic of normal VLANs. These ports are typically used where the switches are connected to upstream devices that do not understand private VLANs.
trunk secondary	Configures an interface as a private VLAN isolated trunk port. These ports can carry traffic of several secondary VLANs and normal VLANs.

5.4.0.2.1 no switchport mode private-vlan

This command removes the private-VLAN association or mapping from the port.

Format `no switchport mode private-vlan`

Mode Interface Config

5.4.0.3 private-vlan

This command configures the private VLANs and configures the association between the primary private VLAN and secondary VLANs.

Format `private-vlan {association [add | remove] secondary-vlan-list | community | isolated | primary}`

Mode VLAN Config

Parameter	Description
association	Associates the primary and secondary VLAN.
secondary-vlan-list	A list of secondary VLANs to be mapped to a primary VLAN.
community	Designates a VLAN as a community VLAN.
isolated	Designates a VLAN as the isolated VLAN.
primary	Designates a VLAN as the primary VLAN.

5.4.0.3.1 no private-vlan

This command restores normal VLAN configuration.

Format `no private-vlan {association}`
Mode VLAN Config

5.4.0.4 show interface ethernet switchport

This command displays the private VLAN mapping information for the switch interfaces.

Format `show interface ethernet` *`interface-id`* `switchport`
Mode Privileged EXEC

Parameter	Description
interface-id	The *slot/port* of the switch.

The command displays the following information. Note that the fields that display depend on the configured mode on the port.

Term	Definition
Port	The port number for which data is displayed.
VLAN Switchport Mode	The private VLAN mode of the interface, which is one of the following: ■ General – The interface is in general mode and is not a member of a private VLAN. ■ Private VLAN Promiscuous – The interface belongs to a primary VLAN and can communicate with all interfaces in the private VLAN, including other promiscuous ports, community ports, and isolated ports. ■ Private VLAN Promiscuous Trunk – The interface belongs to a primary VLAN and can communicate with all interfaces in the private VLAN, including other promiscuous trunk ports, community ports, and isolated ports. ■ Private VLAN Host – The interface belongs to a secondary VLAN and, depending upon the type of secondary VLAN, can either communicate with other ports in the same community (if the secondary VLAN is a community VLAN) and with the promiscuous ports or is able to communicate only with the promiscuous ports (if the secondary VLAN is an isolated VLAN). ■ Private VLAN Isolated Trunk – The interface belongs to an isolated VLAN and can communicate with promiscuous, promiscuous trunk, and trunk ports.
Private VLAN Host Association	The VLAN association for the private-VLAN host ports.
Private VLAN Mapping	The VLAN mapping for the private-VLAN promiscuous ports.
Private VLAN trunk native VLAN	Displays the native VLAN for the promiscuous trunk ports. When the port is configured to operate in Promiscuous Trunk mode, the native VLAN defines VLAN association for untagged packets. If not configured, untagged packets are dropped.
Private VLAN trunk normal VLANs	The list of normal VLANs for the promiscuous trunk ports.
Private-VLAN trunk mappings	The mappings of all the primary VLANs and their associated secondary VLANs of promiscuous trunk ports.
Private-vlan trunk associations	The associations of all the primary VLANs and their associated isolated VLANs of isolated trunk ports.
Operational Private VLANS	The operational private VLANs on this interface.

5.5 Switch Port Mode Commands

This section describes the commands used for switch port mode.

5.5.0.1 switchport mode

Use this command to configure the mode of a switch port as access, trunk or general.

In Trunk mode, the port becomes a member of all VLANs on switch unless specified in the allowed list in the `switchport trunk allowed vlan` command. The PVID of the port is set to the Native VLAN as specified in the `switchport trunk native vlan` command. It means that trunk ports accept both tagged and untagged packets, where untagged packets are processed on the native VLAN and tagged packets are processed on the VLAN ID contained in the packet. MAC learning is performed on both tagged and untagged packets. Tagged packets received with a VLAN ID of which the port is not a member are discarded and MAC learning is not performed. The Trunk ports always transmit packets untagged on native VLAN.

In Access mode, the port becomes a member of only one VLAN. The port sends and receives untagged traffic. It can also receive tagged traffic.The ingress filtering is enabled on port. It means that when the VLAN ID of received packet is not identical to Access VLAN ID, the packet is discarded.

In General mode, the user can perform custom configuration of VLAN membership, PVID, tagging, ingress filtering etc. This is legacy EFOS behavior of switch port configuration. Legacy EFOS CLI commands are used to configure port in general mode.

Default	General mode
Format	`switchport mode {access | trunk | general}`
Mode	Interface Config

5.5.0.1.1 no switchport mode

This command resets the switch port mode to its default value.

Format	`no switchport mode`
Mode	Interface Config

5.5.0.2 switchport trunk allowed vlan

Use this command to configure the list of allowed VLANs that can receive and send traffic on this interface in tagged format when in trunking mode. The default is all.

The VLANs list can be modified using the add or remove options or replaced with another list using the vlan-list, all, or except options. If all is chosen, all VLANs are added to the list of allowed vlan. The except option provides an exclusion list.

Trunk ports accept tagged packets, where tagged packets are processed on the VLAN ID contained in the packet, if this VLAN is in the allowed VLAN list. Tagged packets received with a VLAN ID to which the port is not a member are discarded and MAC learning is not performed. If a VLAN is added to the system after a port is set to the Trunk mode and it is in the allowed VLAN list, this VLAN is assigned to this port automatically.

Default	All
Format	`switchport trunk allowed vlan {`*`vlan-list`*` | all | {add `*`vlan-list`*`} | {remove `*`vlan-list`*`} | {except `*`vlan-list`*` }}`

Mode Interface Config

Parameter	Description
all	Specifies all VLANs from 1 to 4093. This keyword is not allowed on commands that do not permit all VLANs in the list to be set at the same time.
add	Adds the defined list of VLANs to those currently set instead of replacing the list.
remove	Removes the defined list of VLANs from those currently set instead of replacing the list. Valid IDs are from 1 to 4093; extended-range VLAN IDs of the form X-Y or X,Y,Z are valid in this command.
except	Lists the VLANs that should be calculated by inverting the defined list of VLANs. (VLANs are added except the ones specified.)
vlan-list	Either a single VLAN number from 1 to 4093 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen.

5.5.0.2.1 no switchport trunk allowed vlan

This command resets the list of allowed VLANs on the trunk port to its default value.

Format `no switchport trunk allowed vlan`
Mode Interface Config

5.5.0.3 switchport trunk native vlan

Use this command to configure the Trunk port Native VLAN (PVID) parameter. Any ingress untagged packets on the port are tagged with the value of Native VLAN. Native VLAN must be in the allowed VLAN list for tagging of received untagged packets. Otherwise, untagged packets are discarded. Packets marked with Native VLAN are transmitted untagged from Trunk port. The default is 1.

Default 1 (Default VLAN)
Format `switchport trunk native vlan` *`vlan-id`*
Mode Interface Config

5.5.0.3.1 no switchport trunk native vlan

Use this command to reset the switch port trunk mode native VLAN to its default value.

Format `no switchport trunk native vlan`
Mode Interface Config

5.5.0.4 switchport access vlan

Use this command to configure the VLAN on the Access port. Only one VLAN can be assigned to the Access port. Access ports are members of VLAN 1 by default. Access ports may be assigned to a VLAN other than VLAN 1. Removing the Access VLAN on the switch makes the Access port a member of VLAN 1. Configuring an Access port to be a member of a VLAN that does not exist results in an error and does not change the configuration.

Default 1 (Default VLAN)
Format `switchport access vlan` *`vlan-id`*

Mode Interface Config

5.5.0.4.1 no switchport access vlan

This command resets the switch port access mode VALN to its default value.

Format `no switchport access vlan`
Mode Interface Config

5.5.0.5 show interfaces switchport

Use this command to display the switchport status for all interfaces or a specified interface. The output contains information about configured switchport mode, VLAN membership, PVID/Native VLAN, acceptable frame type, and other options per switchport modes.

Format `show interfaces switchport` *`slot/port`*
Mode Privileged EXEC

Example:

```
(Switching) # show interfaces switchport 1/0/20
Port: 1/0/20
Switchport Mode: Access Mode
Access Mode VLAN: 1 (default)
General Mode PVID: 1 (default)
General Mode Ingress Filtering: Enabled
General Mode Acceptable Frame Type: Admit All
General Mode Dynamically Added VLANs:
General Mode Untagged VLANs: 1
General Mode Tagged VLANs:
General Mode Forbidden VLANs:
Trunking Mode Native VLAN: 1 (default)
Trunking Mode Native VLAN Tagging: Disabled
Trunking Mode VLANs Enabled: All
Protected: False

(Routing) #show interfaces switchport

Port: 1/0/1
VLAN Membership Mode: General
Access Mode VLAN: 1 (default)
General Mode PVID: 1 (default)
General Mode Ingress Filtering: Disabled
General Mode Acceptable Frame Type: Admit all
General Mode Dynamically Added VLANs:
General Mode Untagged VLANs: 1
General Mode Tagged VLANs:
General Mode Forbidden VLANs:
Trunking Mode Native VLAN: 1 (default)
Trunking Mode Native VLAN tagging: Disable
Trunking Mode VLANs Enabled: All
Protected Port: False
```

5.5.0.6 show interfaces switchport

Use this command to display the Switchport configuration for a selected mode per interface. If the interface is not specified, the configuration for all interfaces is displayed.

Format `show interfaces switchport {access | trunk | general} [slot/port]`

Mode Privileged EXEC

Example:

```
Switching) # show interfaces switchport access 1/0/1

Intf      PVID
--------- ----
1/0/1     1


(Switching) # show interfaces switchport trunk 1/0/6

Intf      PVID  Allowed Vlans List
--------- ----- -------------------
1/0/6     1     All


(Switching) # show interfaces switchport general 1/0/5

Intf      PVID  Ingress     Acceptable  Untagged  Tagged   Forbidden  Dynamic
                Filtering   Frame Type  Vlans     Vlans    Vlans      Vlans
--------- ----- ----------- ----------  --------- -------- ---------- ---------
1/0/5     1     Enabled     Admit All   7         10-50,55  9,100-200 88,96



(Switching) # show interfaces switchport general

Intf      PVID  Ingress     Acceptable  Untagged  Tagged   Forbidden  Dynamic
                Filtering   Frame Type  Vlans     Vlans    Vlans      Vlans
--------- ----- ----------- ----------  --------- -------- ---------- ---------
1/0/1     1     Enabled     Admit All   1,4-7     30-40,55  3,100-200 88,96
1/0/2     1     Disabled    Admit All   1         30-40,55  none      none
..
```

5.6 VLAN Mapping Commands

The VLAN mapping feature enables the switch to replace a VLAN in a single-tagged packet with another VLAN ID. Based on per-port configuration, the wire VLAN is replaced with a device VLAN on ingress, and the device VLAN is replaced with the wire VLAN on egress. The VLAN tag protocol for the device VLAN and the wire VLAN is 0x8100, which the standard C-VLAN defined in the 802.1d standard.

The VLAN mapping feature simplifies VLAN ID assignment in a data center when using virtual routing and forwarding (VRF). The VRF instances require the switches in the data center to be interconnected with VLAN trunks instead of port-based routing interfaces, so the VLAN mapping feature enables the network administrator to select routing interface VLAN IDs independently on each switch instead of coordinating the VLAN ID assignment across multiple switches.

5.6.0.1 switchport mapping vlan

This command creates a mapping between the VLAN on the wire and the VLAN on the device. The command may be invoked for physical port interfaces. The wire VLANs on the same interface must be unique. The VLAN IDs selected for the wire VLAN cannot be used as the device VLAN ID on the same interface.

Default None

Format `switchport mapping vlan` *`wire-vlan device-vlan`*

Mode Interface Config

5.6.0.1.1 no switchport mapping vlan

This command deletes the specified VLAN mapping entry.

Format `no switchport mapping vlan` *`wire-vlan device-vlan`*

Mode Interface Config

5.6.0.2 show interfaces vlan mapping

This command displays the configured VLAN mapping entries. When the interface is not specified, the command displays VLAN mapping entries for all interfaces.

Format *`show interfaces vlan mapping [slot/port]`*

Mode Global Config

Example:

```
#show interfaces vlan mapping 0/50

Port        Wire VLAN    Device VLAN
---------   -------------      ----------------
0/50        10                   100
0/50        11                   101
```

5.7 Double VLAN Commands

This section describes the commands you use to configure double VLAN (DVLAN). Double VLAN tagging is a way to pass VLAN traffic from one customer domain to another through a Metro Core in a simple and cost effective manner. The additional tag on the traffic helps differentiate between customers in the MAN while preserving the VLAN identification of the individual customers when they enter their own 802.1Q domain.

5.7.0.1 dvlan-tunnel ethertype (Interface Config)

This command configures the ethertype for the specified interface. The two-byte hex ethertype is used as the first 16 bits of the DVLAN tag. The ethertype may have the values of `802.1Q`, `vman`, or `custom`. If the ethertype has an optional value of `custom`, then it is a custom tunnel value, and ethertype must be set to a value in the range of 1 to 65535.

NOTE: This command is not available on all platforms.

Default vman

Format `dvlan-tunnel ethertype {802.1Q | vman | custom` *`1-65535`*`}`

Mode Interface Config

Parameter	Description
802.1Q	Configure the ethertype as 0x8100.
custom	Configure the value of the custom tag in the range from 1 to 65535.
vman	Represents the commonly used value of 0x88A8.

5.7.0.1.1 no dvlan-tunnel ethertype (Interface Config)

Use the `no` form of the command to disassociate globally defined TPID(s) to an interface.

Format `no dvlan-tunnel ethertype {802.1Q | vman | custom` *`1-65535`*`}`

Mode Interface Config

5.7.0.2 dvlan-tunnel ethertype primary-tpid

Use this command to create a new TPID and associate it with the next available TPID register. If no TPID registers are empty, the system returns an error to the user. Specifying the optional keyword [default–tpid] forces the TPID value to be configured as the default TPID at index 0.

NOTE: If the default primary TPID (0x8100) of the switch is changed, this TPID is stored as one of the secondary TPIDs. If the configured Primary TPID is reset with no form of command, the default TPID becomes primary again and is removed from secondary list.

Format `dvlan-tunnel ethertype {802.1Q | vman | custom` *`1-65535`*`} [primary-tpid]`

Mode Global Config

Parameter	Description
802.1Q	Configure the ethertype as 0x8100.

Parameter	Description
custom	Configure the value of the custom tag in the range from 1 to 65535.
vman	Represents the commonly used value of 0x88A8.

5.7.0.2.1 no dvlan-tunnel ethertype primary–tpid

Use the `no` form of the command to reset the TPID register to 0. (At initialization, all TPID registers will be set to their default values.)

Format `no dvlan-tunnel ethertype {802.1Q | vman | custom` *`1-65535`*`} [primary-tpid]`
Mode Global Config

5.7.0.3 mode dot1q-tunnel

This command is used to enable Double VLAN Tunneling on the specified interface.

Default disabled
Format `mode dot1q-tunnel`
Mode Interface Config

5.7.0.3.1 no mode dot1q-tunnel

This command is used to disable Double VLAN Tunneling on the specified interface. By default, Double VLAN Tunneling is disabled.

Format `no mode dot1q-tunnel`
Mode Interface Config

5.7.0.4 mode dvlan-tunnel

Use this command to enable Double VLAN Tunneling on the specified interface.

NOTE: When you use the `mode dvlan-tunnel` command on an interface, it becomes a service provider port. Ports that do not have double VLAN tunneling enabled are customer ports.

Default disabled
Format `mode dvlan-tunnel`
Mode Interface Config

5.7.0.4.1 no mode dvlan-tunnel

This command is used to disable Double VLAN Tunneling on the specified interface. By default, Double VLAN Tunneling is disabled.

Format `no mode dvlan-tunnel`
Mode Interface Config

5.7.0.5 show dot1q-tunnel

Use this command without the optional parameters to display all interfaces enabled for Double VLAN Tunneling. Use the optional parameters to display detailed information about Double VLAN Tunneling for the specified interface or all interfaces.

Format `show dot1q-tunnel [interface {slot/port | all}]`

Mode
- Privileged EXEC
- User EXEC

Parameter	Definition
Interface	*slot/port*
Mode	The administrative mode through which Double VLAN Tunneling can be enabled or disabled. The default value for this field is disabled.
EtherType	A 2-byte hex EtherType to be used as the first 16 bits of the DVLAN tunnel. There are three different EtherType tags. The first is 802.1Q, which represents the commonly used value of 0x8100. The second is vMAN, which represents the commonly used value of 0x88A8. If EtherType is not one of these two values, then it is a custom tunnel value, representing any value in the range of 1 to 65535.

5.7.0.6 show dvlan-tunnel

Use this command without the optional parameters to display all interfaces enabled for Double VLAN Tunneling. Use the optional parameters to display detailed information about Double VLAN Tunneling for the specified interface or all interfaces.

Format `show dvlan-tunnel [interface {slot/port | all}]`

Mode
- Privileged EXEC
- User EXEC

Parameter	Definition
Interface	*slot/port*
Mode	The administrative mode through which Double VLAN Tunneling can be enabled or disabled. The default value for this field is disabled.
EtherType	A 2-byte hex EtherType to be used as the first 16 bits of the DVLAN tunnel. There are three different EtherType tags. The first is 802.1Q, which represents the commonly used value of 0x8100. The second is vMAN, which represents the commonly used value of 0x88A8. If EtherType is not one of these two values, then it is a custom tunnel value, representing any value in the range of 0 to 65535.

Example: The following shows examples of the CLI display output for the commands.

```
(Routing) #show dvlan-tunnel

TPIDs Configured.............................. 0x88a8
Default TPID.................................. 0x88a8
Interfaces Enabled for DVLAN Tunneling......... None

(Routing) #

(Routing) #show dvlan-tunnel interface 0/1

Interface  Mode     EtherType
---------  -------  ------------
0/1        Disable  0x88a8
```

5.8 Provisioning (IEEE 802.1p) Commands

This section describes the commands you use to configure provisioning (IEEE 802.1p,) which allows you to prioritize ports.

5.8.0.1 vlan port priority all

This command configures the port priority assigned for untagged packets for all ports presently plugged into the device. The range for the priority is 0-7. Any subsequent per port configuration will override this configuration setting.

Format `vlan port priority all` *priority*
Mode Global Config

5.8.0.2 vlan priority

This command configures the default 802.1p port priority assigned for untagged packets for a specific interface. The range for the priority is 0–7.

Default 0
Format `vlan priority` *priority*
Mode Interface Config

5.9 Protected Ports Commands

This section describes commands you use to configure and view protected ports on a switch. Protected ports do not forward traffic to each other, even if they are on the same VLAN. However, protected ports can forward traffic to all unprotected ports in their group. Unprotected ports can forward traffic to both protected and unprotected ports. Ports are unprotected by default.

If an interface is configured as a protected port, and you add that interface to a Port Channel or Link Aggregation Group (LAG), the protected port status becomes operationally disabled on the interface, and the interface follows the configuration of the LAG port. However, the protected port configuration for the interface remains unchanged. Once the interface is no longer a member of a LAG, the current configuration for that interface automatically becomes effective.

5.9.0.1 switchport protected (Global Config)

Use this command to create a protected port group. The `groupid` parameter identifies the set of protected ports. Use the `name name` pair to assign a name to the protected port group. The name can be up to 32 alphanumeric characters long, including blanks. The default is blank.

NOTE: Port protection occurs within a single switch. Protected port configuration does not affect traffic between ports on two different switches. No traffic forwarding is possible between two protected ports.

Default	unprotected
Format	`switchport protected` ***`groupid`*** `name` ***`name`***
Mode	Global Config

5.9.0.1.1 no switchport protected (Global Config)

Use this command to remove a protected port group. The `groupid` parameter identifies the set of protected ports. The `name` keyword specifies the name to remove from the group.

Format	`no switchport protected` ***`groupid`*** `name`
Mode	Global Config

5.9.0.2 switchport protected (Interface Config)

Use this command to add an interface to a protected port group. The `groupid` parameter identifies the set of protected ports to which this interface is assigned. You can only configure an interface as protected in one group.

NOTE: Port protection occurs within a single switch. Protected port configuration does not affect traffic between ports on two different switches. No traffic forwarding is possible between two protected ports.

Default	unprotected
Format	`switchport protected` ***`groupid`***
Mode	Interface Config

5.9.0.2.1 no switchport protected (Interface Config)

Use this command to configure a port as unprotected. The `groupid` parameter identifies the set of protected ports to which this interface is assigned.

Format `no switchport protected` *`groupid`*

Mode Interface Config

5.9.0.3 show switchport protected

This command displays the status of all the interfaces, including protected and unprotected interfaces.

Format `show switchport protected` *`groupid`*

Mode
- Privileged EXEC
- User EXEC

Parameter	Definition
Group ID	The number that identifies the protected port group.
Name	An optional name of the protected port group. The name can be up to 32 alphanumeric characters long, including blanks. The default is blank.
List of Physical Ports	List of ports, which are configured as protected for the group identified with *groupid*. If no port is configured as protected for this group, this field is blank.

5.9.0.4 show interfaces switchport

This command displays the status of the interface (protected/unprotected) under the groupid.

Format `show interfaces switchport` *`slot/port groupid`*

Mode
- Privileged EXEC
- User EXEC

Parameter	Definition
Name	A string associated with this group as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. This field is optional.
Protected	Indicates whether the interface is protected or not. It shows TRUE or FALSE. If the group is a multiple groups then it shows TRUE in Group `groupid.`

5.10 Port-Based Network Access Control Commands

This section describes the commands you use to configure port-based network access control (IEEE 802.1X and Authentication Manager). Port-based network access control allows you to permit access to network services only to and devices that are authorized and authenticated.

The authenticator and supplicant PACP state machines comply with the 2010 standard.

Due to this migration, several IEEE 802.1X (dot1x) commands have been deprecated. For information about the deprecated commands, see Section 5.10.3, Deprecated IEEE 802.1X Commands

5.10.0.1 aaa authentication dot1x default

Use this command to configure the authentication method for port-based access to the switch. The possible methods are as follows:

- ias. Uses the internal authentication server users database for authentication. This method can be used in conjunction with any one of the existing methods like **local**, **radius**, etc.
- local. Uses the local username database for authentication.
- none. Uses no authentication.
- radius. Uses the list of all RADIUS servers for authentication.

Format `aaa authentication dot1x default {[ias | local | none | radius]}`

Mode Global Config

Example: The following is an example of the command.

```
(Routing) #configure
(Routing) (Config)#aaa authentication dot1x default local
```

5.10.0.2 clear dot1x statistics

This command resets the 802.1X statistics for the specified port or for all ports.

Format `clear dot1x statistics {`*`slot/port`* `| all}`

Mode Privileged EXEC

5.10.0.3 clear radius statistics

This command is used to clear all RADIUS statistics.

Format `clear radius statistics`

Mode Privileged EXEC

5.10.0.4 dot1x eapolflood

Use this command to enable EAPOL flood support on the switch.

Default disabled

Format `dot1x eapolflood`

Mode Global Config

5.10.0.4.1 no dot1x eapolflood

This command disables EAPOL flooding on the switch.

Format `no dot1x eapolflood`
Mode Global Config

5.10.0.5 authentication dynamic-vlan enable

Use this command to enable the switch to create VLANs dynamically when a RADIUS-assigned VLAN does not exist in the switch.

Default Disabled
Format `authentication dynamic-vlan enable`
Mode Global Config

5.10.0.5.1 no authentication dynamic-vlan enable

Use this command to prevent the switch from creating VLANs when a RADIUS-assigned VLAN does not exist in the switch.

Format `no authentication dynamic-vlan enable`
Mode Global Config

5.10.0.6 authentication event no-response action authorize vlan

This command configures the specified VLAN as the guest VLAN on an interface or a range of interfaces. The range is 1 to the maximum VLAN ID supported by the platform. By default, the guest VLAN is 0, which means it is invalid and is not operational.

Default disabled
Format `authentication event no-response action authorize vlan` *`vlan-id`*
Mode Interface Config

5.10.0.6.1 no authentication event no-response action authorize vlan

This command disables Guest VLAN on the interface.

Default disabled
Format `no authentication event no-response action authorize vlan`
Mode Interface Config

5.10.0.7 authentication event fail action authorize vlan

Use this command to configure the unauthenticated VLAN associated with the specified interface or range of interfaces. This VLAN is used when the AAA server fails to recognize the client credentials and rejects the authentication attempt. The unauthenticated VLAN ID can be a valid VLAN ID from 0-Maximum supported VLAN ID (4093 for EFOS). By default, the unauthenticated VLAN is 0, i.e. invalid and not operational.

Default 0

Format `authentication event fail action authorize vlan` *`vlan id`*
Mode Interface Config

5.10.0.7.1 no authentication event fail action authorize vlan

This command resets the unauthenticated VLAN associated with the port to its default value.

Format `no authentication event fail action authorize vlan`
Mode Interface Config

5.10.0.8 clear authentication sessions

This command clears information for all authentication manager sessions. All the authenticated clients are re-intialized and forced to authenticate again.

Format `clear authentication sessions`
Mode Privileged EXEC

5.10.0.9 dot1x max-reauth-req

This command sets the maximum number of times (attempts), the authenticator state machine on this port will retransmit EAPOL EAP Request-Identity frames before timing out the supplicant. The *`count`* value range is 1 to 20.

Default 2
Format `dot1x max-reauth-req` *`count`*
Mode Interface Config

5.10.0.9.1 no dot1x max-reauth-req

This command resets maximum number of retries allowed per port to its default value.

Format `no dot1x max-reauth-req`
Mode Interface Config

5.10.0.10 dot1x max-req

This command sets the maximum number of times the authenticator state machine on this port will retransmit EAPOL EAP Request frames (excluding Request-Identity frames) before restarting the authentication process.

Default 2
Format `dot1x max-req` *`count`*
Mode Interface Config

5.10.0.10.1 no dot1x max-req

This command resets maximum number of retries allowed per port to its default value.

Format `no dot1x max-req`

Mode Interface Config

5.10.0.11 authentication max-users

Use this command to set the maximum number of clients supported on an interface or range of interfaces when multi-authentication host mode is enabled on the port. The maximum users supported per port is dependent on the product. The *count* value is in the range 1 - 48.

Default 48
Format `authentication max-users` *count*
Mode Interface Config

5.10.0.11.1 no authentication max-users

This command resets the maximum number of clients allowed per port to its default value.

Format `no authentication max-users`
Mode Interface Config

5.10.0.12 authentication periodic

This command enables periodic reauthentication of the supplicant for the specified interface or range of interfaces.

Default Disabled
Format `authentication periodic`
Mode Interface Config

5.10.0.12.1 no authentication periodic

This command resets the periodic reauthenticaton to the default.

Format `no authentication periodic`
Mode Interface Config

5.10.0.13 authentication port-control

This command sets the authentication mode to be used on the specified interface or range of interfaces. The configuration on the interface takes precedence over the global configuration of this parameter.

Use the `force-unauthorized` parameter to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Use the `force-authorized` parameter to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Use the `auto` parameter to specify that the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server.

Default auto
Format `authentication port-control {force-unauthorized | force-authorized | auto }`
Mode Interface Config

5.10.0.13.1 no authentication port-control

This command sets the authentication-enabled port control mode on the specified port to the default value.

Format	`no authentication port-control`
Mode	Interface Config

5.10.0.14 authentication port-control all

This command configures the global authentication port-control mode. The interface port-control mode takes precedence over the global port-control mode.

Select `force-unauthorized` to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Select `force-authorized` to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Select `auto` to specify that the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server.

Default	auto
Format	`authentication port-control all {force-unauthorized | force-authorized | auto }`
Mode	Global Config

5.10.0.14.1 no authentication port-control all

This command sets the authentication mode on all ports to the default value.

Format	`no authentication port-control all`
Mode	Global Config

5.10.0.15 authentication host-mode

This command configures the host mode of a port. The configuration on the interface mode takes precedence over the global configuration of this parameter.

Default	multi-host
Format	`authentication host-mode { multi-auth | multi-domain | multi-host | single-host | multi-domain-multi-host }`
Mode	Interface Config

5.10.0.15.1 no authentication host-mode

This command sets the host mode for the port to the default value.

Format	`no authentication host-mode`
Mode	Interface Config

5.10.0.16 authentication host-mode all

This command configures the global authentication host mode. The interface host mode takes precedence over the global host mode.

Default	multi-host
Format	`authentication host-mode all { multi-auth | multi-domain | multi-host | single-host | multi-domain-multi-host }`
Mode	Global Config

5.10.0.16.1 no authentication host-mode

This command sets the host mode to the default value.

Format	`no authentication host-mode all`
Mode	Global Config

5.10.0.17 mab

This command is used to enable MAC Authentication Bypass (MAB) on an interface. MAB is a supplemental authentication mechanism that allows 802.1X unaware clients - such as printers, fax machines, and some IP phones - to authenticate to the network using the client MAC address as an identifier. However MAB can also be used to authenticate 802.1X aware clients.

This command also provides options to specify the type of authentication to be used, which can be either EAP-MD5, PAP, or CHAP. If enabled, EAP-MD5 is used by default.

Default	Status: Disabled If enabled, the default authentication type is EAP-MD5.
Format	`mab [auth-type {pap | eap-md5 | chap}]`
Mode	Interface Config

5.10.0.17.1 no mab

This command disables MAC authentication bypass (MAB) on an interface and resets the authentication type to the default value.

Format	`no mab`
Mode	Interface Config

5.10.0.18 dot1x system-auth-control

Use this command to enable the dot1x authentication support on the switch and to set the EFOS implementation of the IEEE 802.1X feature (dot1x) to version 1. By default, the current dot1x implementation version is 0.

While disabled, the dot1x configuration is retained and can be changed, but is not activated.

Default	disabled
Format	`dot1x system-auth-control`

Mode Global Config

5.10.0.18.1 no dot1x system-auth-control

This command is used to disable the dot1x authentication support on the switch.

Format `no dot1x system-auth-control`
Mode Global Config

5.10.0.19 authentication monitor

Use this command to enable the authentication monitor mode on the switch. The purpose of Monitor mode is to help troubleshoot port-based authentication configuration issues without disrupting network access for hosts connected to the switch. In Monitor mode, a host is granted network access to an authentication-enabled port even if it fails the authentication process. The results of the process are logged for diagnostic purposes.

Default disabled
Format `authentication monitor`
Mode Global Config

5.10.0.19.1 no authentication monitor

This command disables the authentication monitor mode on the switch.

Format `no authentication monitor`
Mode Global Config

5.10.0.20 dot1x software version

This command configures the version of IEEE 802.1X software implemented on the switch. This command configures the EFOS implementation, and not the protocol version of 802.1X. The value of the current software version is 1, and the value of the legacy software version is 0.

This command cannot be run from the CLI. The software version is set to 1 whenever the `dot1x system-auth-control` command is executed.

Default 0
Format `dot1x software version { 0 | 1 }`
Mode N/A

5.10.0.21 dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator or supplicant state machines on an interface or range of interfaces. Depending on the token used and the value (in seconds) passed, various timeout configurable parameters are set. The following tokens are supported:

Tokens	Definition
quiet-period	The value, in seconds, of the timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. This is the period for which the authenticator state machine stays in the HELD state.
tx-period	The value, in seconds, of the timer used by the authenticator state machine on this port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant.
server-timeout	The value, in seconds, of the timer used by the authenticator state machine on this port to timeout the authentication server.
supp-timeout	The value, in seconds, of the timer used by the authenticator state machine on this port to timeout the supplicant.
auth-period	The value, in seconds, of the timer used by the supplicant state machine on this port to timeout an authenticator when waiting for a response to packets other than EAPOL-Start.
start-period	The value, in seconds, of the timer used by the supplicant state machine on this port to determine the interval between two successive EAPOL-Start frames when they are being retransmitted.
held-period	The value, in seconds, of the timer used by the supplicant state machine on this port to determine the length of time it will wait before trying to send the authentication credentials again after a failed attempt. This is the period for which the supplicant state machine stays in the HELD state.

Default
- quiet-period: 60 seconds
- tx-period: 30 seconds
- supp-timeout: 30 seconds
- server-timeout: 30 seconds
- auth-period: 30 seconds
- start-period: 30 seconds
- held-period: 60 seconds

Format `dot1x timeout {quiet-period` *`seconds`* `| tx-period` *`seconds`* `| supp-timeout` *`seconds`* `| server-timeout` *`seconds`* `| auth-period` *`seconds`* `| start-period` *`seconds`* `| held-period` *`seconds`*`}`

Mode Interface Config

5.10.0.21.1 no dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on this port to the default values. Depending on the token used, the corresponding default values are set.

Format `no dot1x timeout {quiet-period` *`seconds`* `| tx-period` *`seconds`* `| supp-timeout` *`seconds`* `| server-timeout` *`seconds`* `| auth-period` *`seconds`* `| start-period` *`seconds`* `| held-period` *`seconds`*`}`

Mode Interface Config

5.10.0.22 dot1x user

This command adds the specified user to the list of users with access to the specified port or all ports. The *`user`* parameter must be a configured user.

Format `dot1x user` *`user`* `{`*`slot/port`* `| all}`

Mode Global Config

5.10.0.22.1 no dot1x user

This command removes the user from the list of users with access to the specified port or all ports.

Format `no dot1x user` *user* {*slot/port* | all}
Mode Global Config

5.10.0.23 authentication event server dead action

This command configures the actions to take when all the authentication servers are dead. The command also configures the critical VLAN ID. If the VLAN ID is not specified, the port PVID is used as the critical VLAN ID.

The `reinitialize` action triggers re-authentication for all authenticated clients on the port. Supplicants on the voice VLAN, unauthenticated VLAN (authentication failed clients), and guest VLAN are not disturbed. During re-authentication if all the servers are still dead, the supplicant is authorized and placed in the critical VLAN without contacting the RADIUS server for authentication.

The `authorize` action authorizes the authenticated supplicants and assigns them to the critical VLAN. Supplicants on the RADIUS assigned VLAN, voice VLAN, unauthenticated VLAN, and guest VLAN are not disturbed. Supplicants authorized on the port PVID are reauthorized on the critical VLAN.

Default Action: None
VLAN: Port PVID
Format `authentication event server dead action [{reinitialize | authorize}][vlan` *vlan-id*`]]`
Mode Interface Config

5.10.0.23.1 no authentication event server dead action

This command configures the dead server action to none.

Format `no authentication server dead action`
Mode Interface Config

5.10.0.24 authentication event server dead action authorize voice

This command enables authorization of voice devices on the critical voice VLAN when all the authentication servers are dead. The configured voice VLAN of the port, on which the voice device is connected, is used as the critical voice VLAN ID.

The connected device is identified as a voice device by the vendor-specific RADIUS attribute “device-traffic-class=voice”, which is sent in the RADIUS Access-Accept message. This means that the device should have been identified and authenticated once by reachable RADIUS servers before they went dead. The critical voice VLAN feature is activated under the following conditions:

- This command is configured.
- The RADIUS servers have stopped responding (i.e. are dead).
- A re-authentication of identified and authenticated voice devices occurs.

When this command is not configured, the voice device is not authorized when all RADIUS servers are dead.

Default Action: None
Format `authentication event server dead action authorize voice`
Mode Interface Config

5.10.0.24.1 no authentication event server dead action authorize voice

This command configures the dead server action for voice devices to none.

Format `no authentication server dead action authorize voice`
Mode Interface Config

5.10.0.25 authentication event server alive action

This command configures the actions to take when one authentication server comes back alive after all were dead. The `reinitialize` action triggers the re-authentication of supplicants authenticated on the critical VLAN.

Default Action: None
Format `authentication event server alive action [reinitialize]`
Mode Interface Config

5.10.0.25.1 no authentication event server alive action

This command configures the alive server action to none.

Format `no authentication server alive action`
Mode Interface Config

5.10.0.26 authentication violation

This command is used to configure the action to be taken when a security violation occurs on a port. The authentication violation can occur when a device tries to connect to a port where maximum number of devices has been exceeded.

Default Restrict
Format `authentication violation { protect | restrict | shutdown }`
Mode Interface Config

5.10.0.26.1 no authentication violation

This command resets the authentication violation mode allowed per port to its default mode.

Format `no authentication violation`
Mode Interface Config

5.10.0.27 mab request format attribute 1

This command sets configuration parameters that are used to format attribute1 for MAB requests to the RADIUS server. RADIUS attribute 1 is the username, which is often the client MAC address.

Default The group size is 2
The separator is :
The case is uppercase.

Format `mab request format attribute 1 groupsize {1 | 2 | 4 | 12} separator {- | : | .} [lowercase | uppercase]`

Mode Global Config

Parameter	Description
groupsize	The number of characters included in a group. In the following example, the group size is 2: 00:10:18:99:F2:B3 In the following example, the group size is 4: 0010:1899:F2B3
separator	The character that separates the group. In the following example, the separator is - (hyphen): 00-10-18-99-F2-B3 In the following example, the separator is : (colon): 00:10:18:99:F2:B3
lowercase | uppercase	The case of any letters in the username. In the following example, the case is lowercase: 00:10:18:99:f2:b3 In the following example, the case is uppercase: 00:10:18:99:F2:B3

5.10.0.27.1 no mab request format attribute 1

This command attribute1 formats for MAB requests to the RADIUS server to the default values.

Format `no mab request format attribute 1`

Mode Global Config

5.10.0.28 authentication critical recovery max-reauth

This command configures the number of supplicants that are re-authenticated per second. This configuration is for the entire system across all the supplicants on all ports. This is used to control the system and network load when the number of supplicants to be re-authenticated is large. These re-authentications can be triggered due to the configured dead or alive server reinitialize actions.

The range for *`number-of-clients`* is 1 to 50 clients.

Default 10 clients

Format `authentication critical recovery max-reauth` *`number-of-clients`*

Mode Global Config

5.10.0.28.1 no authentication critical recovery max-reauth

This command resets the number of supplicants that are re-authenticated per second to the default value.

Format `no authentication critical recovery max-reauth`

Mode Global Config

5.10.0.29 authentication enable

This command globally enables the Authentication Manager. Interface configuration takes effect only if the Authentication Manager is enabled with this command.

Default	disabled
Format	*authentication enable*
Mode	Global Config

5.10.0.29.1 no authentication enable

This command disables the Authentication Manager.

Format	*no authentication enable*
Mode	Global Config

5.10.0.30 authentication order

This command sets the order of authentication methods used on a port. The available authentication methods are Dot1x, MAB, and captive portal. Ordering sets the order of methods that the switch attempts when trying to authenticate a new device connected to a port. If one method is unsuccessful or timed out, the next method is attempted.

Each method can only be entered once. Ordering is only possible between 802.1x and MAB. Captive portal can be configured either as a stand-alone method or as the last method in the order.

Format	`authentication order {dot1x [mab [captive-portal] | captive-portal] | mab [dot1x [captive-portal]| captive-portal] | captive-portal}`
Mode	Interface Config

5.10.0.30.1 no authentication order

This command returns the port to the default authentication order.

Format	*no authentication order*
Mode	Interface Config

5.10.0.31 authentication priority

This command sets the priority for the authentication methods used on a port. The available authentication methods are Dot1x, MAB, and captive portal. The authentication priority decides if a previously authenticated client is reauthenticated with a higher-priority method when the same is received. Captive portal is always the last method in the list.

Default	`authentication order dot1x mab captive portal`
Format	`authentication priority {dot1x [mab [captive portal] | captive portal] | mab [dot1x [captive portal]| captive portal] | captive portal}`
Mode	Interface Config

5.10.0.31.1 no authentication priority

This command returns the port to the default order of priority for the authentication methods.

Format *no authentication priority*
Mode Interface Config

5.10.0.32 authentication timer restart

This command sets the time, in seconds, after which reauthentication starts. (The default time is 300 seconds.) The timer restarts the authentication only after all the authentication methods fail. At the expiration of this timer, authentication is reinitiated for the port.

Format *authentication timer restart <300-65535>*
Mode Interface Config

5.10.0.32.1 no authentication timer restart

This command sets the reauthentication value to the default value of 3600 seconds.

Format *no authentication timer restart*
Mode Interface Config

5.10.0.33 authentication timer reauthenticate

This command configures the period of time after which the Authenticator attempts to reauthenticate a supplicant on the port. You can specify the timeout value, in seconds, or use the `server` parameter to get the re-authentication timeout value from the server (for example, RADIUS). The `server` option specifies that the server-supplied session timeout and session termination-action are used by the Authenticator to reauthenticate a supplicant on the port. The server option is enabled by default. The reauthenticate `seconds` value range is 1 to 65535.

For reauthentication to happen after the configured or server-provided timeout, the `authentication periodic` command should have periodic reauthentication enabled (see Section 5.10.0.11, authentication max-users).

Format *authentication timer reauthenticate {seconds | server}*
Mode Interface Config

5.10.0.33.1 no authentication timer reauthenticate

This command sets the reauthentication value to the default value.

Format *no authentication timer reauthenticate*
Mode Interface Config

5.10.0.34 clear authentication statistics

Use this command to clear the authentication statistics on an interface.

Format *clear authentication statistics {slot/port] | all}*

Mode Privileged EXEC

5.10.0.35 clear authentication authentication-history

Use this command to clear the authentication history log for an interface.

Format *clear authentication authentication-history {slot/port | all}*

Mode Privileged EXEC

5.10.1 802.1X Supplicant Commands

EFOS supports 802.1X (“dot1x”) supplicant functionality on point-to-point ports. The administrator can configure the user name and password used in authentication and capabilities of the supplicant port.

5.10.1.1 dot1x pae

This command sets the port’s dot1x role. The port can serve as either a supplicant or an authenticator.

Format `dot1x pae {supplicant | authenticator}`
Mode Interface Config

5.10.1.2 dot1x supplicant port-control

This command sets the ports authorization state (Authorized or Unauthorized) either manually or by setting the port to auto-authorize upon startup. By default all the ports are authenticators. If the port’s attribute needs to be moved from <authenticator to supplicant> or <supplicant to authenticator>, use this command.

Format `dot1x supplicant port-control {auto | force-authorized | force_unauthorized}`
Mode Interface Config

Parameter	Description
auto	The port is in the Unauthorized state until it presents its user name and password credentials to an authenticator. If the authenticator authorizes the port, then it is placed in the Authorized state.
force-authorized	Sets the authorization state of the port to Authorized, bypassing the authentication process.
force-unauthorized	Sets the authorization state of the port to Unauthorized, bypassing the authentication process.

5.10.1.2.1 no dot1x supplicant port-control

This command sets the port-control mode to the default, auto.

Default auto
Format `no dot1x supplicant port-control`
Mode Interface Config

5.10.1.3 dot1x max-start

This command configures the number of attempts that the supplicant makes (EAP start frames sent) to find the authenticator before the supplicant assumes that there is no authenticator.

Default 3
Format `dot1x max-start` *<1-10>*
Mode Interface Config

5.10.1.3.1 no dot1x max-start

This command sets the max-start value to the default.

Format `no dot1x max-start`
Mode Interface Config

5.10.1.4 dot1x supplicant user

Use this command to map the given user to the port.

Format `dot1x supplicant user`
Mode Interface Config

5.10.2 Authentication Show Commands

5.10.2.1 show authentication

This command displays the authentication manager global information and the number of authenticated clients.

Format `show authentication`
Mode Privileged EXEC

Term	Definition
Authentication Manager Status	The admin status of the Authentication Manager on the switch. This is a global configuration.
Dynamic VLAN Creation Mode	Indicates whether the switch can dynamically create a RADIUS-assigned VLAN if it does not currently exist on the switch.
VLAN Assignment Mode	Indicates whether assignment of an authorized port to a RADIUS-assigned VLAN is allowed (enabled) or not (disabled).
Authentication Monitor Mode	Indicates whether the Monitor mode on the switch is enabled or disabled.
Critical Recovery Max ReAuth	Indicates the number of supplicants that are re-authenticated per second.
Number of Authenticated clients	The total number of clients authenticated on the switch except the ones in Monitor Mode.
Number of clients in Monitor Mode	The number clients authorized by Monitor mode on the switch.

Example:

```
(dhcp-10-130-86-142) #show authentication

Authentication Manager Status.................. Disabled
Dynamic Vlan Creation Mode..................... Disabled
VLAN Assignment Mode........................... Disabled
Authentication Monitor Mode.................... Disabled
Critical Recovery Max ReAuth................... 10

Number of Authenticated clients................ 2
Number of clients in Monitor mode.............. 0
```

5.10.2.2 show authentication authentication-history

Use this command to display information about the authentication history for a specified interface.

Format `show authentication authentication-history` *`slot/port`*
Mode Privileged EXEC

Term	Definition
Timestamp	The time of the authentication.
Interface	The interface.
MAC-Address	The MAC address for the interface.
Auth Status	The authentication and status for the interface.
Method	The authentication method for the interface.

Example: The following information is shown for the interface.

```
(switch) #show authentication authentication-history 1/0/2

Timestamp             Interface  MAC-Address        Auth Status   Method
--------------------  ---------  -----------------  ------------  ------
May 07 2018 13:02:41  1/0/2      58:05:94:1C:00:00  Unauthorized  802.1X
May 07 2018 13:01:33  1/0/2      58:05:94:1C:00:00  Unauthorized  802.1X
```

5.10.2.3 show authentication clients

Use this command to display Authentication Manager information for the clients authenticated on an interface.

Format `show authentication clients {all | interface` *`slot/port`* `}`

Mode Privileged EXEC

Term	Definition
Interface	The interface for which authentication configuration information is being displayed.
Mac Address	The MAC address of the client.
User Name	The user name associated with the client.
VLAN Assigned Reason	This can take one of the following values **Reason** / **Description** Default VLAN — The client has been authenticated on the port default VLAN and the authentication server is not RADIUS. RADIUS — RADIUS is used for authenticating the client. Voice VLAN — The client is identified as a Voice device. Critical VLAN — The client has been authenticated on the Critical VLAN. Unauthenticated VLAN — The client has been authenticated on the Unauthenticated VLAN. Guest VLAN — The client has been authenticated on the Guest VLAN. Monitor Mode — The client has been authenticated by Monitor mode.
Host Mode	The authentication host mode configured on the interface. The possible values are multi-auth, multi-domain, multi-host, single-host and multi-domain-multi-host.
Method	The method used to authenticate the client on the interface. The possible values are 802.1x. MAB, Captive Portal and None.
Control Mode	The configured control mode for this port. Possible values are force-unauthorized, auto and unauthorized.
Session Time	The amount of time the client session has been active.
Session Timeout	This value indicates the time for which the given session is valid. The time period in seconds is returned by the RADIUS server on authentication of the port.
Session Termination Action	This value indicates the action to be taken once the session timeout expires. Possible values are Default and Radius-Request. If the value is Default, the session is terminated and client details are cleared. If the value is Radius-Request, then a reauthentication of the client is performed.
Filter ID	Identifies the Filter ID returned by the RADIUS server when the client was authenticated. This is a configured DiffServ policy name on the switch.
DACL	Identifies the Downloadable ACL returned by the RADIUS server when the client was authenticated.
Acct Session ID	The Accounting Session Id associated with the client session.

Example:

```
(switch) #show authentication clients interface 1/0/2

Mac Address..................................... 58:05:94:1C:00:00
User Name....................................... testixia
VLAN Assigned Reason............................ Voice VLAN (100)
Host Mode ...................................... multi-auth
Method.......................................... 802.1X
Control Mode.................................... auto
Session time ... ............................... 0
Session timeout ................................ 0
Session Termination Action...................... Default
Filter-Id ...................................... None
DACL............................................ None
Session Termination Action...................... Default
Acct SessionId:................................. testixia:200000003
```

5.10.2.4 show authentication interface

Use this command to display authentication method information either for all interfaces or a specified port.

Format `show authentication interface {all | slot/port }`

Mode Privileged EXEC

The following information is displayed for each interface.

Term	Definition
Authentication Manager Status	The admin status of Authentication on the switch. This is a global configuration.
Interface	The interface for which authentication configuration information is being displayed.
Port Control Mode	The configured control mode for this port. Possible values are force-unauthorized | auto | unauthorized.
Host Mode	The authentication host mode configured on the interface.
Authentication Restart timer	The time, in seconds, after which reauthentication starts.
Configured method order	The order of authentication methods used on the interface.
Enabled method order	The order of authentication methods used on the interface.
Configured method priority	The priority for the authentication methods used on the interface.
Enabled method priority	The priority for the authentication methods used on the interface.
Reauthentication Period	The period after which all clients on the interface will be reauthenticated.
Reauthentication Enabled	Indicates whether reauthentication is enabled on the interface.
Maximum Users	The maximum number of clients that can be authenticated on the interface if the interface is configured as multi-auth host mode.
Guest VLAN ID	The VLAN id to be used to authorize clients that time out or fail authentication due to invalid credentials. This is applicable only for 802.1x unaware clients.
Unauthenticated VLAN ID	The VLAN id to be used to authorize clients that that time out or fail authentication due to invalid credentials. This is applicable only for 802.1x clients.
Critical VLAN ID	The VLAN id to be used to authorize clients that that time out due to unreachable RADIUS servers.
Authentication Violation Mode	The action to be taken when a security violation occurs on a port.
Authentication Server Dead action	The action to be undertaken for data clients when all RADIUS servers are found dead.
Authentication Server Dead action for Voice	The action to be undertaken for voice clients when all RADIUS servers are found dead.

Term	Definition
Authentication Server Alive action	The action to be undertaken for data clients when a RADIUS server comes back alive after all were found dead.

Example: The following example displays the output for the command.

```
(switch) #show  authentication interface 1/0/1

Authentication Manager Status.................. Enabled

Interface..................................... 1/0/1
Authentication Restart timer.................. 300
Configured method order....................... mab undefined undefined
Enabled method order.......................... mab undefined undefined
Configured method priority.................... dot1x mab captive-portal
Enabled method priority....................... dot1x mab undefined
Reauthentication Period (secs)................ 3600
Reauthentication Enabled...................... False
Maximum Users................................. 48
Guest VLAN ID..... ............................ 0
Unauthenticated VLAN ID....................... 0
Critical Vlan Id.............................. 0
Authentication Violation Mode................. Restrict
Authentication Server Dead action.............. None
Authentication Server Dead action for Voice.... None
Authentication Server Alive action............. None
```

5.10.2.5 show authentication methods

Use this command to display information about the authentication methods.

Format `show authentication methods`

Mode Privileged EXEC

Term	Definition
Authentication Login List	The authentication login listname.
Method 1	The first method in the specified authentication login list, if any.
Method 2	The second method in the specified authentication login list, if any.
Method 3	The third method in the specified authentication login list, if any.

Example: The following example displays the authentication configuration.

```
(switch)#show authentication methods

Login Authentication Method Lists
---------------------------------
defaultList         :  local
networkList         :  local

Enable Authentication Method Lists
----------------------------------
enableList          :  enable   none
```

```
enableNetList       :  enable   deny

Line     Login Method List    Enable Method List
-------  -----------------    ------------------
Console  defaultList          enableList
Telnet   networkList          enableNetList
SSH      networkList          enableNetList

HTTPS       :local
HTTP        :local
DOT1X       :
```

5.10.2.6 show authentication statistics

Use this command to display the authentication statistics for an interface.

Format *show authentication statistics slot/port*

Mode Privileged EXEC

The following information is displayed for each interface.

Term	Definition
Port	The port for which information is being displayed.
802.1X attempts	The number of Dot1x authentication attempts for the port.
802.1X failed attempts	The number of failed Dot1x authentication attempts for the port.
MAB attempts	The number of MAB (MAC authentication bypass) authentication attempts for the port.
MAB failed attempts	The number of failed MAB authentication attempts for the port.
Captive-portal attempts	The number of captive portal (Web authorization) authentication attempts for the port.
Captive-portal failed attempts	The number of failed captive portal authentication attempts for the port.

Example:

```
(Routing) #show authentication statistics 1/0/1

Port..................................... 1/0/1
802.1X attempts.......................... 0
802.1X failed attempts................... 0
Mab attempts............................. 0
Mab failed attempts...................... 0
Captive-portal attempts.................. 0
Captive-Portal failed attempts........... 0
```

5.10.2.7 show dot1x

This command is used to show a summary of the global dot1x configuration, summary information of the dot1x configuration for a specified port or all ports, the detailed dot1x configuration for a specified port and the dot1x statistics for a specified port - depending on the tokens used.

Format `show dot1x [{supplicant` ***summary*** `{`***slot/port*** `| all} | detail` ***slot/port*** `| statistics` ***slot/port***`]`

Mode Privileged EXEC

If you do not use the optional parameters *unit/slot/port*, the command displays the global configuration.

Term	Definition
Administrative Mode	Indicates whether 8021X is enabled or disabled.
EAPOL Flood Mode	Indicates whether the EAPOL flood support is enabled on the switch.
Software Version	The version of the dot1X implementation running on the switch.

Example:

```
(switch) #show dot1x

Administrative Mode.............. Enabled
EAPOL Flood Mode................. Disabled
Software Version................. 1
```

If you use the optional parameter *supplicant summary* {*slot/port* | all}, the dot1x supplicant authorization for the specified port or all ports are displayed.

NOTE: MAC-based dot1x authentication support is platform-dependent.

Term	Definition
Port	The interface whose configuration is displayed.
Port Status	Indicates whether the port is authorized or unauthorized. Possible values are authorized | unauthorized.

Example: The following shows example CLI display output for the command `show dot1x supplicant summary 1/0/1.`

```
Operating
Interface     Port Status
---------     ------------
0/1           Authorized
```

If the port is configured as an Authenticator, the optional parameter `detail slot/port` displays the detailed dot1x configuration for the specified port.

Term	Definition
Port	The interface whose configuration is displayed.
Protocol Version	The protocol version associated with this port. The only possible value is 1,corresponding to the first version of the dot1x specification.
PAE Capabilities	The port access entity (PAE) functionality of this port. Possible values are Authenticator or Supplicant.
Quiet Period	The timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The value is expressed in seconds and will be in the range 0 and 65535. This is the period for which the authenticator state machine stays in the HELD state.
Transmit Period	The timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.
Supplicant Timeout	The timer used by the authenticator state machine on this port to timeout the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.
Server Timeout	The timer used by the authenticator on this port to timeout the authentication server. The value is expressed in seconds and will be in the range of 1 and 65535.
Maximum Request-Identities	The maximum number of times (attempts), the authenticator state machine on this port will retransmit an EAPOL EAP Request-Identity frames before timing out the supplicant.

Term	Definition
Maximum Requests	The maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/Identity before restarting the authentication process.
Key Transmission Enabled	Indicates if the key is transmitted to the supplicant for the specified port. Possible values are True or False.

Example: The following shows example CLI display output for the command.

```
(switch) #show dot1x detail 1/0/3
Port..................................... 1/0/3
Protocol Version......................... 1
PAE Capabilities......................... Authenticator
Quiet Period (secs)...................... 60
Transmit Period (secs)................... 30
Supplicant Timeout (secs)................ 30
Server Timeout (secs).................... 30
Maximum Request-Identities............... 2
Maximum Requests......................... 2
Key Transmission Enabled................. False
```

If the port is configured as a Supplicant, the `show dot1x detail` *slot/port*t command will display the following dot1x parameters

Term	Definition
Port	The interface whose statistics are displayed.
Protocol Version	The protocol version associated with this port. The only possible value is 1,corresponding to the first version of the dot1x specification.
PAE Capabilities	The port access entity (PAE) functionality of this port. Possible values are Authenticator or Supplicant.
Control Mode	The configured control mode for this port. Possible values are force-unauthorized | auto | unauthorized.
Supplicant PACP State	Current state of the authenticator PACP state machine. Possible values are Initialize, Logoff, Held, Unauthenticated, Authenticating and Authenticated.
Maximum Start Messages	The maximum number of EAP Start messages that the supplicant will send before moving to Unauthenticated State.
Start period	The timer period between each EAP Start message the supplicant sends when it does not hear from the authenticator.
Held period	The time period the supplicant waits before it restarts authentication after an EAP failure.
Authentication period	The time period the supplicant waits before it declares EAP timeout after it sends an EAP message (except EAP Start).

Example: The following shows example CLI display output for the command.

```
(switch) (Config)#show dot1x detail 1/0/24

Port..................................... 1/0/24
Protocol Version......................... 1
PAE Capabilities......................... Supplicant
Control Mode............................. auto
Supplicant PAE State..................... Authenticated

Maximum Start Messages................... 3
```

```
Start Period (secs)..... 30
Held Period (secs)..... 60
Authentication Period (secs)..... 30
```

If you use the optional parameter `statistics` *`slot/port`*, the following dot1x statistics for the specified port appear.

Term	Definition
Port	The interface whose statistics are displayed.
PAE Capabilities	The port access entity (PAE) functionality of this port. Possible values are Authenticator or Supplicant.
EAPOL Frames Received	The number of valid EAPOL frames of any type that have been received by this authenticator.
EAPOL Frames Transmitted	The number of EAPOL frames of any type that have been transmitted by this authenticator.
EAPOL Start Frames Received	The number of EAPOL start frames that have been received by this authenticator.
EAPOL Logoff Frames Received	The number of EAPOL logoff frames that have been received by this authenticator.
Last EAPOL Frame Version	The protocol version number carried in the most recently received EAPOL frame.
Last EAPOL Frame Source	The source MAC address carried in the most recently received EAPOL frame.
EAP Response/Id Frames Received	The number of EAP response/identity frames that have been received by this authenticator.
EAP Response Frames Received	The number of valid EAP response frames (other than resp/id frames) that have been received by this authenticator.
EAP Request/Id Frames Transmitted	The number of EAP request/identity frames that have been transmitted by this authenticator.
EAP Request Frames Transmitted	The number of EAP request frames (other than request/identity frames) that have been transmitted by this authenticator.
Invalid EAPOL Frames Received	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.
EAP Length Error Frames Received	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.

Example: The following shows example CLI display output for the command.

```
(switch) #show dot1x statistics 0/1
Port..... 0/1
EAPOL Frames Received..... 0
EAPOL Frames Transmitted..... 0
EAPOL Start Frames Transmitted..... 3
EAPOL Logoff Frames Received..... 0
EAP Resp/Id frames transmitted..... 0
EAP Response frames transmitted..... 0
EAP Req/Id frames transmitted..... 0
EAP Req frames transmitted..... 0
Invalid EAPOL frames received..... 0
EAP length error frames received..... 0
Last EAPOL Frame Version..... 0
Last EAPOL Frame Source..... 00:00:00:00:02:01
```

5.10.2.8 show dot1x users

This command displays 802.1X port security user information for locally configured users.

Format `show dot1x users` *`slot/port`*

Mode Privileged EXEC

Term	Definition
Users	Users configured locally to have access to the specified port.

Example:

```
#show dot1x users 1/0/1

Users
-----------------
admin
guest
test4
```

5.10.2.9 show mab

This command shows a summary of the global MAB configuration and summary information about the MAB configuration for all ports. This command also provides the detailed MAB sessions for a specified port.

Format `show mab [interface` *`slot/port`*`]`

Mode Privileged EXEC

Term	Definition
MAB Request Fmt Attr1 Groupsize	Displays the group size to be used by the switch for formatting RADIUS attribute 1 in MAB requests.
MAB Request Fmt Attr1 Separator	Displays the separator to be used by the switch for formatting RADIUS attribute 1 in MAB requests.
MAB Request Fmt Attr1 Case	Displays the case (uppercase or lowercase) to be used by the switch for formatting RADIUS attribute 1 in MAB requests.
Interface	Identifies the port.
Admin Mode	Indicates whether authentication control on the switch is enabled or disabled.
Auth-type	The type of authentication used for a MAB-enabled port, which can be either EAP-MD5, PAP, or CHAP.

Example:

```
(switch) #show mab

MAB Request Fmt Attr1 Groupsize... 2
MAB Request Fmt Attr1 Separator... legacy(:)
MAB Request Fmt Attr1 Case........ uppercase

Interface    Admin Mode    Auth-type
---------    -----------    ---------
1/0/1        Disabled      N/A
1/0/2        Enabled       eap-md5
1/0/3        Disabled      N/A
1/0/4        Disabled      N/A
```

Example:

```
(switch) #show mab interface 1/0/2
```

```
Interface     Admin Mode     Auth-type
---------     -----------    ---------
1/0/2         Enabled        eap-md5
```

5.10.3 Deprecated IEEE 802.1X Commands

The following table lists the CLI commands that are deprecated and replaced as a result of the move from the IEEE 802.1X 2004 standard to the 2010 standard.

Table 10: Deprecated IEEE 802.1X Commands

Deprecated Command	Replaced By
dot1x initialize	clear authentication sessions
dot1x re-authenticate	
dot1x critical recovery max-reauth	authentication critical recovery max-reauth
dot1x system-auth-control monitor	authentication monitor
dot1x port-control all	authentication port-control all
dot1x dynamic-vlan enable	authentication dynamic-vlan enable
dot1x guest-vlan	authentication event no-response action authorize vlan
dot1x unauthenticated-vlan	authentication event fail action authorize vlan
dot1x mac-auth-bypass	mab
dot1x max-users	authentication max-users
dot1x re-authentication	authentication periodic
dot1x timer reauth-period	authentication timer reauthenticate
dot1x supplicant timeout start-period	dot1x timer start-period
dot1x supplicant timeout auth-period	dot1x timer auth-period
dot1x supplicant timeout held-period	dot1x timer held-period
dot1x supplicant max-start	dot1x max-start
dot1x port-control mac-based	authentication enable authentication port-control auto authentication host-mode multi-auth
dot1x port-control auto	authentication enable authentication port-control auto authentication host-mode multi-domain-multi-host
dot1x port-control force-authorized	authentication enable authentication port-control force-authorized authentication host-mode multi-host
dot1x port-control force-unauthorized	authentication enable authentication port-control force-unauthorized authentication host-mode multi-host
clear dot1x authentication-history	clear authentication authentication-history
show dot1x authentication-history	show authentication authentication-history
show dot1x clients	show authentication clients

5.11 Microsoft Active Directory Authentication Commands

EFOS supports Microsoft Active Directory (MS AD) user authentication for management interfaces. MS AD provides an Lightweight Directory Access Protocol (LDAP) interface through which authentication is performed.

LDAP is defined in RFC 4511 and is a standard application protocol for accessing and maintaining distributed directory information services over the network. It is typically used to store information such as organizations, individuals, and other resources such as files and devices in a hierarchical manner. Microsoft Windows domain users and devices can be authenticated by looking up such information by using the LDAP protocol.

In EFOS, authentication into the Windows domain network is done via an LDAP simple bind operation and optionally over TLS. Authorization is done based on the *memberOf* attribute or the *description* attribute carrying a Cisco VSA (cisco-av-pair) configured on MS AD.

5.11.1 Global Configuration Commands

5.11.1.1 ldap-server host

This command adds a new LDAP server entry. During authentication the LDAP client (the switch) uses the configured server details to authenticate the user. In LDAP, DN is the distinguished name, which is a unique name for an entry in the directory service.

Format `ldap-server host { ipv4-address | ipv6-address | host-name } [enable-ssl] [rootDN dnString [password passwd]] [ port tcp-port [ timeout seconds ]]`

Default port = 389, timeout = 5 seconds, enable-ssl = false

Mode Global Config

Example: The following examples configure various LDAP server parameters.

```
(switch) (Config)#ldap-server host 10.130.84.11 port 389 timeout 10
(switch) (Config)#ldap-server host 10.130.84.11 rootDN cn=admin,dc=fp,dc=broadcom,dc=in password test
(switch) (Config)#ldap-server host 10.130.84.12 enable-ssl
```

Example: If SSL is enabled for a server, proper root CA certificates need to be installed on the device. This can be done by using `copy` command with the `nvram:root-ca-certs` option.

```
(switch)#copy scp://jdoe@192.168.25.12/cacert.pem nvram:root-ca-certs
```

5.11.1.1.1 no ldap-server host

This command deletes the LDAP server entry configuration or resets the SSL mode, port, and timeout to the default values.

Format `no ldap-server host { ipv4-address | ipv6-address | host-name } [enable-ssl] [rootDN dnString [password passwd]] [ port tcp-port [ timeout seconds ]]`

Mode Global Config

5.11.1.2 ldap authentication bind-first

This command instructs the switch to bind first and then search. The default authentication method is to first search and then bind. This command is helpful if an LDAP search is not allowed without a valid authentication.

Format `ldap authentication bind-first [ append-with-baseDN DNstring]`

Mode Global Config

5.11.1.2.1 no ldap authentication bind-first

This command resets the authentication method to the default method, which is to search first and then bind. Optionally, this command resets the `append-with-baseDN` string to none.

Format `no ldap authentication bind-first [ append-with-baseDN` *`DNstring`*`]`
Mode Global Config

5.11.1.3 ldap search-map

This command creates a search map and enters LDAP Search Map Mode. In this mode, it is possible to configure the LDAP search to send the search query to the server. The search query is used to fetch the user's privilege level or group membership information.

Format `ldap search-map` *`map-name`*
Mode Global Config

5.11.1.3.1 no ldap search-map

This command deletes search map configuration entry.

Format `no ldap search-map` *`map-name`*
Mode Global Config

5.11.2 LDAP Search Map Mode Config Commands

5.11.2.1 userprofile attribute-name

This command configures search map details for fetching a user privilege level. The attribute-name argument is the name of the attribute in the LDAP server that contains the privilege-level information. For example, the vendor specific *Cisco-AVPair* attribute can contain `shell:priv-lvl=15`, which sets the authenticating user to privilege level 15.

Format	`userprofile attribute-name` ***`attribute-name`*** `search-filter` ***`filter`*** `base-DN` ***`base-DN-name`***
Mode	LDAP Search Map Mode Config

Example:

```
(switch) (config-ldap-search-map)#userprofile attribute-name memberOf search-filter "(cn=$userid)"
base-DN DC=broadcom,DC=net
```

5.11.2.2 no userprofile

This command deletes the user profile mapping with the LDAP search query

Format	`no userprofile`
Mode	LDAP Search Map Mode Config

5.11.3 Privileged Exec mode Config Commands

5.11.3.1 debug ldap

This command enables LDAP authentication or packet debugging.

Format	`debug ldap {authentication | packet}`
Mode	Privileged EXEC

5.11.3.1.1 no debug ldap authentication

This command disables LDAP authentication debugging.

Format	`no debug ldap {authentication | packet}`
Mode	Privileged EXEC

5.11.4 Show Commands

5.11.4.1 show ldap-server

This command displays LDAP server configuration information for all hosts or for the specified host.

Format `show ldap-server [`*`ip-address`*`|`*`ipv6-address`*`|`*`host-name`*`]`

Mode Privileged EXEC

The command output includes the fields shown in the following table.

Term	Definition
Host Address	Host address of the LDAP server
SSL Enabled	Whether SSL mode is enabled
Port	LDAP port
Timeout	Timeout value for the LDAP operation, in seconds.

Example:

```
(localhost) (Config)#show ldap-server

Authentication : Bind and Search
Bind and Search : append with basedn "cn=$userid,ou=users"


Host address                                SSL Enabled  Port  Timeout
------------------------------------------- ------------ ----- -------
192.168.1.1                                 No           389   10 sec
server1.broadcom.net                        Yes          636   5 sec

(localhost) (Config)#show  ldap-server 192.168.1.1

Authentication : Bind and Search
Bind and Search : append with basedn "cn=$userid,ou=users"


Host address                                SSL Enabled  Port  Timeout
------------------------------------------- ------------ ----- -------
192.168.1.1                                 No           389   10 sec
```

5.11.4.2 show ldap-search-map

This command displays LDAP search map configuration information.

Format `show ldap-search-map`

Mode Privileged EXEC

The command output includes the fields shown in the following table.

Term	Definition
Search Map Name	User-configured name of the search map.

Term	Definition
Attribute Name	Name of the LDAP attribute.
Search Filter	Search filter names
Base DN	Base DN within which the search was performed.

Example:

```
(localhost)#show ldap-search-map

SEARCH MAP map1:
User Profile:
BaseDN..................... DC=broadcom,DC=net
Attribute Name.............. Cisco-AVPair
Search Filter.............. (cn=$userid)

SEARCH MAP map2:
User Profile:
BaseDN ..................... DC=broadcom,DC=net
Attribute Name.............. memberOf
Search Filter............... (sAMAccountName=$userid
```

5.11.4.3 show ldap-server statistics

This command displays LDAP server statistics for all hosts or for the specified host.

Format `show ldap-server statistics[`*`ip-address`*`|`*`ipv6-address`*`|`*`host-name`*`]`

Mode Privileged EXEC

The command output includes the fields shown in the following table.

Term	Definition
Failed Transactions	Number of failed transactions
Successful Transactions	Number of successful transactions
Number of requests sent	Number of total requests sent
Number of requests timed out	Number of requests timed out
Number of requests searches	Number of searches done

5.12 Task-based Authorization

Task-based authorization allows users to have different permission levels (read, write, execute, debug) at a per-component level. Task-based authorization uses the concept of components/tasks to define permission for commands for a given user.

Users are assigned to User Groups that are, in turn, associated with Task Groups. Each Task Group is then associated with one or more tasks/components. This release supports the AAA, BGP and OSPF components. Also, this feature is supported only for users who are authenticated locally via the CLI interface.

5.12.0.1 usergroup

This command creates a user group with the specified name and enters user group configuration mode.

Format `usergroup` *`usergroup-name`*
Mode Global Config

5.12.0.1.1 no usergroup

This command removes the user group with the specified name.

Format `no usergroup` *`usergroup-name`*
Mode Global Config

5.12.0.2 taskgroup

This command creates a task group with the specified name and enters task group configuration mode.

Format `taskgroup` *`taskgroup-name`*
Mode Global Config

5.12.0.2.1 no taskgroup

This command removes the task group with the specified name.

Format `no taskgroup` *`taskgroup-name`*
Mode Global Config

5.12.0.3 username usergroup

This command assigns the specified user to the specified user group.

Format `username <`*`username`*`> usergroup` *`usergroup-name`*
Mode Global Config

5.12.0.3.1 no username usergroup

This command removes the specified user from the specified user group.

Format `no usergroup` *`usergroup-name`*

Mode Global Config

5.12.0.4 description (User Group Mode)

This command sets a description for the user group.

Format `description` *`description`*
Mode User Group

5.12.0.4.1 no description (User Group Mode)

This command removes the description from the user group.

Format `no description`
Mode User Group

5.12.0.5 inherit usergroup

This command sets the parent user group of the current user group. The user group will have the permissions of the specified parent group.

Format `inherit usergroup` *`usergroup-name`*
Mode User Group

5.12.0.5.1 no inherit usergroup

This command removes the specified parent group relationship from the user group.

Format `no inherit usergroup` *`usergroup-name`*
Mode User Group

5.12.0.6 taskgroup (User Group Mode)

This command associates the user group with the specified task group.

Format `taskgroup` *`taskgroup-name`*
Mode User Group

5.12.0.6.1 no taskgroup (User Group Mode)

This command removes the user group’s relationship with the associated task group.

Format `no taskgroup` *`taskgroup-name`*
Mode User Group

5.12.0.7 description (Task Group Mode)

This command sets a description for the task group.

Format `description` *description*
Mode Task Group

5.12.0.7.1 no description (Task Group Mode)

This command removes the description from the task group.

Format `no description`
Mode Task Group

5.12.0.8 inherit taskgroup

This command sets the parent task group of the current task group. The task group will have the permissions of the specified parent task group.

Format `inherit taskgroup` *taskgroup-name*
Mode Task Group

5.12.0.8.1 no inherit taskgroup

This command removes the specified parent group relationship from the user group.

Format `no inherit taskgroup` *taskgroup-name*
Mode Task Group

5.12.0.9 task [read] [write] [debug] [execute]

This command associates the task group with the specified set of task permissions.

Default No permissions
Format *task [read] [write] [debug] [execute] {aaa | ospf | bgp}*
Mode Task Group

Example: The following example gives all users in the task group tg1 read-only permissions for AAA and read, write, execute, and debug permissions for OSPF.

```
(Routing) #configure
(Routing) (Config)#taskgroup tg1
(Routing) (config-taskgroup)#task read aaa
(Routing) (config-taskgroup)#task read write execute debug ospf
```

5.12.0.9.1 no task <aaa | ospf | bgp>

This command removes all relationships with the associated task.

Format *no task {aaa | ospf | bgp}*
Mode Task Group

5.12.0.10 show aaa usergroup

This command displays a list of user groups and their configuration.

Format `show aaa usergroup [`*`usergroup-name`*`]`
Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) #show aaa usergroup group1

User group "group1"

Description : "Example"
Parent user groups: “”
Contained task groups:
task group#1: "tg1"

Operational permissions:
Task: aaa                      : READ     WRITE     EXECUTE     DEBUG
Task: ospf                     : READ     WRITE     EXECUTE     DEBUG
Task: bgp                      : READ     WRITE     EXECUTE     DEBUG
```

5.12.0.11 show aaa taskgroup

This command displays a list of task groups and their configuration.

Format `show aaa taskgroup [`*`taskgroup-name`*`]`
Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) #show aaa taskgroup

Task group "default-taskgroup-name"

Description : ""
Parent taskgroups: ""

Configured permissions:
Task: aaa                    : READ     WRITE     EXECUTE     DEBUG
Task: ospf                   : READ     WRITE     EXECUTE     DEBUG
Task: bgp                    : READ     WRITE     EXECUTE     DEBUG

Operational permission:
Task: aaa                    : READ     WRITE     EXECUTE     DEBUG
Task: ospf                   : READ     WRITE     EXECUTE     DEBUG
Task: bgp                    : READ     WRITE     EXECUTE     DEBUG

Task group "task1"

Description : ""
Parent taskgroups: ""

Configured permissions:
```

```
Task: aaa                     : READ     WRITE     EXECUTE     DEBUG
Task: ospf                    : READ
Task: bgp                     : READ

Operational permission:
Task: aaa                     : READ     WRITE     EXECUTE     DEBUG
Task: ospf                    : READ
Task: bgp                     : READ
```

5.12.0.12 show aaa userdb

This command displays a list of users and list of groups the users participate in.

Format `show aaa userdb [username]`

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) #show aaa userdb admin

User "admin"

Contained user groups:
user group#1 : "EFOS-Root"

Operational permissions:
Task: aaa                       : READ     WRITE     EXECUTE     DEBUG
Task: ospf                      : READ     WRITE     EXECUTE     DEBUG
Task: bgp                       : READ     WRITE     EXECUTE     DEBUG
```

5.13 Cut-Through (ASF) Commands

The Cut-through Mode (or Alternative Store and Forward Mode, ASF) feature allows the switch to operate in a mode such that the egress pipeline begins transmitting a packet before the ingress pipeline has completely received the entire packet. Enabling this mode decreases latency for large packets.

Alternate Store and forward (ASF) reduces latency for larger packets. In this mode, the MMU is allowed to forward a packet to the egress port before it has been entirely received in the Cell Buffer Pool (CBP) memory. These switch devices provide a threshold to define how many cells must be received before the MMU is allowed to dispatch a packet to the egress. This value is generally configurable between 3-15 cells. Cell size varies from silicon to silicon.

NOTE: Support for cut-through mode is platform-dependent.

5.13.0.1 cut-through mode

Use this command to enable or disable cut-through mode on the switch. If you change the mode, you must reload the switch for the mode to take effect.

Default	Enabled
Format	`cut-through mode`
Mode	Global Config

5.13.0.1.1 no cut-through mode

This command resets the cut-through mode to the default value.

Format	`no cut-through mode`
Mode	Global Config

5.13.0.2 show cut-through mode

Use this command to view the current and configured status of cut-through mode.

Format	`show cut-through mode`
Mode	Global Config

Example: The following shows example CLI display output for the command.

```
(Routing) #show cut-through mode

Current mode    :Disable
Configured mode :Enable (This mode is effective on next reload)
```

5.14 Asymmetric Flow Control Commands

This feature enables you to configure the switch to use symmetric, asymmetric or no flow control. Asymmetric flow control allows the switch to respond to received PAUSE frames, but the port cannot generate PAUSE frames. Symmetric flow control allows the switch to both respond to, and generate MAC control PAUSE frames.

This feature is typically used with iSCSI disk arrays.

802.3x Flow control, the MAC control PAUSE operation, is specified in IEEE 802.3 Annex 31 B. It allows traffic from one device to be throttled for a specified period of time and is defined for devices that are directly connected. A device that wishes to inhibit transmission of data frames from another device on the LAN transmits a PAUSE frame as defined in the IEEE specification.

When Symmetric flow control is enabled, the ports asserts back pressure to the MAC, the MAC will respond by generating PAUSE frames, and the partner device will respond by stopping packet transmission to avoid packet loss. The ports are also capable of throttling the transmit rate in response to the PAUSE frames received from peer. When transmission of symmetric flow control frames is enabled, the entire switch is placed in ingress drop mode. When in ingress drop mode, the switch will behave like any other ingress buffered switch and exhibit head of line blocking during times of congestion.

Asymmetric flow control provides the switch the ability to respond to PAUSE frames received from peer, but the switch does not have the ability to generate MAC control PAUSE frames. It allows the user to configure the switch such that it never generates a MAC control PAUSE frame but will respond to received MAC control PAUSE frame by stopping the packet transmission.

5.14.0.1 flowcontrol

Use this command to enable or disable the symmetric or asymmetric flow control on the switch. Asymmetric here means that Tx Pause can never be enabled. Only Rx Pause can be enabled.

NOTE: Support for asymmetric flow control is platform-dependent. For platforms that support only symmetric flow control, the `{symmetric | asymmetric}` keywords are not available.

Default disabled

Format `flowcontrol {symmetric | asymmetric}`

Mode
- Global Config

5.14.0.1.1 no flowcontrol

Use this command to disable the symmetric or asymmetric flow control.

Format `no flowcontrol`

Mode
- Global Config

5.14.0.2 show flowcontrol

Use this command to display the IEEE 802.3 Annex 31B flow control settings and status for a specific interface or all interfaces. It also displays 802.3 Tx and Rx pause counts. Priority Flow Control frames counts are not displayed. If the port is enabled for priority flow control, operational flow control status is displayed as *Inactive*.

Format `show flowcontrol [slot/port]`

Mode ■ Privileged EXEC

Parameter	Definition
Admin Flow Control	The administrative mode of flow control.
Port	The port associated with the rest of the data in the row.
Flow Control Oper	The operational mode of flow control.
RxPause	The received pause frame count.
TxPause	The transmitted pause frame count.

Example: The following shows example CLI display output for the command.

```
(Routing)#show flowcontrol

Admin Flow Control: Symmetric

Port    Flow Control    RxPause    TxPause
        Oper
------  ------------    --------   ---------
0/1     Active          310        611
0/2     Inactive        0          0
--More-- or (q)uit

(Routing)#show flowcontrol interface 0/1

Admin Flow Control: Symmetric

Port       Flow Control  RxPause      TxPause
           Oper
---------  -------       --------     -------
0/1        Active        310          611
```

5.15 Storm-Control Commands

This section describes commands you use to configure storm-control and view storm-control configuration information. A traffic storm is a condition that occurs when incoming packets flood the LAN, which creates performance degradation in the network. The Storm-Control feature protects against this condition.

EFOS provides broadcast, and unicast story recovery for individual interfaces. Unicast Storm-Control protects against traffic whose MAC addresses are not known by the system. For broadcast and unicast storm-control, if the rate of traffic ingressing on an interface increases beyond the configured threshold for that type, the traffic is dropped.

To configure storm-control, you will enable the feature for all interfaces or for individual interfaces, and you will set the threshold (storm-control level) beyond which the broadcast or unicast traffic will be dropped. The Storm-Control feature allows you to limit the rate of specific types of packets through the switch on a per-port, per-type, basis.

Configuring a storm-control level also enables that form of storm-control. Disabling a storm-control level (using the “no” version of the command) sets the storm-control level back to the default value and disables that form of storm-control. Using the “no” version of the “storm-control” command (not stating a “level”) disables that form of storm-control but maintains the configured “level” (to be active the next time that form of storm-control is enabled.)

NOTE: The actual rate of ingress traffic required to activate storm-control is based on the size of incoming packets and the hard-coded average packet size of 512 bytes - used to calculate a packet-per-second (pps) rate - as the forwarding-plane requires pps versus an absolute rate kbps. For example, if the configured limit is 10%, this is converted to ~25000 pps, and this pps limit is set in forwarding plane (hardware). You get the approximate desired output when 512bytes packets are used.

5.15.0.1 storm-control broadcast

Use this command to enable broadcast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If the mode is enabled, broadcast storm recovery is active and, if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.

Default disabled

Format `storm-control broadcast`

Mode
- Global Config
- Interface Config

5.15.0.1.1 no storm-control broadcast

Use this command to disable broadcast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format `no storm-control broadcast`

Mode
- Global Config
- Interface Config

5.15.0.2 storm-control broadcast action

This command configures the broadcast storm recovery action to either `shutdown` or `trap` for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If configured to `shutdown`, the interface that receives the broadcast packets at a rate above the threshold is diagnostically disabled. If set to `trap`, the interface sends trap messages approximately every 30 seconds until broadcast storm control recovers.

Default None

Format `storm-control broadcast action {shutdown | trap}`

Mode
- Global Config
- Interface Config

5.15.0.2.1 no storm-control broadcast action

This command configures the broadcast storm recovery action option to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format `no storm-control broadcast action`

Mode
- Global Config
- Interface Config

5.15.0.3 storm-control broadcast level

Use this command to configure the broadcast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) as a percentage of link speed and enable broadcast storm recovery. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Default 5

Format `storm-control broadcast level` ***0-100***

Mode
- Global Config
- Interface Config

5.15.0.3.1 no storm-control broadcast level

This command sets the broadcast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables broadcast storm recovery.

Format `no storm-control broadcast level`

Mode
- Global Config
- Interface Config

5.15.0.4 storm-control broadcast rate

Use this command to configure the broadcast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) in packets per second. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Default 0

Format `storm-control broadcast rate` *`0-33554431`*

Mode
- Global Config
- Interface Config

5.15.0.4.1 no storm-control broadcast rate

This command sets the broadcast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables broadcast storm recovery.

Format `no storm-control broadcast rate`

Mode
- Global Config
- Interface Config

5.15.0.5 storm-control multicast

This command enables multicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default disabled

Format `storm-control multicast`

Mode
- Global Config
- Interface Config

5.15.0.5.1 no storm-control multicast

This command disables multicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format `no storm-control multicast`

Mode
- Global Config
- Interface Config

5.15.0.6 storm-control multicast action

This command configures the multicast storm recovery action to either `shutdown` or `trap` for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If configured to `shutdown`, the interface that receives multicast packets at a rate above the threshold is diagnostically disabled. The option `trap` sends trap messages approximately every 30 seconds until multicast storm control recovers.

Default None

Format `storm-control multicast action {shutdown | trap}`

Mode
- Global Config
- Interface Config

5.15.0.6.1 no storm-control multicast action

This command returns the multicast storm recovery action option to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format `no storm-control multicast action`

Mode
- Global Config
- Interface Config

5.15.0.7 storm-control multicast level

This command configures the multicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) as a percentage of link speed and enables multicast storm recovery mode. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default 5

Format `storm-control multicast level` *`0-100`*

Mode
- Global Config
- Interface Config

5.15.0.7.1 no storm-control multicast level

This command sets the multicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables multicast storm recovery.

Format `no storm-control multicast level` *`0-100`*

Mode
- Global Config
- Interface Config

5.15.0.8 storm-control multicast rate

Use this command to configure the multicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) in packets per second. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of multicast traffic is limited to the configured threshold.

Default 0

Format `storm-control multicast rate` *`0-33554431`*

Mode
- Global Config
- Interface Config

5.15.0.8.1 no storm-control multicast rate

This command sets the multicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables multicast storm recovery.

Format `no storm-control multicast rate`

Mode
- Global Config
- Interface Config

5.15.0.9 storm-control unicast

This command enables unicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

Default disabled

Format `storm-control unicast`

Mode
- Global Config
- Interface Config

5.15.0.9.1 no storm-control unicast

This command disables unicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format `no storm-control unicast`

Mode
- Global Config
- Interface Config

5.15.0.10 storm-control unicast action

This command configures the unicast storm recovery action to either `shutdown` or `trap` for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode). If configured to `shutdown`, the interface that receives unicast packets at a rate above the threshold is diagnostically disabled. The option `trap` sends trap messages approximately every 30 seconds until unicast storm control recovers.

Default None

Format `storm-control unicast action {shutdown | trap}`

Mode
- Global Config
- Interface Config

5.15.0.10.1 no storm-control unicast action

This command returns the unicast storm recovery action option to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format `no storm-control unicast action`

Mode
- Global Config
- Interface Config

5.15.0.11 storm-control unicast level

This command configures the unicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) as a percentage of link speed, and enables unicast storm recovery. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.This command also enables unicast storm recovery mode for an interface.

Default 5

Format `storm-control unicast level` *`0-100`*

Mode
- Global Config
- Interface Config

5.15.0.11.1 no storm-control unicast level

This command sets the unicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables unicast storm recovery.

Format `no storm-control unicast level`

Mode
- Global Config
- Interface Config

5.15.0.12 storm-control unicast rate

Use this command to configure the unicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) in packets per second. If the mode is enabled, unicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of unicast traffic is limited to the configured threshold.

Default 0

Format `storm-control unicast rate` *`0-33554431`*

Mode
- Global Config
- Interface Config

5.15.0.12.1 no storm-control unicast rate

This command sets the unicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables unicast storm recovery.

Format `no storm-control unicast rate`

Mode
- Global Config
- Interface Config

5.15.0.13 show storm-control

This command displays switch configuration information. If you do not use any of the optional parameters, this command displays global storm control configuration parameters:

- **Broadcast Storm Recovery Mode** may be enabled or disabled. The factory default is disabled.

- **802.3x Flow Control Mode** may be enabled or disabled. The factory default is disabled.

Use the `all` keyword to display the per-port configuration parameters for all interfaces, or specify the `slot/port` to display information about a specific interface.

Format `show storm-control [all | slot/port]`

Mode Privileged EXEC

Parameter	Definition
Bcast Mode	Shows whether the broadcast storm control mode is enabled or disabled. The factory default is disabled.
Bcast Level	The broadcast storm control level.
Mcast Mode	Shows whether the multicast storm control mode is enabled or disabled.
Mcast Level	The multicast storm control level.
Ucast Mode	Shows whether the Unknown Unicast or DLF (Destination Lookup Failure) storm control mode is enabled or disabled.
Ucast Level	The Unknown Unicast or DLF (Destination Lookup Failure) storm control level.

Example: The following shows example CLI display output for the command.

```
(Routing) #show storm-control

Broadcast Storm Control Mode..................... Disable
Broadcast Storm Control Level.................... 5 percent
Broadcast Storm Control Action................... None
Multicast Storm Control Mode..................... Disable
Multicast Storm Control Level.................... 5 percent
Multicast Storm Control Action................... None
Unicast Storm Control Mode....................... Disable
Unicast Storm Control Level...................... 5 percent
Unicast Storm Control Action..................... None
```

Example: The following shows example CLI display output for the command.

```
(Routing) #show storm-control 0/1


       Bcast   Bcast    Bcast      Mcast   Mcast    Mcast      Ucast   Ucast    Ucast
 Intf  Mode    Level    Action     Mode    Level    Action     Mode    Level    Action
------ ------- -------- ---------- ------- -------- ---------- ------- -------- ----------
1/0/1  Disable 5%       None       Disable 5%       None       Disable 5%       None
```

Example: The following shows an example of part of the CLI display output for the command.

```
(Routing) #show storm-control all

     Bcast   Bcast    Bcast     Mcast   Mcast    Mcast     Ucast   Ucast    Ucast
Intf Mode    Level    Action    Mode    Level    Action    Mode    Level    Action
------ -------   --------   ---------- -------   --------   ---------- -------   -------- ----------
0/1  Enable  50        Trap       Disable 5%       None       Disable 5%       None
0/2  Enable  50        Trap       Disable 5%       None       Disable 5%       None
0/3  Enable  50        Trap       Disable 5%       None       Disable 5%       None
0/4  Enable  50        Trap       Disable 5%       None       Disable 5%       None
0/5  Enable  50        Trap       Disable 5%       None       Disable 5%       None
0/6  Enable  50        Trap       Disable 5%       None       Disable 5%       None
0/7  Enable  50        Trap       Disable 5%       None       Disable 5%       None
```

```
0/8  Enable  50        Trap       Disable 5%       None       Disable 5%       None
0/9  Enable  50        Trap       Disable 5%       None       Disable 5%       None
0/10 Enable  50        Trap       Disable 5%       None       Disable 5%       None
0/11 Enable  50        Trap       Disable 5%       None       Disable 5%       None
0/12 Enable  50        Trap       Disable 5%       None       Disable 5%       None
0/13 Enable  50        Trap       Disable 5%       None       Disable 5%       None
0/14 Enable  50        Trap       Disable 5%       None       Disable 5%       None
0/15 Enable  50        Trap       Disable 5%       None       Disable 5%       None
0/16 Enable  50        Trap       Disable 5%       None       Disable 5%       None
0/17 Enable  50        Trap       Disable 5%       None       Disable 5%       None
0/18 Enable  50        Trap       Disable 5%       None       Disable 5%       None
0/19 Enable  50        Trap       Disable 5%       None       Disable 5%       None
```

5.16 Link Dependency Commands

The following commands configure link dependency. Link dependency allows the link status of specified ports to be dependent on the link status of other ports. Consequently, if a port that is depended on by other ports loses link, the dependent ports are administratively disabled or administratively enabled so that the dependent ports links are brought down or up respectively.

5.16.0.1 link state track

A link-dependency group is configured if the upstream and downstream interfaces are configured for group.

Use this command to set link-dependency options for the selected group identifier.

Format `link state track` *`group-id`*
Mode Global Config

5.16.0.1.1 no link state track

This command clears link-dependency options for the selected group identifier.

Format `no link state track` *`group-id`*
Mode Global Config

5.16.0.2 link state group

Use this command to indicate if the downstream interfaces of the group should mirror or invert the status of the upstream interfaces. The default configuration for a group is down (that is, the downstream interfaces will mirror the upstream link status by going down when all upstream interfaces are down). The action up option causes the downstream interfaces to be up when no upstream interfaces are down.

Default Down
Format `link state group` *`group-id`* `action {up | down}`
Mode Global Config

5.16.0.2.1 no link state group

Use this command to restore the link state to down for the group.

Format `no link state group` *`group-id`* `action`
Mode Global Config

5.16.0.3 link state group downstream

Use this command to add interfaces to the downstream interface list. Adding an interface to a downstream list brings the interface down until an upstream interface is added to the group. The link status then follows the interface specified in the upstream command. To avoid bringing down interfaces, enter the upstream command prior to entering the downstream command.

Format `link state group` *`group-id`* `downstream`
Mode Interface Config

5.16.0.3.1 no link state group downstream

Use this command to remove the selected interface from the downstream list.

Format `no link state group` *`group-id`* `downstream`
Mode Interface Config

5.16.0.4 link state group upstream

Use this command to add interfaces to the upstream interface list. Note that an interface that is defined as an upstream interface cannot also be defined as a downstream interface in the same link state group or as a downstream interface in a different link state group, if either configuration creates a circular dependency between groups.

Format `link state group` *`group-id`* `upstream`
Mode Interface Config

5.16.0.4.1 no link state group upstream

Use this command to remove the selected interfaces from upstream list.

Format `no link state group` *`group-id`* `upstream`
Mode Interface Config

5.16.0.5 show link state group

Use this command to display information for all configured link-dependency groups or a specified link-dependency group.

Format `show link state group` *`group-id`*
Mode Privileged EXEC

Example: This example displays information for all configured link-dependency groups.

```
(Switching)#show link-state group

GroupId Downstream Interfaces      Upstream Interfaces  Link Action Group State
------- ------------------------- -------------------- ----------- -----------
1       2/0/3-2/0/7,2/0/12-2/0/17  2/0/12-2/0/32,0/3/5  Link Up     Up
4       2/0/18,2/0/27              2/0/22-2/0/33,0/3/1  Link Up     Down
```

Example: This example displays information for a specified link-dependency groups

```
(Switching)#show link state group 1

GroupId Downstream Interfaces      Upstream Interfaces  Link Action Group State
------- ------------------------- -------------------- ----------- -----------
1       2/0/3-2/0/7,2/0/12-2/0/17  2/0/12-2/0/32,0/3/5  Link Up     Up
```

5.16.0.6 show link state group detail

Use this command to display detailed information about the state of upstream and downstream interfaces for a selected link-dependency group. Group Transitions is a count of the number of times the downstream interface has gone into its “action” state as a result of the upstream interfaces link state.

Format `show link state group` *`group-id`* `detail`

Mode Privileged EXEC

```
(Switching) # show link state group 1 detail
GroupId:     1
Link Action: Up
Group State: Up

Downstream Interface State:
Link Up:     2/0/3
Link Down:   2/0/4-2/0/7,2/0/12-2/0/17

Upstream Interface State:
Link Up:     -
Link Down:  2/0/12-2/0/32,0/3/5

Group Transitions: 0
Last Transition Time: 00:52:35 (UTC+0:00) Jan 1 1970
```

5.17 Link Local Protocol Filtering Commands

Link Local Protocol Filtering (LLPF) allows the switch to filter out multiple proprietary protocol PDUs, such as Port Aggregation Protocol (PAgP), if the problems occur with proprietary protocols running on standards-based switches. If certain protocol PDUs cause unexpected results, LLPF can be enabled to prevent those protocol PDUs from being processed by the switch.

NOTE: LLPF is supported on the efos platforms.

5.17.0.1 llpf

Use this command to block LLPF protocol(s) on a port.

Default	Enabled for the blockudld parameter; disabled for all others.
Format	`llpf {blockisdp | blockvtp | blockdtp | blockudld | blockpagp | blocksstp | blockall}`
Mode	Interface Config

5.17.0.1.1 no llpf

Use this command to unblock LLPF protocol(s) on a port.

Format	`no llpf {blockisdp | blockvtp | blockdtp | blockudld | blockpagp | blocksstp | blockall }`
Mode	Interface Config

5.17.0.2 show llpf interface all

Use this command to display the status of LLPF rules configured on a particular port or on all ports.

Format	`show llpf interface [all | slot/port]`
Mode	Privileged EXEC

Parameter	Definition
Block ISDP	Shows whether the port blocks ISDP PDUs.
Block VTP	Shows whether the port blocks VTP PDUs.
Block DTP	Shows whether the port blocks DTP PDUs.
Block UDLD	Shows whether the port blocks UDLD PDUs.
Block PAGP	Shows whether the port blocks PAgP PDUs.
Block SSTP	Shows whether the port blocks SSTP PDUs.
Block All	Shows whether the port blocks all proprietary PDUs available for the LLDP feature.

5.18 MVR Commands

This section lists the Multicast VLAN Registration (MVR) commands.

5.18.0.1 mvr

Use this command to enable MVR. This is disabled by default.

Default	Disabled
Format	`mvr`
Mode	Interface Config; Global Config

5.18.0.1.1 no mvr

Use this command to disable MVR.

Format	`no mvr`
Mode	Interface Config; Global Config

5.18.0.2 mvr group

Use this command to add an MVR membership group.

Format	`mvr group`
Mode	Global Config

5.18.0.2.1 no mvr group

Use this command to disable an MVR membership group.

Format	`no mvr group`
Mode	Global Config

5.18.0.3 mvr immediate

Use this command to enable MVR Immediate Leave mode. If the interface is configured as source port, MVR Immediate Leave mode cannot be enabled. MVR Immediate Leave mode disabled by default.

Default	Disabled
Format	`mvr immediate`
Mode	Interface Config

5.18.0.3.1 no mvr immediate

Use this command to disable MVR Immediate Leave mode.

Format	`mvrm immediate`
Mode	Interface Config

5.18.0.4 mvr mode

Use this command to change the MVR mode type. Compatible is the default mode type.

Format `mvr mode [compatible | dynamic]`
Mode Global Config

5.18.0.4.1 no mvr mode

Use this command to set the MVR mode type to the default value of compatible.

Format `no mvr mode`
Mode Global Config

5.18.0.5 mvr querytime

Use this command to set the MVR query response time in units of tenths of a second. The query time is the maximum time to wait for an IGMP membership report on a receiver port before removing the port from the multicast group. The query time only applies to receiver ports and is specified in tenths of a second. The default is 5.

Format `mvr querytime` *`1-100`*
Mode Global Config

5.18.0.5.1 no mvr querytime

Use this command to set the MVR query response time to the default value.

Format `no mvr querytime`
Mode Global Config

5.18.0.6 mvr type

Use this command to set the MVR port type. The default is none.

Format `mvr type [receiver | source]`
Mode Interface Config

5.18.0.6.1 no mvr type

Use this command to reset the MVR port type to None.

Format `no mvr type`
Mode Interface Config

5.18.0.7 mvr vlan

Use this command to set the MVR multicast VLAN.

Default	1
Format	`mvr vlan` *`1-4093`*
Mode	Global Config

5.18.0.7.1 no mvr vlan

Use this command to set the MVR multicast VLAN to the default value.

Format	`no mvr vlan`
Mode	Global Config

5.18.0.8 mvr vlan group

Use this command to make a port participate in a specific MVR group. The default value is None.

Format	`mvr vlan` *`mvlan`* `group` *`A.B.C.D.`*
Mode	Interface Config

5.18.0.8.1 no mvr vlan group

Use this command to remove port participation in the specific MVR group.

Format	`no mvr vlan` *`mvlan`* `group` *`A.B.C.D.`*
Mode	Interface Config

5.18.0.9 show mvr

Use this command to display global MVR settings.

Format	`show mvr`
Mode	Privileged EXEC

Example:

```
(Switching) #  show mvr
MVR Disabled.

(Switching) #  show mvr
MVR Running...................... TRUE
MVR multicast VLAN............... 1
MVR Max Multicast Groups.......... 256
MVR Current multicast groups...... 0
MVR Global query response time.... 5 (tenths of sec)
MVR Mode......................... compatible
```

5.18.0.10 show mvr members

Use this command to display the allocated MVR membership groups.

Format	`show mvr members [`*`A.B.C.D.`*`]`

Mode Privileged EXEC

Example:

```
(Switching) # show mvr members
MVR Disabled

(Switching) # show mvr members

MVR Group IP        Status              Members
---------------     ---------------     --------------------------------
224.1.1.1           INACTIVE            1/0/1, 1/0/2, 1/0/3

(Switching) # show mvr members 224.1.1.1

MVR Group IP        Status              Members
---------------     ---------------     --------------------------------
224.1.1.1           INACTIVE            1/0/1, 1/0/2, 1/0/3
```

5.18.0.11 show mvr interface

Use this command to display the configuration of MVR-enabled interfaces.

Format `show mvr interface [`*`interface-id`* `[members [vlan` *`vlan-id`*`]]]`

Mode Privileged EXEC

Example:

```
(Switching) # show mvr interface
Port        Type            Status              Immediate Leave
----------- --------------- ------------------- ---------------
1/0/9       RECEIVER        ACTIVE/inVLAN       DISABLED

(Switching) # show mvr interface 0/4

Type: NONE   Status: INACTIVE/InVLAN  Immediate Leave: DISABLED

show mvr interface 1/0/23 members
235.0.0.1 STATIC  ACTIVE

(Switching) # show mvr interface 1/0/23 members vlan 12
235.0.0.1 STATIC  ACTIVE
235.1.1.1 STATIC  ACTIVE
```

5.18.0.12 show mvr traffic

Use this command to display global MVR statistics.

Format `show mvr traffic`

Mode Privileged EXEC

Example:

```
(Switching) # show mvr traffic
```

```
IGMP Query Received.............. 0
IGMP Report V1 Received.......... 0
IGMP Report V2 Received.......... 0
IGMP Leave Received.............. 0
IGMP Query Transmitted........... 0
IGMP Report V1 Transmitted....... 0
IGMP Report V2 Transmitted....... 0
IGMP Leave Transmitted........... 0
IGMP Packet Receive Failures..... 0
IGMP Packet Transmit Failures..... 0
```

5.18.0.13 debug mvr trace

Use this command to enable MVR debug tracing. The default value is disabled.

Format `debug mvr trace`
Mode Privileged EXEC

5.18.0.13.1 no debug mvr trace

Use this command to disable MVR debug tracing.

Format `no debug mvr trace`
Mode Privileged EXEC

5.18.0.14 debug mvr packet

Use this command to enable MVR receive/transmit packets debug tracing. If it is executed without specifying the arguments, both receive and transmit packets debugging is enabled. The default is enabled.

Format `debug mvr packet [receive | transmit]`
Mode Privileged EXEC

5.18.0.14.1 no debug mvr packet

Use this command to disable MVR receive/transmit packet debug tracing.

Format `no debug mvr packet [receive | transmit]`
Mode Privileged EXEC

5.19 Port-Channel/LAG (802.3ad) Commands

This section describes the commands you use to configure port-channels, which is defined in the 802.3ad specification, and that are also known as link aggregation groups (LAGs). Link aggregation allows you to combine multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and provides load sharing. The LAG feature initially load shares traffic based upon the source and destination MAC address. Assign the port-channel (LAG) VLAN membership after you create a port-channel. If you do not assign VLAN membership, the port-channel might become a member of the management VLAN which can result in learning and switching issues.

A port-channel (LAG) interface can be either static or dynamic, but not both. All members of a port channel must participate in the same protocols.) A static port-channel interface does not require a partner system to be able to aggregate its member ports.

NOTE: If you configure the maximum number of dynamic port-channels (LAGs) that your platform supports, additional port-channels that you configure are automatically static.

5.19.0.1 port-channel

This command configures a new port-channel (LAG) and generates a logical *slot/port* number for the port-channel. The `name` field is a character string which allows the dash "-" character as well as alphanumeric characters. Use the `show port-channel` command to display the *slot/port* number for the logical interface.

NOTE: Before you include a port in a port-channel, set the port physical mode. For more information, see Section 5.1.0.10, speed.

Format `port-channel` *name*
Mode Global Config

5.19.0.2 addport

This command adds one port to the port-channel (LAG). The first interface is a logical *slot/port* number of a configured port-channel. You can add a range of ports by specifying the port range when you enter Interface Config mode (for example: `interface 0/1-0/4`.

NOTE: Before adding a port to a port-channel, set the physical mode of the port. For more information, see Section 5.1.0.10, speed.

Format `addport` *logical slot/port*
Mode Interface Config

5.19.0.3 deleteport (Interface Config)

This command deletes a port or a range of ports from the port-channel (LAG). The interface is a logical *slot/port* number of a configured port-channel (or range of port-channels).

Format `deleteport` *logical slot/port*
Mode Interface Config

5.19.0.4 deleteport (Global Config)

This command deletes all configured ports from the port-channel (LAG). The interface is a logical *slot/port* number of a configured port-channel.

Format `deleteport {`*`logical slot/port`* `| all}`

Mode Global Config

5.19.0.5 lacp admin key

Use this command to configure the administrative value of the key for the port-channel. The value range of *key* is 0 to 65535.

Default 0x8000

Format `lacp admin key` *`key`*

Mode Interface Config

NOTE: This command is applicable only to port-channel interfaces.

This command can be used to configure a single interface or a range of interfaces.

5.19.0.5.1 no lacp admin key

Use this command to configure the default administrative value of the key for the port-channel.

Format `no lacp admin key`

Mode Interface Config

5.19.0.6 lacp collector max-delay

Use this command to configure the port-channel collector max delay. This command can be used to configure a single interface or a range of interfaces.The valid range of `delay` is 0-65535.

Default 0x8000

Format `lacp collector max delay` *`delay`*

Mode Interface Config

NOTE: This command is applicable only to port-channel interfaces.

5.19.0.6.1 no lacp collector max delay

Use this command to configure the default port-channel collector max delay.

Format `no lacp collector max delay`

Mode Interface Config

5.19.0.7 lacp actor admin key

Use this command to configure the administrative value of the LACP actor admin key on an interface or range of interfaces. The valid range for `key` is 0-65535.

Default Internal Interface Number of this Physical Port

Format `lacp actor admin key` *`key`*

Mode Interface Config

NOTE: This command is applicable only to physical interfaces.

5.19.0.7.1 no lacp actor admin key

Use this command to configure the default administrative value of the key.

Format `no lacp actor admin key`
Mode Interface Config

5.19.0.8 lacp actor admin state

Use this command to configure the administrative value of actor state as transmitted by the Actor in LACPDUs. This command can be used to configure a single interfaces or a range of interfaces.

Default 0x07
Format `lacp actor admin state {individual|longtimeout|passive}`
Mode Interface Config

NOTE: This command is applicable only to physical interfaces.

5.19.0.8.1 no lacp actor admin state

Use this command the configure the default administrative values of actor state as transmitted by the Actor in LACPDUs.

NOTE: Both the `no portlacptimeout` and the `no lacp actor admin state` commands set the values back to default, regardless of the command used to configure the ports. Consequently, both commands will display in `show running-config`.

Format `no lacp actor admin state {individual|longtimeout|passive}`
Mode Interface Config

5.19.0.9 lacp actor port priority

Use this command to configure the priority value assigned to the Aggregation Port for an interface or range of interfaces. The valid range for `priority` is 0 to 65535.

Default 0x80
Format `lacp actor port priority` *`0-65535`*
Mode Interface Config

NOTE: This command is applicable only to physical interfaces.

5.19.0.9.1 no lacp actor port priority

Use this command to configure the default priority value assigned to the Aggregation Port.
Format `no lacp actor port priority`

Mode Interface Config

5.19.0.10 lacp partner admin key

Use this command to configure the administrative value of the Key for the protocol partner. This command can be used to configure a single interface or a range of interfaces. The valid range for `key` is 0 to 65535.

Default 0x0

Format `lacp partner admin key` *`key`*

Mode Interface Config

NOTE: This command is applicable only to physical interfaces.

5.19.0.10.1 no lacp partner admin key

Use this command to set the administrative value of the Key for the protocol partner to the default.

Format `no lacp partner admin key`

Mode Interface Config

5.19.0.11 lacp partner admin state

Use this command to configure the current administrative value of actor state for the protocol Partner.

Format `lacp partner admin state {individual|longtimeout|passive}`

Mode Interface Config

NOTE: This command is applicable only to physical interfaces.

5.19.0.11.1 no lacp partner admin state

Use this command the configure the default current administrative value of actor state for the protocol partner. This command can be used to configure a single interface or a range of interfaces.

Format `no lacp partner admin state {individual|longtimeout|passive}`

Mode Interface Config

5.19.0.12 lacp partner port id

Use this command to configure the LACP partner port id. This command can be used to configure a single interface or a range of interfaces. The valid range for `port-id` is 0 to 65535.

Default 0x80

Format `lacp partner port-id` *`port-id`*

Mode Interface Config

NOTE: This command is applicable only to physical interfaces.

5.19.0.12.1 no lacp partner port id

Use this command to set the LACP partner port id to the default.

Format `no lacp partner port-id`

Mode Interface Config

5.19.0.13 lacp partner port priority

Use this command to configure the LACP partner port priority. This command can be used to configure a single interface or a range of interfaces. The valid range for `priority` is 0 to 65535.

Default 0x0

Format `lacp partner port priority` ***priority***

Mode Interface Config

NOTE: This command is applicable only to physical interfaces.

5.19.0.13.1 no lacp partner port priority

Use this command to configure the default LACP partner port priority.

Format `no lacp partner port priority`

Mode Interface Config

5.19.0.14 lacp partner system-id

Use this command to configure the 6-octet MAC Address value representing the administrative value of the Aggregation Port's protocol Partner's System ID. This command can be used to configure a single interface or a range of interfaces. The valid range of `system-id` is 00:00:00:00:00:00 - FF:FF:FF:FF:FF.

Default 00:00:00:00:00:00

Format `lacp partner system-id` ***system-id***

Mode Interface Config

NOTE: This command is applicable only to physical interfaces.

5.19.0.14.1 no lacp partner system-id

Use this command to configure the default value representing the administrative value of the Aggregation Port's protocol Partner's System ID.

Format `no lacp partner system-id`

Mode Interface Config

5.19.0.15 lacp partner system priority

Use this command to configure the administrative value of the priority associated with the Partner's System ID. This command can be used to configure a single interface or a range of interfaces. The valid range for `priority` is 0 to 65535.

Default 0x0

Format `lacp partner system priority` ***0-65535***

Mode Interface Config

NOTE: This command is applicable only to physical interfaces.

5.19.0.15.1 no lacp partner system priority

Use this command to configure the default administrative value of priority associated with the Partner's System ID.

Format `no lacp partner system priority`
Mode Interface Config

5.19.0.16 interface lag

Use this command to enter Interface configuration mode for the specified LAG.

Format `interface lag lag-interface-number`
Mode Global Config

5.19.0.17 ip resilient-hashing

Use this command to enable resilient hashing on all ECMP objects on the router. The default value is enabled.

NOTE: This command takes effect after reboot. The behavior of the system after executing the command and before rebooting the switch is undefined. The user is asked to confirm before proceeding. After successful execution of the command, the User is asked to reboot the switch.

Format `ip resilient-hashing`
Mode Global Config

5.19.0.17.1 no ip resilient-hashing

Use this command to disable resilient hashing on all the ECMP objects on the router.

NOTE: This command takes effect after reboot. The behavior of the system after executing the command and before rebooting the switch is undefined. The user is asked to confirm before proceeding. After successful execution of the command, the User is asked to reboot the switch.

Format `no ip resilient-hashing`
Mode Global Config

5.19.0.18 port-channel resilient-hashing

Use this command to enable resilient hashing on all port-channels on the switch. The default is enabled.

NOTE: This command takes effect after reboot. The behavior of the system after executing the command and before rebooting the switch is undefined. The user must confirm before proceeding.

Format `port-channel resilient-hashing`
Mode Global Config

5.19.0.18.1 no port-channel resilient-hashing

Use this command to disable resilient hashing on all the trunk ports on the switch.

Format	`no port-channel resilient-hashing`
Mode	Global Config

NOTE: This command takes effect after reboot. The behavior of the system after executing the command and before rebooting the switch is undefined. The user is asked to confirm before proceeding. After completion, the User is asked to reboot the switch

5.19.0.19 port-channel static

This command enables the static mode on a port-channel (LAG) interface or range of interfaces. By default the static mode for a new port-channel is enabled, which means the port-channel is static. If the maximum number of allowable dynamic port-channels are already present in the system, the static mode for a new port-channel is enabled, which means the port-channel is static. You can only use this command on port-channel interfaces.

Default	enabled
Format	`port-channel static`
Mode	Interface Config

5.19.0.19.1 no port-channel static

This command sets the static mode on a particular port-channel (LAG) interface to the default value. This command will be executed only for interfaces of type port-channel (LAG).

Format	`no port-channel static`
Mode	Interface Config

5.19.0.20 port lacpmode

This command enables Link Aggregation Control Protocol (LACP) on a port or range of ports.

Default	enabled
Format	`port lacpmode`
Mode	Interface Config

5.19.0.20.1 no port lacpmode

This command disables Link Aggregation Control Protocol (LACP) on a port.

Format	`no port lacpmode`
Mode	Interface Config

5.19.0.21 port lacpmode enable all

This command enables Link Aggregation Control Protocol (LACP) on all ports.

Format `port lacpmode enable all`
Mode Global Config

5.19.0.21.1 no port lacpmode enable all

This command disables Link Aggregation Control Protocol (LACP) on all ports.

Format `no port lacpmode enable all`
Mode Global Config

5.19.0.22 port lacptimeout (Interface Config)

This command sets the timeout on a physical interface or range of interfaces of a particular device type (actor or partner) to either long or short timeout.

Default long
Format `port lacptimeout {actor | partner} {long | short}`
Mode Interface Config

5.19.0.22.1 no port lacptimeout

This command sets the timeout back to its default value on a physical interface of a particular device type (actor or partner).

NOTE: Both the `no portlacptimeout` and the `no lacp actor admin state` commands set the values back to default, regardless of the command used to configure the ports. Consequently, both commands will display in `show running-config`.

Format `no port lacptimeout {actor | partner}`
Mode Interface Config

5.19.0.23 port lacptimeout (Global Config)

This command sets the timeout for all interfaces of a particular device type (actor or partner) to either long or short timeout.

Default long
Format `port lacptimeout {actor | partner} {long | short}`
Mode Global Config

5.19.0.23.1 no port lacptimeout

This command sets the timeout for all physical interfaces of a particular device type (actor or partner) back to their default values.

NOTE: Both the `no portlacptimeout` and the `no lacp actor admin state` commands set the values back to default, regardless of the command used to configure the ports. Consequently, both commands will display in `show running-config`.

Format `no port lacptimeout {actor | partner}`

Mode Global Config

5.19.0.24 port-channel adminmode

This command enables all configured port-channels with the same administrative mode setting.

Format `port-channel adminmode all`
Mode Global Config

5.19.0.24.1 no port-channel adminmode

This command disables all configured port-channels with the same administrative mode setting.

Format `no port-channel adminmode all`
Mode Global Config

5.19.0.25 port-channel linktrap

This command enables link trap notifications for the port-channel (LAG). The interface is a logical *slot/port* for a configured port-channel. The option `all` sets every configured port-channel with the same administrative mode setting.

Default enabled
Format `port-channel linktrap {`*`logical slot/port`* `| all}`
Mode Global Config

5.19.0.25.1 no port-channel linktrap

This command disables link trap notifications for the port-channel (LAG). The interface is a logical slot and port for a configured port-channel. The option `all` sets every configured port-channel with the same administrative mode setting.

Format `no port-channel linktrap {`*`logical slot/port`* `| all}`
Mode Global Config

5.19.0.26 port-channel load-balance

This command selects the load-balancing option used on a port-channel (LAG). Traffic is balanced on a port-channel (LAG) by selecting one of the links in the channel over which to transmit specific packets. The link is selected by creating a binary pattern from selected fields in a packet, and associating that pattern with a particular link.

Load-balancing is not supported on every device. The range of options for load-balancing may vary per device.

This command can be configured for a single interface, a range of interfaces, or all interfaces.

Default 3
Format `port-channel load-balance {1 | 2 | 3 | 4 | 5 | 6 | 7} {`*`slot/port`* `| all}`
Mode Interface Config
Global Config

Parameter	Definition
1	Source MAC, VLAN, EtherType, and incoming port associated with the packet
2	Destination MAC, VLAN, EtherType, and incoming port associated with the packet
3	Source/Destination MAC, VLAN, EtherType, and incoming port associated with the packet
4	Source IP and Source TCP/UDP fields of the packet
5	Destination IP and Destination TCP/UDP Port fields of the packet
6	Source/Destination IP and source/destination TCP/UDP Port fields of the packet
7	Enhanced hashing mode
slot/port| all	Global Config Mode only: The interface is a logical *slot/port* number of a configured port-channel. `All` applies the command to all currently configured port-channels.

5.19.0.26.1 no port-channel load-balance

This command reverts to the default load balancing configuration.

Format `no port-channel load-balance {`*slot/port* | `all}`
Mode Interface Config
Global Config

Parameter	Definition
slot/port| **all**	Global Config Mode only: The interface is a logical *slot/port* number of a configured port-channel. **All** applies the command to all currently configured port-channels.

5.19.0.27 port-channel min-links

This command configures the port-channel's minimum links for lag interfaces.

Default `1`
Format `port-channel min-links` *1-8*
Mode Interface Config

5.19.0.28 port-channel name

This command defines a name for the port-channel (LAG). The interface is a logical *slot/port* for a configured port-channel, and `name` is an alphanumeric string up to 15 characters.

Format `port-channel name {`*logical slot/port*`}` *name*
Mode Global Config

5.19.0.29 port-channel system priority

Use this command to configure port-channel system priority. The valid range of *priority* is 0-65535.

Default 0x8000
Format `port-channel system priority` *priority*
Mode Global Config

5.19.0.29.1 no port-channel system priority

Use this command to configure the default port-channel system priority value.

Format `no port-channel system priority`
Mode Global Config

5.19.0.30 show hashdest

Use this command to predict how packets are forwarded over a LAG or to the next hop device when ECMP is the destination. Given the link aggregation method, ingress physical port and values of various packet fields, this command predicts an egress physical port within the LAG or ECMP for the packet.

Format `show hashdest {lag` ***lag-id*** `| ecmp` ***prefix/prefix-length***`} in_port` ***slot/port*** `src-mac` ***macaddr*** `dst-mac` ***macaddr*** `[vlan` ***vlan-id***`] ethertype` ***0xXXXX*** `[src-ip {`***ipv4-addr*** `|` ***ipv6-addr***`} dst-ip {`***ipv4-addr*** `|` ***ipv6-addr***`} protocol` ***pid*** `src-l4-port` ***port-num*** `dst-l4-port` ***port-num***`]`
Mode Privileged EXEC

Parameter	Definition
lag	The LAG group for which to display the egress physical port.
ecmp	The IP address of the EMC_ group for which to display the egress physical port.
in_port	The incoming physical port for the system.
src-mac	The source MAC address.
dst-mac	The destination MAC address.
vlan	The VLAN ID for VLAN-tagged packets. Do not use this parameter or enter 0 for non-VLAN-tagged packets.
ethertype	The 16-bit EtherType value, in the form *0xXXXX*. For layer 3 packets, hash prediction is only available for IPv4 (0x0800) and IPv6 (0x86DD).
src-ip	The source IP address, entered as *x.x.x.x* for IPv4 or *x:x:x:x:x:x:x:x* for IPv6 packets.
dst-ip	The destination IP address, entered as *x.x.x.x* for IPv4 or *x:x:x:x:x:x:x:x* for IPv6 packets.
protocol	The protocol ID.
src-l4-port	The layer 4 source port.
dst-l4-port	The layer 4 destination port.

Example: Layer 2 VLAN tagged packet forwarded to a LAG

```
(Routing) #show hashdest lag 1 in_port 0/3 src-mac 00:00:20:21:AE:8A dst-mac 00:10:18:99:F7:4E vlan
10 ethertype 0x8870

LAG            Destination Port
-----------     ----------------
1                  0/29
```

Example: Layer 2 non-VLAN tagged packet forwarded to a LAG

```
(Routing) # show hashdest lag 1 in_port 0/3 src-mac 00:00:20:21:AE:8A dst-mac 00:10:18:99:F7:4E
ethertype 0x8870

LAG           Destination Port
-----------     ----------------
1          0/31
```

Example: Non-VLAN tagged IPv4 UDP packet forwarded to a LAG

```
(Routing) #show hashdest lag 1 in_port 0/3 src-mac 00:00:20:21:AE:8A dst-mac 00:10:18:99:F7:4E
ethertype 0x0800 src-ip 7.0.0.2 dst-ip 3.0.0.2 protocol 17 src-l4-port 63 dst-l4-port 64

LAG            Destination Port
-----------     ----------------
1                  0/32
```

Example: VLAN tagged IPv4 TCP packet forwarded to a LAG

```
(Routing) #show hashdest lag 1 in_port 0/3 src-mac 00:00:20:21:AE:8A dst-mac 00:10:18:99:F7:4E vlan
10 ethertype 0x0800 src-ip 7.0.0.2 dst-ip 3.0.0.2 protocol 6 src-l4-port 67 dst-l4-port 68

LAG           Destination Port
-----------     ----------------
1                 0/31
```

Example: Non-VLAN tagged IPv4 UDP packet forwarded to an ECMP group

```
(Routing) #show hashdest ecmp  10.0.0.2/16 in_port 0/3 src-mac 00:00:20:21:AE:8A dst-mac
00:10:18:99:F7:4E vlan 0 ethertype 0x0800 src-ip 7.0.0.2 dst-ip 3.0.0.2 protocol 17 src-l4-port 63
dst-l4-port 64

Egress Port
---------------------------
30.0.0.2 on interface 0/31
```

Example: VLAN tagged IPv4 TCP packet forwarded to an ECMP group

```
(Routing) #show hashdest ecmp 10.0.0.2/16 in_port 0/3 src-mac 00:00:20:21:AE:8A dst-mac
00:10:18:99:F7:4E vlan 10 ethertype 0x0800 src-ip 7.0.0.2 dst-ip 3.0.0.2 protocol 6 src-l4-port 67
dst-l4-port 68

Egress Port
-----------
0/29
```

Example: Non-VLAN tagged IPv6 UDP packet forwarded to an ECMP group

```
(Routing) #show hashdest ecmp 4001::200/64 in_port 0/3 src-mac 00:00:20:21:AE:8A dst-mac
00:10:18:99:F7:4E ethertype 0x86dd src-ip 7001:0:0:0:0:0:0:2 dst-ip 3001:0:0:0:0:0:0:2 protocol 17
src-l4-port 63 dst-l4-port 64

Egress Port
---------------------------
6001::200 on interface 0/31
```

Example: Non-VLAN tagged IPv6 TCP packet forwarded to an ECMP group

```
(Routing) #show hashdest ecmp 6001::200/64 in_port 0/3 src-mac 00:00:20:21:AE:8A dst-mac
00:10:18:99:F7:4E ethertype 0x86dd src-ip 7001:0:0:0:0:0:0:2 dst-ip 3001:0:0:0:0:0:0:2 protocol 6 src-
l4-port 67 dst-l4-port 68

Egress Port
---------------------------
8001::200 on interface 0/32
```

5.19.0.31 show ip resilient-hashing

Use this command to display the resilient hashing property for the ECMP.

Format	`show ip resilient-hashing`
Mode	Privileged EXEC

Term	Definition
Resilient Hashing	Resilient hashing mode for the system.

Example:

```
(Routing) #show ip resilient-hashing

Resilient Hashing.............................. Enabled

(Routing)#
```

5.19.0.32 show lacp actor

Use this command to display LACP actor attributes.

Format `show lacp actor {`*`slot/port`*`|all}`
Mode Global Config

The following output parameters are displayed.

Parameter	Description
System Priority	The administrative value of the Key.
Actor Admin Key	The administrative value of the Key.
Port Priority	The priority value assigned to the Aggregation Port.
Admin State	The administrative values of the actor state as transmitted by the Actor in LACPDUs.

5.19.0.33 show lacp partner

Use this command to display LACP partner attributes.

Format `show lacp actor {`*`slot/port`*`|all}`
Mode Privileged EXEC

The following output parameters are displayed.

Parameter	Description
System Priority	The administrative value of priority associated with the Partner's System ID.
System-ID	Represents the administrative value of the Aggregation Port's protocol Partner's System ID.
Admin Key	The administrative value of the Key for the protocol Partner.
Port Priority	The administrative value of the Key for protocol Partner.
Port-ID	The administrative value of the port number for the protocol Partner.
Admin State	The administrative values of the actor state for the protocol Partner.

5.19.0.34 show port-channel brief

This command displays the static capability of all port-channel (LAG) interfaces on the device as well as a summary of individual port-channel interfaces.

Format `show port-channel brief`

Mode
- Privileged EXEC
- User EXEC

For each port-channel the following information is displayed:

Parameter	Definition
Logical Interface	The *slot/port* of the logical interface.
Port-channel Name	The name of port-channel (LAG) interface.
Link-State	Shows whether the link is up or down.
Trap Flag	Shows whether trap flags are enabled or disabled.
Type	Shows whether the port-channel is statically or dynamically maintained.
Mbr Ports	The members of this port-channel.
Active Ports	The ports that are actively participating in the port-channel.

5.19.0.35 show port-channel

This command displays an overview of all port-channels (LAGs) on the switch. Instead of `slot/port`, `lag lag-intf-num` can be used as an alternate way to specify the LAG interface. `lag lag-intf-num` can also be used to specify the LAG interface where `lag-intf-num` is the LAG port number.

Format `show port-channel`

Mode
- Privileged EXEC

Term	Definition
Logical Interface	The valid slot/port number.
Port-Channel Name	The name of this port-channel (LAG). You may enter any string of up to 15 alphanumeric characters.
Link State	Indicates whether the Link is up or down.
Admin Mode	May be enabled or disabled. The factory default is enabled.
Type	The status designating whether a particular port-channel (LAG) is statically or dynamically maintained. ■ **Static** - The port-channel is statically maintained. ■ **Dynamic** - The port-channel is dynamically maintained.
Load Balance Option	The load balance option associated with this LAG. See Section 5.19.0.26, port-channel load-balance.
Local Preference Mode	Indicates whether the local preference mode is **enabled** or **disabled**.
Mbr Ports	A listing of the ports that are members of this port-channel (LAG), in *slot/port* notation. There can be a maximum of eight ports assigned to a given port-channel (LAG).
Device Timeout	For each port, lists the timeout (**long** or **short**) for Device Type (**actor** or **partner**).
Port Speed	Speed of the port-channel port.
Active Ports	This field lists ports that are actively participating in the port-channel (LAG).

Example: The following shows example CLI display output for the command.

```
(Switch) #show port-channel 3/1


Local Interface................................ 3/1
```

```
Channel Name..................................... ch1
Link State....................................... Up
Admin Mode....................................... Enabled
Type............................................. Static
Load Balance Option.............................. 3
(Src/Dest MAC, VLAN, EType, incoming port)
Local Preference Mode............................ Enabled

Mbr    Device/       Port      Port
Ports  Timeout       Speed     Active
------ ------------- --------- -------
0/1    actor/long    Auto      True
       partner/long
0/2    actor/long    Auto      True
       partner/long
0/3    actor/long    Auto      False
       partner/long
0/4    actor/long    Auto      False
       partner/long
```

5.19.0.36 show port-channel counters

Use this command to display port-channel counters for the specified port.

Format `show port-channel` *`slot/port`* `counters`

Mode Privileged EXEC

Term	Definition
Local Interface	The valid slot/port number.
Channel Name	The name of this port-channel (LAG).
Link State	Indicates whether the Link is up or down.
Admin Mode	May be enabled or disabled. The factory default is enabled.
Port Channel Flap Count	The number of times the port-channel was inactive.
Mbr Ports	The slot/port for the port member.
Mbr Flap Counters	The number of times a port member is inactive, either because the link is down, or the admin state is disabled.

Example: The following shows example CLI display output for the command.

```
(Switch) #show port-channel 0/3/1 counters


Local Interface.............................. 3/1
Channel Name................................. ch1
Link State................................... Down
Admin Mode................................... Enabled
Port Channel Flap Count...................... 0

Mbr    Mbr Flap
Ports  Counters
------ ---------
0/1    0
0/2    0
```

```
0/3     1
0/4     0
0/5     0
0/6     0
0/7     0
0/8     0
```

5.19.0.37 show port-channel resilient-hashing

Use this command to display the resilient hashing property for the port channel interface.

Format `show port-channel resilient-hashing`
Mode Privileged EXEC

Term	Definition
Resilient Hashing	Resilient hashing mode for the system.

Example:

```
(Routing) #show port-channel resilient-hashing

Resilient Hashing.............................. Enabled

(Routing) #
```

5.19.0.38 show port-channel system priority

Use this command to display the port-channel system priority.

Format `show port-channel system priority`
Mode Privileged EXEC

5.19.0.39 clear port-channel counters

Use this command to clear and reset specified port-channel and member flap counters for the specified interface.

Format `clear port-channel {lag-intf-num | slot/port} counters`
Mode Privileged EXEC

5.19.0.40 clear port-channel all counters

Use this command to clear and reset all port-channel and member flap counters for the specified interface.

Format `clear port-channel all counters`
Mode Privileged EXEC

5.20 VPC Commands

VPC (also known as MLAG) enables a LAG to be created across two independent switches, so that some member ports of a VPC can reside on one switch and the other members of a VPC can reside on another switch. The partner device on the remote side can be a VPC-unaware unit. To the unaware unit, the VPC appears to be a single LAG connected to a single switch.

5.20.0.1 vpc domain

Use this command to enter into VPC configuration mode and creates a VPC domain with the specified domain-id. Only one VPC domain can be created on a given device. The domain-id of the VPC domain should be equal to the one configured on the other VPC peer with which this device wants to form a VPC pair. The configured VPC domain-ids are exchanged during role election and if they are configured differently on the peer devices, the VPC does not become operational.

The administrator needs to ensure that the no two VPC domains can share the same VPC domain-id. Domain-id is used to derive the auto-generated VPC MAC address that is used in the actor ID field in the LACP PDUs and STP BPDUs sent out on VPC interfaces. When two VPC domains have the same domain-id, it leads to the same actor IDs and results in LACP convergence issues and STP convergence issues.

The range of domain id is 1-255.

Format `vpc domain` *`domain-id`*
Mode Global Config

5.20.0.1.1 no vpc domain

Use this command to deletes the VPC domain, disable peer-keepalive, disable peer-detection, and reset the configured parameters (role priority, VPC MAC address and VPC system priority) for the VPC domain.

Format `no vpc domain` *`domain-id`*
Mode Global Config

5.20.0.2 feature vpc

This command enables VPC globally. VPC role election occurs if both VPC and the keepalive state machine are enabled (see Section 5.20.0.7, peer-keepalive timeout). Peer link also has to be configured for role election to occur.

Format `feature vpc`
Mode Global Config

5.20.0.2.1 no feature vpc

This command disables VPC.

Format `no feature vpc`
Mode Global Config

5.20.0.3 peer detection enable

This command starts the dual control plane detection protocol (DCPDP) on the VPC switch. The peer VPC switch's IP address must be configured for the DCPDP to start on an VPC switch.

Default None
Format `peer detection enable`
Mode VPC Config

5.20.0.3.1 no peer detection enable

This command disables the dual control plane (DCPDP) detection protocol on the VPC switch.

Format `no peer detection enable`
Mode VPC Config

5.20.0.4 peer detection interval

Use this command to configure the DCPDP transmission interval and reception timeout.

The configurable transmission interval range is 200 ms–4000 ms. The configurable reception timeout range is 700 ms–14000 ms. The default transmission interval is 1000 ms; the default reception timeout is 3500 ms.

Default
- Transmission interval: 1000 ms
- Reception timeout: 3500 ms

Format `peer detection interval` *`msecs`* `timeout` *`seconds`*
Mode VPC Config

5.20.0.4.1 no peer detection interval

Use this command to reset the DCPDP transmission interval and reception timeout to default values.

Format `no peer detection interval` *`msecs`* `timeout` *`seconds`*
Mode VPC Config

5.20.0.5 peer-keepalive destination

This command configures the IP address of the peer VPC switch, which is the destination IP address of the dual control plane detection protocol (DCPDP) on the peer VPC switch. This configuration is used by the dual control plane detection protocol (DCPDP) on the VPC switches. It also configures the source IP address of the DCPDP message, which is the self IP on the VPC switch. The UDP port on which the VPC switch listens to the DCPDP messages can also be configured with this command.

The configurable range for the UDP port 1 to 65535 (Default is 60000).

Format `peer-keepalive destination` *`ipaddress`* `switch` *`ipaddress`* `[udp-port` *`port`*`]`
Mode VPC Config

5.20.0.5.1 no peer-keepalive destination

This command unconfigures the self IP address, peer IP address, and the UDP port.

Format `no peer-keepalive destination` *`ipaddress`* `switch` *`ipaddress`* `[udp-port` *`port`*`]`
Mode VPC Config

5.20.0.6 peer-keepalive enable

This command starts the keepalive state machine on the VPC device, if VPC is globally enabled.

Default `Disabled`
Format `peer-keepalive enable`
Mode VPC Config

5.20.0.6.1 no peer-keepalive enable

This command stops the keepalive state machine of the VPC switch.

Format `no peer-keepalive enable`
Mode VPC Config

5.20.0.7 peer-keepalive timeout

This command configures the peer keepalive timeout value (in seconds). If an VPC switch does not receive a keepalive message from the peer for the duration of this timeout value, it transitions its role (if required).

NOTE: The keepalive state machine is not restarted if keepalive priority is modified post election.

The configurable range is 2 to 15 seconds. The default is 5 seconds.

Format `peer-keepalive timeout` *`value`*
Mode VPC Config

5.20.0.7.1 no peer-keepalive timeout

This command resets the keepalive timeout to the default value of 5 seconds.

Format `no keepalive timeout`
Mode VPC Config

5.20.0.8 role priority

This command configures VPC switch priority. This value is used for VPC role election. The priority value is sent to the peer in the VPC keepalive messages. The VPC switch with lower priority becomes the Primary and the switch with higher priority becomes the Secondary. If both VPC peer switches have the same role priority, the device with the lower system MAC address becomes the Primary.

NOTE: The keepalive state machine is not restarted even if the keepalive priority is modified post-election.

The priority can be between 1 and 255 seconds. The default is 100.

Format `role priority` *`value`*
Mode VPC Config

5.20.0.8.1 no role priority

This command resets the keepalive priority and timeout to the default value of 100.

Format `no role priority`
Mode VPC Config

5.20.0.9 system-mac

Use this command to manually configure the MAC address for the VPC domain. The VPC MAC address should be configured same on both the peer devices. The specified MAC address should be a unicast MAC address in <aa:bb:cc:dd:ee:ff> format and cannot be equal to the MAC address of either the primary VPC or secondary VPC device. The configured VPC MAC address is exchanged during role election and, if they are configured differently on the peer devices, VPC does not become operational.

The *mac-address* is used in the LACP PDUs and STP BPDUs that are sent out on VPC member ports, if VPC primary device election takes place after the VPC MAC address is configured. When the VPC MAC address is configured after the VPC primary device is elected, the operational VPC MAC address is used in the LACP PDUs and STP BPDUs instead of the configured VPC MAC address.

Format `system-mac` *`mac-address`*
Mode VPC Domain

5.20.0.9.1 no system-mac

This command unconfigures the manually configured VPC MAC address for the VPC domain.

Format `no system-mac`
Mode VPC Domain

5.20.0.10 system-priority

Use this command to manually configures a system priority for the VPC domain. The *system-priority* should be configured identically on both VPC peers. If the configured VPC system priority is different on VPC peers, the VPC will not come up.

The system-priority is used in the LACP PDUs that are sent out on VPC member ports if VPC primary device election takes place after the VPC system priorities are configured. When the VPC system priority is configured after the VPC primary device is elected, the operational VPC system priority is used in the LACP PDUs instead of the configured VPC system priority.

The configurable range is 1 to 65535. The default is 32767.

Format `system-priority` *`priority`*
Mode VPC Domain

5.20.0.10.1 no system-priority

This command restores the VPC system priority to the default value.

Format `no system-priority` *`priority`*
Mode VPC Domain

5.20.0.11 vpc

This command configures a port-channel (LAG) as part of an VPC. Upon issuing this command, the port-channel is down until the port-channel member information is exchanged and agreed between the VPC peer switches.

The configurable range for the VPC id 1 to (Max number of LAG interfaces (64) -1).

Default `none`
Format `vpc` *`id`*
Mode LAG Interface

5.20.0.11.1 no vpc

This command unconfigures a port-channel as VPC.

Format `no vpc` *`id`*
Mode LAG Interface

5.20.0.12 vpc peer-link

This command configures a port channel as the VPC peer link.

Format `vpc peer-link`
Mode LAG Interface

5.20.0.12.1 no vpc peer-link

This command unconfigures a port channel as the VPC peer link.

Format `no vpc peer-link`
Mode LAG Interface

5.20.0.13 show running-config vpc

Use this command to display running configuration information for virtual port channels (VPC).

Format `show running-config vpc`
Mode Privileged EXEC

Example:

```
(Switching) #  show running-config vpc
```

```
feature vpc
vpc domain 1
role priority 120
system-mac 00:10:18:82:1A:A0
system-priority 32767
peer-keepalive destination 1.1.1.1 source 1.1.1.2
                        peer detection interval 2000  timeout 6000

interface lag 1
vpc peer-link

interface lag 2
vpc 2
```

5.20.0.14 show vpc

This command displays information about an VPC. The configuration and operational modes of the VPC are displayed; the VPC is operationally enabled if all the preconditions are met. The port-channel that is configured as an VPC interface is also displayed with the member ports on the current switch and peer switch (with their link status)

Format `show vpc` *id*

Mode User EXEC

Example: The following shows an example of the command.

```
(Switching) # show vpc 10
VPC id#10
-----------------
Config mode.....................................Enabled
Operational mode...............................Enabled
Port channel.....................................3/1
Self member ports Status
----------------- ---------
              0/2 UP
              0/6 DOWN
Peer member ports Status
----------------- ---------
              0/8 UP
```

5.20.0.15 show vpc brief

This command displays the VPC global status and current VPC operational mode (the VPC is in operational mode if the preconditions are met). The peerlink and keepalive statuses as well as the number of configured and operational VPCs and the system MAC and role are displayed.

Format `show vpc brief`

Mode Privileged EXEC

Example: The following shows an example of the command.

```
(Switching) # show vpc brief
VPC config Mode.............................. Enabled
Keepalive config mode........................ Enabled
VPC operational Mode......................... Enabled
Self Role.................................... Primary
```

```
Peer Role..................................... Secondary
Peer detection................................ Disabled

Peer-Link details
-----------------
Interface..................................... 3/2
Peer link status.............................. UP
Peer-link STP Mode............................ Disabled
Configured Vlans.............................. 1
Egress tagging................................ none

VPC Details
-----------
Number of VPCs configured..................... 1
Number of VPCs operational.................... 1

VPC id# 1
-----------
Interface..................................... 3/1
Configured Vlans.............................. 1
VPC Interface State........................... Active

Local MemberPorts       Status
-----------------       ------
             0/19       UP
             0/20       UP
             0/21       UP
             0/22       UP

Peer MemberPorts        Status
----------------        ------
            0/27        UP
            0/28        UP
            0/29        UP
            0/30        UP
```

5.20.0.16 show vpc consistency-parameters

Use this command to display global consistency parameters and LAG interface consistency parameters for virtual port channels (VPC) on the switch.

Format `show vpc consistency-parameters {global | interface lag` *`lag-id`*`}`

Mode Privileged EXEC

Example:

```
switch # show vpc consistency-parameters global
Parameter
Name                          Value
---------------------        ------------------------------------------
STP Mode                      Enabled
STP Version                   IEEE  802.1s
BPDU Filter Mode              Enabled
BPDU Guard Mode               Enabled
MST Instances                 1,2,4
FDB Aging Time                300 seconds
VPC system MAC address        <AA:BB:CC:DD:EE:FF>
```

```
VPC system priority           32767
VPC Domian ID                 1
MST VLAN Configuration
Instance        Associated VLANS
-------------  ------------------------------------
7,8,10,20
2               4,5,40-50

4               30,32,34-38

PV(R)STP Configuration:

PV(R)STP Mode                                        Enabled/Disabled
PV(R)STP Version                                     PVST/Rapid-PVST
FastUplinkfast                                       Enabled/Disabled
FastUpLinkfast max-update-rate                       <0-32000>
FastBackbone                                         Enabled/Disabled

VLAN          Mode          STP       Hello         Forward       MaximumAge            Priority
                            Root      Time          Time          Time
--------      ------        -----     --------     ----------     ----------------       ---------
4             Enabled       Primary   2            15             15                     0

switch# show vpc consistency-parameters interface lag 2
Parameter
Name                                  Value
-----------------              ---------------------------
Port Channel Mode               Enabled
STP Mode                        Enabled
BPDU Filter  Mode               Enabled
BPDU Flood Mode                 Enabled
Auto-edge                       FALSE
TCN Guard                       True
Port Cost                       2
Edge Port                       True
Root Guard                      True
Loop Guard                      True
Hash Mode                       3
Minimum Links                   1
Channel Type                    Static
Configured VLANs                4,5,7,8
MTU                             1518



Active Port     Speed       Duplex
------------    ---------   --------
0/1                  100         Full
0/2                  100         Full

MST VLAN Configuration

Instance       Associated VLANS
-------------  ------------------------------------

1                       7,8

2                       4,5
```

```
PV(R)STP Configuration:
STP port-priority       <0-240>

VLAN         port-priority              cost
-------      -----------------    ---------------------------
<ID>           <0-240>            auto | <1- 200000000>
```

5.20.0.17 show vpc peer-keepalive

This command displays the peer VPC switch IP address used by the dual control plane detection protocol. The port used for the DCPDP is shown. This command also displays if peer detection is enabled. If enabled, the detection status is displayed. The DCPDP message transmission interval and reception timeout are also displayed.

Format `show vpc peer-keepalive`

Mode User EXEC

Example: The following shows an example of the command.

```
(Switching) # show vpc peer-keepalive
Peer IP address.............................. 10.130.14.55
Source IP address............................ 10.130.14.54
UDP port..................................... 50000
Peer detection admin status.................. Enabled
Peer detection operational status............ Down
Peer is detected............................. True
Configured Tx interval....................... 1000 milliseconds
Configured Rx timeout........................ 3500 milliseconds
Operational Tx interval...................... 500 milliseconds
Operational Rx timeout....................... 2000 milliseconds
```

5.20.0.18 show vpc role

This command displays information about the keepalive status and parameters. The role of the VPC switch as well as the system MAC address and priority are displayed.

Format `show vpc role`

Mode User EXEC

Example: The following shows an example of the command.

```
(Switching) # show vpc role
Self
----
VPC domain ID.................................1
Keepalive config mode........................ Enabled
Keepalive operational mode................... Enabled
Role Priority................................ 100
Configured VPC MAC ..........................<AA:BB:CC:DD:EE:FF>
Operational VPC MAC..........................<AA:BB:CC:DD:EE:FF>
Configured VPC system priority................32767
Operational VPC system priority...............32767
Local System MAC.................................. 00:10:18:82:18:63
Timeout...................................... 5
VPC State.................................... Primary
```

```
VPC Role..................................... Primary

Peer
----
VPC Domain ID................................ 1
Role Priority................................ 100
Configured VPC MAC...........................<AA:BB:CC:DD:EE:FF>
Operational VPC MAC..........................<AA:BB:CC:DD:EE:FF>
Configured VPC system priority..............32767
Operational VPC system priority..............32767
Role.....................................Secondary
Local System MAC............................00:10:18:82:1b:ab
```

5.20.0.19 show vpc statistics

This command displays counters for the keepalive messages transmitted and received by the VPC switch.

Format `show vpc statistics {peer-keepalive | peer-link}`

Mode User EXEC

Example: The following shows examples of the command.

Example 1

```
(Switching) # show vpc statistics peer-keepalive
Total trasmitted……. 123
Tx successful……. 118
Tx errors…….. 5
Total received……. 115
Rx successful…….. 108
Rx Errors…… 7
Timeout counter……. 6
```

Example2 :

```
(Switching) #show vpc statistics peer-link
Peer link control messages trasmitted……... 123
Peer link control messages Tx errors..... 5
Peer link control messages Tx timeout…….…….. 4
Peer link control messages ACK transmitted……. 34
Peer link control messages ACK Tx erorrs……. 5
Peer link control messages received..……. 115
Peer link data messages trasmitted……. 123
Peer link data messages Tx errors..... 5
Peer link data messages Tx imeout…….……... 4
Peer link data messages ACK transmitted……. 34
Peer link data messages ACK Tx erorrs……. 5
Peer link data messages received…...……. 115
Peer link BPDU’s tranmsitted to peer……. 123
Peer link BPDU’s Tx error…….. 9
Peer link BPDU’s received from peer……. 143
Peer link BPDU’s Rx error…….. 1
Peer link LACPDU’s tranmsitted to peer……. 123
Peer link LACPDU’s Tx error…….. 9
Peer link LACPDU’s received from peer……. 143
Peer link LACPDU’s Rx error…….. 1
```

5.20.0.20 clear vpc statistics

This command clears all the keepalive statistics.

Format `clear vpc statistics {peer-keepalive | peer-link}`
Mode User EXEC

Example: The following shows an example of the command.

```
(Switching) # clear vpc statistics peer-keepalive
(Switching) # clear vpc statistics peer-link
```

5.20.0.21 debug vpc peer-keepalive

This command enables debug traces of the keepalive state machine transitions.

Format `debug vpc peer-keepalive`
Mode User EXEC

5.20.0.22 debug vpc peer-link data-message

This command enables debug traces for the control messages exchanged between the VPC devices on the peer link.

Format `debug vpc peer-link data-message`
Mode User EXEC

5.20.0.23 debug vpc peer-link control-message async

This command enables debug traces for the asynchronous reliable control messages exchanged between the MLAG devices on the peer link. For `error`, only the errors in the communication are traced. For `msg`, the control message contents that are exchanged can be traced. Both transmitted and received control messages contents can be traced.

Format `debug vpc peer-link control-message async {error | msg [receive | transmit]}`
Mode User EXEC

5.20.0.24 debug vpc peer-link control-message bulk

This command enables debug traces for the periodic control messages exchanged between the MLAG devices on the peer link. For `error`, only the errors in the communication are traced. For `msg`, the control message contents that are exchanged can be traced. Both transmitted and received control messages contents can be traced.

Format `debug vpc peer-link control-message bulk {error | msg [receive | transmit]}`
Mode User EXEC

5.20.0.25 debug vpc peer-link control-message ckpt

This command enables debug traces for the checkpointing control messages exchanged between the MLAG devices on the peer link. For `error`, only the errors in the communication are traced. For `msg`, the control message contents that are exchanged can be traced. Both transmitted and received control messages contents can be traced.

Format `debug vpc peer-link control-message ckpt {error | msg [receive | transmit]}`
Mode User EXEC

5.20.0.26 debug vpc peer detection

This command enables debug traces for the dual control plane detection protocol. Traces are seen when the DCPDP transmits or receives detection packets to or from the peer VPC switch.

Format `debug vpc peer detection`
Mode User EXEC

5.21 Port Mirroring

Port mirroring, which is also known as port monitoring, selects network traffic that you can analyze with a network analyzer, such as a SwitchProbe device or other Remote Monitoring (RMON) probe.

5.21.0.1 monitor session source

This command configures the source interface for a selected monitor session. Use the `source interface` ***slot/port*** parameter to specify the interface to monitor. Use `rx` to monitor only ingress packets, or use ***tx*** to monitor only egress packets. If you do not specify an `{rx | tx}` option, the destination port monitors both ingress and egress packets.

A VLAN can be configured as the source to a session (all member ports of that VLAN are monitored). Remote port mirroring is configured by adding the RSPAN VLAN ID. At the source switch, the destination is configured as the RSPAN VLAN and at the destination switch, the source is configured as the RSPAN VLAN.

NOTE: The source and destination cannot be configured as remote on the same device.

The commands described below add a mirrored port (source port) to a session identified with *session-id*. The *session-id* parameter is an integer value used to identify the session. The maximum number of sessions which can be configured is L7_MIRRORING_MAX_SESSIONS. Option *rx* is used to monitor only ingress packets. Option *tx* is used to monitor only egress packets. If no option is specified, both ingress and egress packets, RX and TX, are monitored.

A VLAN can also be configured as the source to a session (all the member ports of that VLAN are monitored).

NOTE: If an interface participates in some VLAN and is a LAG member, this VLAN cannot be assigned as a source VLAN for a Monitor session. At the same time, if an interface participates in some VLAN and this VLAN is assigned as a source VLAN for a Monitor session, the interface can be assigned as a LAG member.

Remote port mirroring is configured by giving the RSPAN VLAN ID. At the source switch the destination is configured as RSPAN VLAN and at the destination switch the source is configured as RSPAN VLAN.

NOTE: On the intermediate switch, RSPAN VLAN should be created, the ports connected towards Source and Destination switch should have the RSPAN VLAN participation. RSPAN VLAN egress tagging should be enabled on the interface on the intermediate switch connected towards the Destination switch.

Default	None
Format	`monitor session` ***session-id*** `source {interface {`***slot/port*** `| cpu | lag } | vlan` ***vlan-id*** `| remote vlan` ***vlan-id*** `}[{rx | tx}]`
Mode	Global Config

5.21.0.1.1 no monitor session source

This command removes the specified mirrored port from the selected port mirroring session.

Default	None
Format	`no monitor session` ***session-id*** `source {interface {`***slot/port*** `| cpu | lag } | vlan | remote vlan}`
Mode	Global Config

5.21.0.2 monitor session destination

This command configures the probe interface for a selected monitor session. This command configures a probe port and a monitored port for monitor session (port monitoring). Use `rx` to monitor only ingress packets, or use *`tx`* to monitor only egress packets. If you do not specify an `{rx | tx}` option, the destination port monitors both ingress and egress packets.

A VLAN can be configured as the source to a session (all member ports of that VLAN are monitored). Remote port mirroring is configured by adding the RSPAN VLAN ID. At the source switch, the destination is configured as the RSPAN VLAN and at the destination switch, the source is configured as the RSPAN VLAN.

NOTE: The source and destination cannot be configured as remote on the same device.

The `reflector-port` is configured at the source switch along with the destination RSPAN VLAN. The `reflector-port` forwards the mirrored traffic towards the destination switch.

NOTE: This port must be configured with RSPAN VLAN membership.

Use the `destination interface` ***`slot/port`*** to specify the interface to receive the monitored traffic.

The commands described below add a mirrored port (source port) to a session identified with *session-id*. The *session-id* parameter is an integer value used to identify the session. The maximum number of sessions which can be configured is L7_MIRRORING_MAX_SESSIONS. Option *rx* is used to monitor only ingress packets. Option *tx* is used to monitor only egress packets. If no option is specified, both ingress and egress packets, RX and TX, are monitored.

A VLAN can also be configured as the source to a session (all the member ports of that VLAN are monitored).

NOTE: If an interface participates in some VLAN and is a LAG member, this VLAN cannot be assigned as a source VLAN for a Monitor session. At the same time, if an interface participates in some VLAN and this VLAN is assigned as a source VLAN for a Monitor session, the interface can be assigned as a LAG member.

Remote port mirroring is configured by giving the RSPAN VLAN ID. At the source switch the destination is configured as RSPAN VLAN and at the destination switch the source is configured as RSPAN VLAN.

NOTE: On the intermediate switch: RSPAN VLAN should be created, the ports connected towards Source and Destination switch should have the RSPAN VLAN participation. RSPAN VLAN egress tagging should be enabled on the interface on the intermediate switch connected towards the Destination switch.

Default	None
Format	`monitor session` ***`session-id`*** `destination {interface` ***`slot/port`*** `[remove-rspan-tag] |remote vlan` ***`vlan-id`*** `reflector-port` ***`slot/port`***`}`
Mode	Global Config

5.21.0.2.1 no monitor session destination

This command removes the specified probe port from the selected port mirroring session.

Format	`no monitor session` ***`session-id`*** `destination {interface` ***`slot/port`*** `|remote vlan` ***`vlan-id`*** `reflector-port` ***`slot/port`***`}`
Mode	Global Config

5.21.0.3 monitor session filter

This command attaches an IP/MAC ACL to a selected monitor session. This command configures a probe port and a monitored port for monitor session (port monitoring).

An IP/MAC ACL can be attached to a session by giving the access list number/name.

Use the `filter` parameter to filter a specified access group either by IP address or MAC address.

The commands described below add a mirrored port (source port) to a session identified with *session-id*. The *session-id* parameter is an integer value used to identify the session. The maximum number of sessions which can be configured is L7_MIRRORING_MAX_SESSIONS.

Remote port mirroring is configured by giving the RSPAN VLAN ID. At the source switch the destination is configured as RSPAN VLAN and at the destination switch the source is configured as RSPAN VLAN.

NOTE: Note the following:

- Source and destination cannot be configured as remote on the same device.
- IP/MAC ACL can be attached to a session by giving the access list number/name. On the platforms that do not support both IP and MAC ACLs to be assigned on the same Monitor session, an error message is thrown when user tries to configure ACLs of both types.

Default	None
Format	`monitor session` ***`session-id`*** `filter {ip access-group` ***`acl-id/aclname`*** `| mac access-group` ***`acl-name`***`}`
Mode	Global Config

5.21.0.3.1 no monitor session filter

This command removes the specified IP/MAC ACL from the selected monitoring session.

Format	`no smonitor session` ***`session-id`*** `filter {ip access-group | mac access-group }`
Mode	Global Config

5.21.0.4 monitor session mode

This command enables the selected port mirroring session. This command configures a probe port and a monitored port for monitor session (port monitoring).

A VLAN can be configured as the source to a session (all member ports of that VLAN are monitored). Remote port mirroring is configured by adding the RSPAN VLAN ID. At the source switch, the destination is configured as the RSPAN VLAN and at the destination switch, the source is configured as the RSPAN VLAN.

NOTE: The source and destination cannot be configured as remote on the same device.

The commands described below add a mirrored port (source port) to a session identified with *session-id*. The *session-id* parameter is an integer value used to identify the session. The maximum number of sessions which can be configured is L7_MIRRORING_MAX_SESSIONS. Option *rx* is used to monitor only ingress packets. Option *tx* is used to monitor only egress packets. If no option is specified, both ingress and egress packets, RX and TX, are monitored.

A VLAN can also be configured as the source to a session (all the member ports of that VLAN are monitored).

NOTE: If an interface participates in some VLAN and is a LAG member, this VLAN cannot be assigned as a source VLAN for a Monitor session. At the same time, if an interface participates in some VLAN and this VLAN is assigned as a source VLAN for a Monitor session, the interface can be assigned as a LAG member.

Remote port mirroring is configured by giving the RSPAN VLAN ID. At the source switch the destination is configured as RSPAN VLAN and at the destination switch the source is configured as RSPAN VLAN.

NOTE: Note the following:

- Source and destination cannot be configured as remote on the same device.
- On the intermediate switch: RSPAN VLAN should be created, the ports connected towards the Source and Destination switch should have the RSPAN VLAN participation. RSPAN VLAN egress tagging should be enabled on interface on intermediate switch connected towards Destination switch.

Default None

Format `monitor session` *`session-id`* `mode`

Mode Global Config

5.21.0.4.1 no monitor session mode

This command disables the selected port mirroring session.

Format `no monitor session` *`session-id`* `mode`

Mode Global Config

5.21.0.5 no monitor session

Use this command without optional parameters to remove the monitor session (port monitoring) designation from the source probe port, the destination monitored port and all VLANs. Once the port is removed from the VLAN, you must manually add the port to any desired VLANs. Use the `source interface` *`slot/port`* parameter or `destination interface` to remove the specified interface from the port monitoring session. Use the `mode` parameter to disable the administrative mode of the session

Format `no monitor session` *`session-id`* `{source {interface` *`slot/port`* `| cpu | lag} |vlan| remote vlan} | destination { interface | remote vlan | mode |filter {ip access-group |mac access-group}}]`

Mode Global Config

5.21.0.6 no monitor

This command removes all the source ports and a destination port and restores the default value for mirroring session mode for all the configured sessions.

NOTE: This is a stand-alone “no” command. This command does not have a “normal” form.

Default enabled

Format `no monitor`

Mode Global Config

5.21.0.7 remote-span

This command identifies the VLAN as the RSPAN VLAN.

Default None
Format remote-span
Mode VLAN configuration

5.21.0.7.1 no remote-span

This command clears RSPAN information for the VLAN.

Format no remote-span
Mode VLAN configuration

5.21.0.8 show monitor session

This command displays the Port monitoring information for a particular mirroring session.

NOTE: The *session-id* parameter is an integer value used to identify the session. In the current version of the software, the *session-id* parameter is always one (1).

Format show monitor session *session-id* | all
Mode Privileged EXEC

Term	Definition
Session ID	An integer value used to identify the session. Its value can be anything between 1 and the maximum number of mirroring sessions allowed on the platform.
Admin Mode	Indicates whether the Port Mirroring feature is enabled or disabled for the session identified with *session-id*. The possible values are Enabled and Disabled.
Probe Port	Probe port (destination port) for the session identified with *session-id*. If probe port is not set then this field is blank.
Remove RSPAN Tag	Remove RSPAN VLAN tag on the probe (destination) port. To configure this value probe port and remove RSPAN tag values should be specified simultaneously. If no probe port is configured for the session then this field is blank.
Mirrored Port(s)	The port that is configured as a mirrored port (source port) for the session identified with *session-id*. If no source port is configured for the session, this field is blank.
Session Type	The type of monitor session.
Source VLAN	All member ports of this VLAN are mirrored. If the source VLAN is not configured, this field is blank.
Reflector Port	This port carries all the mirrored traffic at the source switch.
Source RSPAN VLAN	The source VLAN configured at the destination switch. If remote VLAN is not configured, this field is blank
Destination RSPAN VLAN	The destination VLAN configured at the source switch. If remote VLAN is not configured, this field is blank
Source ERSPAN Flow ID	The ID number used by the source session to identify the ERSPAN traffic.
Destination ERSPAN Flow ID	The ID number used by the destination session to identify the ERSPAN traffic, must also be entered in the ERSPAN destination session configuration.

Term	Definition
Source ERSPAN IP address	The ERSPAN flow destination IP address , which must be an address on a local interface and match the address entered in the ERSPAN destination session configuration.
Destination ERSPAN IP address	The ERSPAN flow destination IPv4 address , which must also be configured on an interface on the destination switch and be entered in the ERSPAN destination session configuration.
Destination ERSPAN Origin IP address	The IPv4 address used as the source of the ERSPAN traffic.
Destination ERSPAN IP TTL	The IPv4 TTL value of the packets in the ERSPAN traffic.
Destination ERSPAN IP DSCP	The IP DSCP value of the packets in the ERSPAN traffic.
Destination ERSPAN IP Precedence	The IP precedence value of the packets in the ERSPAN traffic.
IP ACL	The IP access-list id or name attached to the port mirroring session.
MAC ACL	The MAC access-list name attached to the port mirroring session.

Example: This example shows the command output when the session ID is specified.

```
(Switch)#show monitor session 1
Session ID..................................... 1
Session Type................................... ERSPAN Source
Admin Mode..................................... Enabled
Probe Port..................................... 1/0/8
Remove RSPAN Tag............................... False
Source VLAN.....................................
Mirrored Port(s)................................
Reflector Port..................................
Source RSPAN VLAN...............................
Destination RSPAN VLAN..........................
Source ERSPAN Flow ID.......................... 1023
Source ERSPAN IP Address....................... 255.255.255.255
Destination ERSPAN Flow ID.....................
Destination ERSPAN IP Address..................
Destination ERSPAN Origin IP...................
Destination ERSPAN IP TTL......................
Destination ERSPAN IP DSCP.....................
Destination ERSPAN IP Precedence...............
IP ACL..........................................
MAC ACL........................................ mymac
```

Example: This example shows the command output when `all` is specified.

```
(Routing)#show monitor session all

Session ID..................................... 1
Session Type................................... ERSPAN Destination
Admin Mode..................................... Enable
Probe Port..................................... 1/0/8
Remove RSPAN Tag............................... False
Source VLAN.....................................
Mirrored Port(s)................................
Reflector Port..................................
Source RSPAN VLAN...............................
Destination RSPAN VLAN..........................
Source ERSPAN Flow ID.......................... 1023
Source ERSPAN IP Address....................... 255.255.255.255
Destination ERSPAN Flow ID.....................
```

```
Destination ERSPAN IP Address.................
Destination ERSPAN Origin IP..................
Destination ERSPAN IP TTL.....................
Destination ERSPAN IP DSCP....................
Destination ERSPAN IP Precedence..............
IP ACL........................................
MAC ACL....................................... mymac

Session ID.................................... 2
Session Type.................................. Local
Admin Mode.................................... Disabled
Probe Port.................................... 1/0/2
Remove RSPAN Tag.............................. False
Source VLAN...................................
Mirrored Port(s).............................. 1/0/1(Rx), 1/0/19(Rx,Tx), 1/0/20(Tx)
Reflector Port................................
Source RSPAN VLAN.............................
Destination RSPAN VLAN........................
Source ERSPAN Flow ID.........................
Source ERSPAN IP Address......................
Destination ERSPAN Flow ID....................
Destination ERSPAN IP Address.................
Destination ERSPAN Origin IP..................
Destination ERSPAN IP TTL.....................
Destination ERSPAN IP DSCP....................
Destination ERSPAN IP Precedence..............
IP ACL........................................
MAC ACL.......................................

Session ID.................................... 3
Session Type.................................. RSPAN Source
Admin Mode.................................... Disabled
Probe Port....................................
Remove RSPAN Tag..............................
Source VLAN...................................
Mirrored Port(s).............................. 0/5/1(Rx,Tx)
Reflector Port................................ 1/0/10
Source RSPAN VLAN.............................
Destination RSPAN VLAN........................ 2
Source ERSPAN Flow ID.........................
Source ERSPAN IP Address......................
Destination ERSPAN Flow ID....................
Destination ERSPAN IP Address.................
Destination ERSPAN Origin IP..................
Destination ERSPAN IP TTL.....................
Destination ERSPAN IP DSCP....................
Destination ERSPAN IP Precedence..............
IP ACL........................................
MAC ACL.......................................

Session ID.................................... 4
Session Type.................................. RSPAN Destination
Admin Mode.................................... Disabled
Probe Port....................................
Remove RSPAN Tag..............................
Source VLAN...................................
Mirrored Port(s).............................. 0/3/1(Rx,Tx)
Reflector Port................................ 1/0/3
```

```
Source RSPAN VLAN.............................
Destination RSPAN VLAN.......................... 2
Source ERSPAN Flow ID.........................
Source ERSPAN IP Address......................
Destination ERSPAN Flow ID.....................
Destination ERSPAN IP Address..................
Destination ERSPAN Origin IP...................
Destination ERSPAN IP TTL......................
Destination ERSPAN IP DSCP.....................
Destination ERSPAN IP Precedence...............
IP ACL.......................................... ipacl
MAC ACL......................................... mmac
```

5.21.0.9 show vlan remote-span

This command displays the configured RSPAN VLAN.

Format `show vlan remote-span`
Mode Privileged EXEC Mode

Example: The following shows example output for the command.

```
(Switch)# show vlan remote-span

Remote SPAN VLAN
-------------------------------------------------------------------------
100,102,201,303
```

5.21.0.10 monitor session type erspan-source

This command configures an ERSPAN source session number and enters ERSPAN Source Session Configuration mode for the session.

Format `monitor session` ***`session-id`*** `type erspan-source`
Mode Global Config

5.21.0.10.1 no monitor session type erspan-source

This command removes the specified ERSPAN source session configuration.

Format `no monitor session` ***`session-id`*** `type erspan-source`
Mode Global Config

5.21.0.11 monitor session type erspan-destination

This command configures an ERSPAN destination session number and enters ERSPAN Destination Session Configuration mode for the session.

Format `monitor session` ***`session-id`*** `type erspan-destination`
Mode Global Config

5.21.0.11.1 no monitor session type erspan-destination

This command removes the specified ERSPAN destination session configuration.

Format `no monitor session` *`session-id`* `type erspan-destination`

Mode Global Config

5.22 Encapsulated Remote Switched Port Analyzer Commands

The Encapsulated Remote Port Analyzer (ERSPAN) feature allows port-mirroring collection points to be located anywhere across a routed network. This is achieved by encapsulating L2 mirrored packets using GRE with IP delivery. After a packet has been encapsulated, it can be forwarded throughout the L3-routed network.

ERSPAN uses a GRE tunnel to carry traffic between switches. ERSPAN consists of an ERSPAN source session, an ERSPAN destination session, and routable ERSPAN GRE-encapsulated traffic. All participating switches must be connected at Layer 3, and the network path must support the size of the ERSPAN traffic for the egress mirroring session.

To configure the source ERSPAN session, the following parameters should be configured at the source switch:

- Source ports (i.e. the traffic on this port is mirrored)
- ERSPAN destination IPv4 address
- ERSPAN origin IPv4 address
- ERSPAN session ID
- TX/RX

To configure the destination ERSPAN session, the following parameters should be configured at the destination switch:

- ERSPAN destination IPv4 address (as source)
- ERSPAN session ID
- Probe port

5.22.1 ERSPAN Destination Configuration Commands

ERSPAN uses separate source and destination sessions. The source session and destination session should be configured on different switches. This section describes the commands to configure the ERSPAN destination session.

5.22.1.1 source

This command configures the source interface for selected ERSPAN monitor session.

Default	None
Format	`source {interface {`*`slot/port`* `| cpu | lag` *`lag-group-id`*`} | vlan` *`vlan-id`* `}[rx | tx]`
Mode	ERSPAN Source Session Configuration Mode

5.22.1.1.1 no source

This command removes the specified mirrored port from the selected ERSPAN mirroring session.

Format	`no source {interface {`*`slot/port`* `| cpu | lag` *`lag-group-id`*`} | vlan` *`vlan-id`* `}`
Mode	ERSPAN Source Session Configuration Mode

5.22.1.2 destination

Use this command to enter the ERSPAN Source Session Destination Configuration mode.

Default	None
Format	`destination`

Mode ERSPAN Source Session Configuration Mode

5.22.1.3 ip address

This command configures the ERSPAN destination IP address.

NOTE: The same IP address must also be configured on an interface on the destination switch and be entered in the ERSPAN destination session configuration.

Default None
Format `ip address` *`ip-address`*
Mode ERSPAN Source Session Destination Configuration Mode

5.22.1.3.1 no ip address

This command removes the ERSPAN destination IP address configuration.

Format `no ip address`
Mode ERSPAN Source Session Destination Configuration Mode

5.22.1.4 erspan-id

This command configures the ERSPAN flow ID number used by the source and destination sessions to identify the ERSPAN traffic. The valid range for *`erspan-id`* is 1 to 1023.

NOTE: The same ERSPAN flow ID must also be configured in the ERSPAN destination session configuration.

Default None
Format `erspan-id` *`erspan-id`*
Mode ERSPAN Source Session Destination Configuration Mode

5.22.1.4.1 no erspan-id

This command removes the ERSPAN destination IP address configuration..

Format `no erspan-id`
Mode ERSPAN Source Session Destination Configuration Mode

5.22.1.5 origin ip address

This command configures the IP address used as the source of the ERSPAN traffic.

Default None
Format `origin ip address` *`ip-address`*
Mode ERSPAN Source Session Destination Configuration Mode

5.22.1.5.1 no origin ip address

This command removes the ERSPAN origin IP address configuration.

Format `no origin ip address`
Mode ERSPAN Source Session Destination Configuration Mode

5.22.1.6 ip ttl

This command configures the IP time-to-live (TTL) value of the packets in the ERSPAN traffic. The valid range for *`ttl-value`* is 1 to 255.

Default 64
Format `ip ttl` *`ttl-value`*
Mode ERSPAN Source Session Destination Configuration Mode

5.22.1.6.1 no ip ttl

This command removes the ERSPAN IP TTL value configuration.

Format `no ip ttl`
Mode ERSPAN Source Session Destination Configuration Mode

5.22.1.7 ip dscp

This command configures the IP DSCP value of the packets in the ERSPAN traffic. The valid range for *`dscp-value`* is 0 to 63.

Default 64
Format `ip dscp` *`dscp-value`*
Mode ERSPAN Source Session Destination Configuration Mode

5.22.1.7.1 no ip dscp

This command removes the ERSPAN IP DSCP value configuration.

Format `no ip dscp`
Mode ERSPAN Source Session Destination Configuration Mode

5.22.1.8 ip prec

This command configures the IP precedence value of the packets in the ERSPAN traffic. The valid range for *`precedence-value`* is 0 to 7.

Default 0
Format `ip prec` *`precedence-value`*
Mode ERSPAN Source Session Destination Configuration Mode

5.22.1.8.1 no ip prec

This command removes the ERSPAN IP precedence value configuration.

Format `no ip prec`
Mode ERSPAN Source Session Destination Configuration Mode

5.22.1.9 reflector-port

This command configures the reflector interface for the selected ERSPAN monitor session.

Default 0
Format `reflector-port` *`slot/port`*
Mode ERSPAN Source Session Configuration Mode

5.22.1.9.1 no reflector-port

This command removes the reflector port from the selected ERSPAN mirroring session.

Format `no reflector-port`
Mode ERSPAN Source Session Configuration Mode

5.22.2 ERSPAN Source Configuration Commands

ERSPAN uses separate source and destination sessions. The source session and destination session should be configured on different switches. This section describes the commands to configure the ERSPAN source session.

5.22.2.1 destination interface

This command configures the destination interface (probe port) for the selected ERSPAN monitor session.

Default None
Format `destination interface` *`slot/port`*
Mode ERSPAN Destination Session Configuration Mode

5.22.2.1.1 no destination interface

This command removes the specified probe port from the selected ERSPAN mirroring session.

Format `no destination interface`
Mode ERSPAN Destination Session Configuration Mode

5.22.2.2 source

Use this command to enter the ERSPAN Destination Session Source Configuration Mode.

Default None
Format `source`

Mode ERSPAN Destination Session Configuration Mode

5.22.2.2.1 no source

This command removes the ERSPAN Destination Session Source Configuration.

Format `no source`
Mode ERSPAN Destination Session Configuration Mode

5.22.2.3 ip address

This command configures the ERSPAN destination IP address.

NOTE: This IP address must be an address on a local interface and match the address entered in the ERSPAN source session configuration.

Default None
Format `ip address` *`ip-address`*
Mode ERSPAN Destination Session Source Configuration Mode

5.22.2.3.1 no ip address

This command removes the ERSPAN destination IP address configuration.

Format `no ip address`
Mode ERSPAN Destination Session Source Configuration Mode

5.22.2.4 erspan-id

This command configures the ERSPAN flow ID number used by the source and destination sessions to identify the ERSPAN traffic. The valid range for *`erspan-id`* is 1 to 1023.

NOTE: The same ERSPAN flow ID must also be configured in the ERSPAN source session configuration.

Default None
Format `erspan-id` *`erspan-id`*
Mode ERSPAN Destination Session Source Configuration Mode

5.22.2.4.1 no erspan-id

This command removes the ERSPAN destination IP address configuration..

Format `no erspan-id`
Mode ERSPAN Destination Session Source Configuration Mode

5.23 Static MAC Filtering

The commands in this section describe how to configure static MAC filtering. Static MAC filtering allows you to configure destination ports for a static multicast MAC filter irrespective of the platform.

5.23.0.1 macfilter

This command adds a static MAC filter entry for the MAC address `macaddr` on the VLAN `vlanid`. The value of the `macaddr` parameter is a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The restricted MAC Addresses are: 00:00:00:00:00:00, 01:80:C2:00:00:00 to 01:80:C2:00:00:0F, 01:80:C2:00:00:20 to 01:80:C2:00:00:21, and FF:FF:FF:FF:FF:FF. The `vlanid` parameter must identify a valid VLAN.

The number of static mac filters supported on the system is different for MAC filters where source ports are configured and MAC filters where destination ports are configured.

For current Broadcom platforms, you can configure the following combinations:

- Unicast MAC and source port
- Multicast MAC and source port
- Multicast MAC and destination port (only)
- Multicast MAC and source ports and destination ports

Format `macfilter` *`macaddr vlanid`*
Mode Global Config

5.23.0.1.1 no macfilter

This command removes all filtering restrictions and the static MAC filter entry for the MAC address `macaddr` on the VLAN `vlanid`. The `macaddr` parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The `vlanid` parameter must identify a valid VLAN.

Format `no macfilter` *`macaddr vlanid`*
Mode Global Config

5.23.0.2 macfilter adddest

Use this command to add the interface or range of interfaces to the destination filter set for the MAC filter with the given `macaddr` and VLAN of `vlanid`. The `macaddr` parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The `vlanid` parameter must identify a valid VLAN.

NOTE: Configuring a destination port list is only valid for multicast MAC addresses.

Format `macfilter adddest` *`macaddr`*
Mode Interface Config

5.23.0.2.1 no macfilter adddest

This command removes a port from the destination filter set for the MAC filter with the given `macaddr` and VLAN of `vlanid`. The `macaddr` parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The `vlanid` parameter must identify a valid VLAN.

Format `no macfilter adddest` *`macaddr`*

Mode Interface Config

5.23.0.3 macfilter adddest all

This command adds all interfaces to the destination filter set for the MAC filter with the given `macaddr` and VLAN of `vlanid`. The `macaddr` parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The `vlanid` parameter must identify a valid VLAN.

NOTE: Configuring a destination port list is only valid for multicast MAC addresses.

Format `macfilter adddest all` *`macaddr`*

Mode Global Config

5.23.0.3.1 no macfilter adddest all

This command removes all ports from the destination filter set for the MAC filter with the given `macaddr` and VLAN of `vlanid`. The `macaddr` parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The `vlanid` parameter must identify a valid VLAN.

Format `no macfilter adddest all` *`macaddr`*

Mode Global Config

5.23.0.4 macfilter addsrc

This command adds the interface or range of interfaces to the source filter set for the MAC filter with the MAC address of *`macaddr`* and VLAN of `vlanid`. The *`macaddr`* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *`vlanid`* parameter must identify a valid VLAN.

Format `macfilter addsrc` *`macaddr vlanid`*

Mode Interface Config

5.23.0.4.1 no macfilter addsrc

This command removes a port from the source filter set for the MAC filter with the MAC address of *`macaddr`* and VLAN of *`vlanid`*. The *`macaddr`* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The `vlanid` parameter must identify a valid VLAN.

Format `no macfilter addsrc` *`macaddr vlanid`*

Mode Interface Config

5.23.0.5 macfilter addsrc all

This command adds all interfaces to the source filter set for the MAC filter with the MAC address of `macaddr` and `vlanid`. You must specify the `macaddr` parameter as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The `vlanid` parameter must identify a valid VLAN.

Format `macfilter addsrc all` *`macaddr vlanid`*
Mode Global Config

5.23.0.5.1 no macfilter addsrc all

This command removes all interfaces to the source filter set for the MAC filter with the MAC address of `macaddr` and VLAN of `vlanid`. You must specify the `macaddr` parameter as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The `vlanid` parameter must identify a valid VLAN.

Format `no macfilter addsrc all` *`macaddr vlanid`*
Mode Global Config

5.23.0.6 show mac-address-table static

This command displays the Static MAC Filtering information for all Static MAC Filters. If you specify `all`, all the Static MAC Filters in the system are displayed. If you supply a value for `macaddr`, you must also enter a value for `vlanid`, and the system displays Static MAC Filter information only for that MAC address and VLAN.

Format `show mac-address-table static {`*`macaddr vlanid`* `| all}`
Mode Privileged EXEC

Parameter	Definition
MAC Address	The MAC Address of the static MAC filter entry.
VLAN ID	The VLAN ID of the static MAC filter entry.
Source Port(s)	The source port filter set's slot and port(s).

NOTE: Only multicast address filters will have destination port lists.

5.23.0.7 show mac-address-table staticfiltering

This command displays the Static Filtering entries in the Multicast Forwarding Database (MFDB) table.

Format `show mac-address-table staticfiltering`
Mode Privileged EXEC

Parameter	Definition
VLAN ID	The VLAN in which the MAC Address is learned.
MAC Address	A unicast MAC address for which the switch has forwarding and or filtering information. As the data is gleaned from the MFDB, the address will be a multicast address. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.

Parameter	Definition
Type	The type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

5.24 DHCP L2 Relay Agent Commands

You can enable the switch to operate as a DHCP Layer 2 relay agent to relay DHCP requests from clients to a Layer 3 relay agent or server. The Circuit ID and Remote ID can be added to DHCP requests relayed from clients to a DHCP server. This information is included in DHCP Option 82, as specified in sections 3.1 and 3.2 of RFC3046.

5.24.0.1 dhcp l2relay

This command enables the DHCP Layer 2 Relay agent for an interface a range of interfaces in, or all interfaces. The subsequent commands mentioned in this section can only be used when the DHCP L2 relay is enabled.

Format `dhcp l2relay`

Mode
- Global Config
- Interface Config

5.24.0.1.1 no dhcp l2relay

This command disables DHCP Layer 2 relay agent for an interface or range of interfaces.

Format `no dhcp l2relay`

Mode
- Global Config
- Interface Config

5.24.0.2 dhcp l2relay circuit-id subscription-name

This command sets the Option-82 Circuit ID for a given service subscription identified by `subscription-string` on a given interface. The `subscription-string` is a character string which needs to be matched with a configured DOT1AD subscription string for correct operation. When circuit-id is enabled using this command, all Client DHCP requests that fall under this service subscription are added with Option-82 circuit-id as the incoming interface number.

Default disabled

Format `dhcp l2relay circuit-id subscription-name subscription-string`

Mode Interface Config

5.24.0.2.1 no dhcp l2relay circuit-id subscription-name

This command resets the Option-82 Circuit ID for a given service subscription identified by `subscription-string` on a given interface. The `subscription-string` is a character string which needs to be matched with a configured DOT1AD subscription string for correct operation. When circuit-id is disabled using this command, all Client DHCP requests that fall under this service subscription are no longer added with Option-82 circuit-id.

Format `no dhcp l2relay circuit-id subscription-name` *`subscription-string`*

Mode Interface Config

5.24.0.3 dhcp l2relay circuit-id vlan

This parameter sets the DHCP Option-82 Circuit ID for a VLAN. When enabled, the interface number is added as the Circuit ID in DHCP option 82.

Format `dhcp l2relay circuit-id vlan` *`vlan-list`*
Mode Global Config

Parameter	Description
vlan–list	The VLAN ID. The range is 1–4093. Separate non-consecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.

5.24.0.3.1 no dhcp l2relay circuit-id vlan

This parameter clears the DHCP Option-82 Circuit ID for a VLAN.

Format `no dhcp l2relay circuit-id vlan` *`vlan-list`*
Mode Global Config

5.24.0.4 dhcp l2relay remote-id subscription-name

This command sets the Option-82 Remote-ID string for a given service subscription identified by `subscription-string` on a given interface or range of interfaces. The *subscription-string* is a character string which needs to be matched with a configured DOT1AD subscription string for correct operation. The *remoteid-string* is a character string. When remote-id string is set using this command, all Client DHCP requests that fall under this service subscription are added with Option-82 Remote-id as the configured remote-id string.

Default empty string
Format `dhcp l2relay remote-id` *`remoteid-string`* `subscription-name` *`subscription-string`*
Mode Interface Config

5.24.0.4.1 no dhcp l2relay remote-id subscription-name

This command resets the Option-82 Remote-ID string for a given service subscription identified by *subscription-string* on a given interface. The *subscription-string* is a character string which needs to be matched with a configured DOT1AD subscription string for correct operation. When remote-id string is reset using this command, the Client DHCP requests that fall under this service subscription are not added with Option-82 Remote-id.

Format `no dhcp l2relay remote-id` *`remoteid-string`* `subscription-name` *`subscription-string`*
Mode Interface Config

5.24.0.5 dhcp l2relay remote-id vlan

This parameter sets the DHCP Option-82 Remote ID for a VLAN and subscribed service (based on subscription-name).

Format `dhcp l2relay remote-id` *`remote-id-string`* `vlan` *`vlan-list`*
Mode Global Config

Parameter	Description
vlan–list	The VLAN ID. The range is 1–4093. Separate non-consecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.

5.24.0.5.1 no dhcp l2relay remote-id vlan

This parameter clears the DHCP Option-82 Remote ID for a VLAN and subscribed service (based on subscription-name).

Format `no dhcp l2relay remote-id vlan` *`vlan-list`*

Mode Global Config

5.24.0.6 dhcp l2relay subscription-name

This command enables relaying DHCP packets on an interface or range of interfaces that fall under the specified service subscription. The *subscription-string* is a character string that needs to be matched with configured DOT1AD subscription string for correct operation.

Default disabled (i.e. no DHCP packets are relayed)

Format `dhcp l2relay subscription-name` *`subscription-string`*

Mode Interface Config

5.24.0.6.1 no dhcp l2relay subscription-name

This command disables relaying DHCP packets that fall under the specified service subscription. The *subscription-string* is a character string that needs to be matched with configured DOT1AD subscription string for correct operation.

Format `no dhcp l2relay subscription-name` *`subscription-string`*

Mode Interface Config

5.24.0.7 dhcp l2relay trust

Use this command to configure an interface or range of interfaces as trusted for Option-82 reception.

Default untrusted

Format `dhcp l2relay trust`

Mode Interface Config

5.24.0.7.1 no dhcp l2relay trust

Use this command to configure an interface to the default untrusted for Option-82 reception.

Format `no dhcp l2relay trust`

Mode Interface Config

5.24.0.8 dhcp l2relay vlan

Use this command to enable the DHCP L2 Relay agent for a set of VLANs. All DHCP packets which arrive on interfaces in the configured VLAN are subject to L2 Relay processing.

Default `disable`

Format `dhcp l2relay vlan` *`vlan-list`*

Mode Global Config

Parameter	Description
vlan–list	The VLAN ID. The range is 1–4093. Separate non-consecutive IDs with a comma (,) no spaces and no zeros in between the range. Use a dash (–) for the range.

5.24.0.8.1 no dhcp l2relay vlan

Use this command to disable the DHCP L2 Relay agent for a set of VLANs.

Format `no dhcp l2relay vlan` *`vlan-list`*

Mode Global Config

5.24.0.9 show dhcp l2relay all

This command displays the summary of DHCP L2 Relay configuration.

Format `show dhcp l2relay all`

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Switching) #show dhcp l2relay all

DHCP L2 Relay is Enabled.

Interface  L2RelayMode   TrustMode
---------  -----------  --------------
 0/2        Enabled      untrusted
 0/4        Disabled     trusted

VLAN Id    L2 Relay  CircuitId  RemoteId
--------- ----------  ---------- ------------
3           Disabled    Enabled    --NULL--
5           Enabled     Enabled    --NULL--
6           Enabled     Enabled    broadcom
7           Enabled     Disabled   --NULL--
8           Enabled     Disabled   --NULL--
9           Enabled     Disabled   --NULL--
10          Enabled     Disabled   --NULL--
```

5.24.0.10 show dhcp l2relay circuit-id vlan

This command displays DHCP circuit-id vlan configuration.

Format `show dhcp l2relay circuit-id vlan` *`vlan-list`*
Mode Privileged EXEC

Parameter	Description
vlan-list	Enter VLAN IDs in the range 1–4093. Use a dash (–) to specify a range or a comma (,) to separate VLAN IDs in a list. Spaces and zeros are not permitted.

5.24.0.11 show dhcp l2relay interface

This command displays DHCP L2 relay configuration specific to interfaces.

Format `show dhcp l2relay interface {all |` *`interface-num`*`}`
Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Switching) #show dhcp l2relay interface all

DHCP L2 Relay is  Enabled.

Interface  L2RelayMode   TrustMode
---------  -----------  --------------
 0/2        Enabled      untrusted
 0/4        Disabled     trusted
```

5.24.0.12 show dhcp l2relay remote-id vlan

This command displays DHCP Remote-id vlan configuration.

Format `show dhcp l2relay remote-id vlan` *`vlan-list`*
Mode Privileged EXEC

Parameter	Description
vlan-list	Enter VLAN IDs in the range 1–4093. Use a dash (–) to specify a range or a comma (,) to separate VLAN IDs in a list. Spaces and zeros are not permitted.

5.24.0.13 show dhcp l2relay stats interface

This command displays statistics specific to DHCP L2 Relay configured interface.

Format `show dhcp l2relay stats interface {all |` *`interface-num`*`}`
Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Switching) #show dhcp l2relay stats interface all

DHCP L2 Relay is  Enabled.
```

```
Interface  UntrustedServer    UntrustedClient  TrustedServer     TrustedClient
            MsgsWithOpt82    MsgsWithOpt82    MsgsWithoutOpt82  MsgsWithoutOpt82
---------  --------------- -----------------  ----------------- --------------
 0/1           0                 0                 0                 0
 0/2           0                 0                 3                 7
 0/3           0                 0                 0                 0
 0/4           0                 12                0                 0
 0/5           0                 0                 0                 0
 0/6           3                 0                 0         0
 0/7           0                 0                 0                 0
 0/8           0                 0                 0                 0
 0/9           0                 0                 0                 0
```

5.24.0.14 show dhcp l2relay subscription interface

This command displays DHCP L2 Relay configuration specific to a service subscription on an interface.

Format `show dhcp l2relay subscription interface {all|`*`interface-num`*`}`

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Switching) #show dhcp l2relay subscription interface all
Interface   SubscriptionName    L2Relay mode  Circuit-Id mode  Remote-Id mode
----------  ----------------   -------------- ---------------  ----------------
  0/1             sub1             Enabled       Disabled         --NULL--
  0/2             sub3             Enabled       Disabled         EnterpriseSwitch
  0/2             sub22            Disabled      Enabled          --NULL--
  0/4             sub4             Enabled       Enabled          --NULL--
```

5.24.0.15 show dhcp l2relay agent-option vlan

This command displays the DHCP L2 Relay Option-82 configuration specific to VLAN.

Format `show dhcp l2relay agent-option vlan` *`vlan-range`*

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Switching) #show dhcp l2relay agent-option vlan 5-10

DHCP L2 Relay is  Enabled.

VLAN Id    L2 Relay    CircuitId  RemoteId
--------- ----------  ----------- ------------
5           Enabled     Enabled    --NULL--
6           Enabled     Enabled    broadcom
7           Enabled     Disabled   --NULL--
8           Enabled     Disabled   --NULL--
9           Enabled     Disabled   --NULL--
10          Enabled     Disabled   --NULL--
```

5.24.0.16 show dhcp l2relay vlan

This command displays DHCP vlan configuration.

Format `show dhcp l2relay vlan` *`vlan-list`*

Mode Privileged EXEC

Parameter	Description
vlan-list	Enter VLAN IDs in the range 1–4093. Use a dash (–) to specify a range or a comma (,) to separate VLAN IDs in a list. Spaces and zeros are not permitted.

5.24.0.17 clear dhcp l2relay statistics interface

Use this command to reset the DHCP L2 relay counters to zero. Specify the port with the counters to clear, or use the `all` keyword to clear the counters on all ports.

Format `clear dhcp l2relay statistics interface {`*`slot/port`* `|` *`all`*`}`

Mode Privileged EXEC

5.25 DHCP Client Commands

EFOS can include vendor and configuration information in DHCP client requests sent to a DHCP server. This information is included in DHCP Option 60, Vendor Class Identifier. The information is a string of 128 octets.

5.25.0.1 dhcp client vendor-id-option

This command enables the inclusion of DHCP Option-60, Vendor Class Identifier included in the requests transmitted to the DHCP server by the DHCP client operating in the EFOS switch.

Format `dhcp client vendor-id-option` *`string`*
Mode Global Config

5.25.0.1.1 no dhcp client vendor-id-option

This command disables the inclusion of DHCP Option-60, Vendor Class Identifier included in the requests transmitted to the DHCP server by the DHCP client operating in the EFOS switch.

Format `no dhcp client vendor-id-option`
Mode Global Config

5.25.0.2 dhcp client vendor-id-option-string

This parameter sets the DHCP Vendor Option-60 string to be included in the requests transmitted to the DHCP server by the DHCP client operating in the EFOS switch.

Format `dhcp client vendor-id-option-string` *`string`*
Mode Global Config

5.25.0.2.1 no dhcp client vendor-id-option-string

This parameter clears the DHCP Vendor Option-60 string.

Format `no dhcp client vendor-id-option-string`
Mode Global Config

5.25.0.3 show dhcp client vendor-id-option

This command displays the configured administration mode of the vendor-id-option and the vendor-id string to be included in Option-43 in DHCP requests.

Format `show dhcp client vendor-id-option`
Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Switching) #show dhcp client vendor-id-option

DHCP Client Vendor Identifier Option.....Enabled
```

```
DHCP Client Vendor Identifier Option String...EFOSClient.
```

5.26 DHCP Snooping Configuration Commands

This section describes commands you use to configure DHCP Snooping.

5.26.0.1 ip dhcp snooping

Use this command to enable DHCP Snooping globally.

Default	disabled
Format	`ip dhcp snooping`
Mode	Global Config

5.26.0.1.1 no ip dhcp snooping

Use this command to disable DHCP Snooping globally.

Format	`no ip dhcp snooping`
Mode	Global Config

5.26.0.2 ip dhcp snooping vlan

Use this command to enable DHCP Snooping on a list of comma-separated VLAN ranges.

Default	disabled
Format	`ip dhcp snooping vlan` *`vlan-list`*
Mode	Global Config

5.26.0.2.1 no ip dhcp snooping vlan

Use this command to disable DHCP Snooping on VLANs.

Format	`no ip dhcp snooping vlan` *`vlan-list`*
Mode	Global Config

5.26.0.3 ip dhcp snooping verify mac-address

Use this command to enable verification of the source MAC address with the client hardware address in the received DCHP message.

Default	enabled
Format	`ip dhcp snooping verify mac-address`
Mode	Global Config

5.26.0.3.1 no ip dhcp snooping verify mac-address

Use this command to disable verification of the source MAC address with the client hardware address.

Format `no ip dhcp snooping verify mac-address`
Mode Global Config

5.26.0.4 ip dhcp snooping database

Use this command to configure the persistent location of the DHCP Snooping database. This can be local or a remote file on a given IP machine.

Default local
Format `ip dhcp snooping database {local|tftp://hostIP/filename}`
Mode Global Config

5.26.0.5 ip dhcp snooping database write-delay

Use this command to configure the interval in seconds at which the DHCP Snooping database will be persisted. The interval value ranges from 15 to 86400 seconds.

Default 300 seconds
Format `ip dhcp snooping database write-delay in seconds`
Mode Global Config

5.26.0.5.1 no ip dhcp snooping database write-delay

Use this command to set the write delay value to the default value.

Format `no ip dhcp snooping database write-delay`
Mode Global Config

5.26.0.6 ip dhcp snooping binding

Use this command to configure static DHCP Snooping binding.

Format `ip dhcp snooping binding` *`mac-address`* `vlan` *`vlan id ip address`* `interface` *`interface id`*
Mode Global Config

5.26.0.6.1 no ip dhcp snooping binding

Use this command to remove the DHCP static entry from the DHCP Snooping database.

Format `no ip dhcp snooping binding` *`mac-address`*
Mode Global Config

5.26.0.7 ip verify binding

Use this command to configure static IP source guard (IPSG) entries.

Format `ip verify binding` *`mac-address`* `vlan` *`vlan id ip address`* `interface` *`interface id`*

Mode Global Config

5.26.0.7.1 no ip verify binding

Use this command to remove the IPSG static entry from the IPSG database.

Format `no ip verify binding` *`mac-address`* `vlan` *`vlan id ip address`* `interface` *`interface id`*
Mode Global Config

5.26.0.8 ip dhcp snooping limit

Use this command to control the rate at which the DHCP Snooping messages come on an interface or range of interfaces. By default, rate limiting is disabled. When enabled, the rate can range from 0 to 300 packets per second. The burst level range is 1 to 15 seconds.

Default disabled (no limit)
Format `ip dhcp snooping limit {rate pps [`*`burst interval seconds`*`]}`
Mode Interface Config

5.26.0.8.1 no ip dhcp snooping limit

Use this command to set the rate at which the DHCP Snooping messages come, and the burst level, to the defaults.

Format `no ip dhcp snooping limit`
Mode Interface Config

5.26.0.9 ip dhcp snooping log-invalid

Use this command to control the logging DHCP messages filtration by the DHCP Snooping application. This command can be used to configure a single interface or a range of interfaces.

Default disabled
Format `ip dhcp snooping log-invalid`
Mode Interface Config

5.26.0.9.1 no ip dhcp snooping log-invalid

Use this command to disable the logging DHCP messages filtration by the DHCP Snooping application.

Format `no ip dhcp snooping log-invalid`
Mode Interface Config

5.26.0.10 ip dhcp snooping trust

Use this command to configure an interface or range of interfaces as trusted.

Default disabled
Format `ip dhcp snooping trust`

Mode Interface Config

5.26.0.10.1 no ip dhcp snooping trust

Use this command to configure the port as untrusted.

Format `no ip dhcp snooping trust`
Mode Interface Config

5.26.0.11 ip verify source

Use this command to configure the IPSG source ID attribute to filter the data traffic in the hardware. Source ID is the combination of IP address and MAC address. Normal command allows data traffic filtration based on the IP address. With the “port-security” option, the data traffic will be filtered based on the IP and MAC addresses.

This command can be used to configure a single interface or a range of interfaces.

Default `the source ID is the IP address`
Format `ip verify source {port-security}`
Mode Interface Config

5.26.0.11.1 no ip verify source

Use this command to disable the IPSG configuration in the hardware. You cannot disable port-security alone if it is configured.

Format `no ip verify source`
Mode Interface Config

5.26.0.12 show ip dhcp snooping

Use this command to display the DHCP Snooping global configurations and per port configurations.

Format `show ip dhcp snooping`
Mode
- Privileged EXEC
- User EXEC

Parameter	Definition
Interface	The interface for which data is displayed.
Trusted	If it is enabled, DHCP snooping considers the port as trusted. The factory default is disabled.
Log Invalid Pkts	If it is enabled, DHCP snooping application logs invalid packets on the specified interface.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip dhcp snooping
DHCP snooping is Disabled
DHCP snooping source MAC verification is enabled
DHCP snooping is enabled on the following VLANs:
```

```
11 - 30, 40

Interface   Trusted    Log Invalid Pkts
---------   --------   ----------------
0/1          Yes             No
0/2          No             Yes
0/3          No             Yes
0/4          No              No
```

5.26.0.13 show ip dhcp snooping binding

Use this command to display the DHCP Snooping binding entries. To restrict the output, use the following options:

- Dynamic: Restrict the output based on DCHP snooping.
- Interface: Restrict the output based on a specific interface.
- Static: Restrict the output based on static entries.
- VLAN: Restrict the output based on VLAN.

Format `show ip dhcp snooping binding [{static/dynamic}] [interface` *`slot/port`*`] [vlan id]`

Mode
- Privileged EXEC
- User EXEC

Parameter	Definition
MAC Address	Displays the MAC address for the binding that was added. The MAC address is the key to the binding database.
IP Address	Displays the valid IP address for the binding rule.
VLAN	The VLAN for the binding rule.
Interface	The interface to add a binding into the DHCP snooping interface.
Type	Binding type; statically configured from the CLI or dynamically learned.
Lease (sec)	The remaining lease time for the entry.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip dhcp snooping binding

Total number of bindings: 2

MAC Address          IP Address   VLAN  Interface  Type  Lease time (Secs)
------------------  ------------  ----  ---------  ---- ------------------
00:02:B3:06:60:80   210.1.1.3      10   0/1              86400
00:0F:FE:00:13:04   210.1.1.4      10   0/1              86400
```

5.26.0.14 show ip dhcp snooping database

Use this command to display the DHCP Snooping configuration related to the database persistency.

Format `show ip dhcp snooping database`

Mode
- Privileged EXEC
- User EXEC

Parameter	Definition
Agent URL	Bindings database agent URL.
Write Delay	The maximum write time to write the database into local or remote.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip dhcp snooping database

agent url:  /10.131.13.79:/sai1.txt

write-delay:  5000
```

5.26.0.15 show ip dhcp snooping interfaces

Use this command to show the DHCP Snooping status of the interfaces.

Format `show ip dhcp snooping interfaces`

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip dhcp snooping interfaces

 Interface    Trust State  Rate Limit    Burst Interval
                              (pps)       (seconds)
-----------   ----------   ----------   --------------
   0/1             No           15              1
   0/2             No           15              1
   0/3             No           15              1

(Routing) #show ip dhcp snooping interfaces ethernet 0/15

 Interface    Trust State  Rate Limit    Burst Interval
                              (pps)       (seconds)
-----------   ----------   ----------   --------------
   0/15            Yes          15              1
```

5.26.0.16 show ip dhcp snooping statistics

Use this command to list statistics for DHCP Snooping security violations on untrusted ports.

Format `show ip dhcp snooping statistics`

Mode
- Privileged EXEC
- User EXEC

Parameter	Definition
Interface	The IP address of the interface in *slot/port* format.
MAC Verify Failures	Represents the number of DHCP messages that were filtered on an untrusted interface because of source MAC address and client HW address mismatch.
Client Ifc Mismatch	Represents the number of DHCP release and Deny messages received on the different ports than learned previously.

Parameter	Definition
DHCP Server Msgs Rec'd	Represents the number of DHCP server messages received on Untrusted ports.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip dhcp snooping statistics

 Interface    MAC Verify   Client Ifc   DHCP Server
               Failures     Mismatch    Msgs Rec'd
-----------   ----------   ----------   -----------
0/2                  0            0             0
0/3                  0            0             0
0/4                  0            0             0
0/5                  0            0             0
0/6                  0            0             0
0/7                  0            0             0
0/8                  0            0             0
0/9                  0            0             0
0/10                 0            0             0
0/11                 0            0             0
0/12                 0            0             0
0/13                 0            0             0
0/14                 0            0             0
0/15                 0            0             0
0/16                 0            0             0
0/17                 0            0             0
0/18                 0            0             0
0/19                 0            0             0
0/20                 0            0             0
```

5.26.0.17 clear ip dhcp snooping binding

Use this command to clear all DHCP Snooping bindings on all interfaces or on a specific interface.

Format `clear ip dhcp snooping binding [interface` *`slot/port`*`]`

Mode
- Privileged EXEC
- User EXEC

5.26.0.18 clear ip dhcp snooping statistics

Use this command to clear all DHCP Snooping statistics.

Format `clear ip dhcp snooping statistics`

Mode
- Privileged EXEC
- User EXEC

5.26.0.19 show ip verify source

Use this command to display the IPSG configurations on all ports.

Format `show ip verify source`

Mode
- Privileged EXEC
- User EXEC

Parameter	Definition
Interface	Interface address in *slot/port* format.
Filter Type	Is one of two values: ■ ip-mac: User has configured MAC address filtering on this interface. ■ ip: Only IP address filtering on this interface.
IP Address	IP address of the interface
MAC Address	If MAC address filtering is not configured on the interface, the MAC Address field is empty. If port security is disabled on the interface, then the MAC Address field displays “permit-all.”
VLAN	The VLAN for the binding rule.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip verify source

Interface  Filter Type    IP Address       MAC Address      Vlan
---------  -----------  ---------------  -----------------  -----
    0/1     ip-mac       210.1.1.3       00:02:B3:06:60:80     10
    0/1     ip-mac       210.1.1.4       00:0F:FE:00:13:04     10
```

5.26.0.20 show ip verify interface

Use this command to display the IPSG filter type for a specific interface.

Format `show ip verify interface` *slot/port*

Mode
- Privileged EXEC
- User EXEC

Parameter	Definition
Interface	Interface address in *slot/port* format.
Filter Type	Is one of two values: ■ ip-mac: User has configured MAC address filtering on this interface. ■ ip: Only IP address filtering on this interface.

5.26.0.21 show ip source binding

Use this command to display the IPSG bindings.

Format `show ip source binding [{static/dynamic}] [interface` *slot/port*`] [vlan id]`

Mode
- Privileged EXEC
- User EXEC

Parameter	Definition
MAC Address	The MAC address for the entry that is added.
IP Address	The IP address of the entry that is added.
Type	Entry type; statically configured from CLI or dynamically learned from DHCP Snooping.
VLAN	VLAN for the entry.
Interface	IP address of the interface in *slot/port* format.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip source binding

MAC Address        IP Address        Type          Vlan     Interface
-----------------  ---------------  -------------  -----  -------------
00:00:00:00:00:08          1.2.3.4  dhcp-snooping     2    0/1
00:00:00:00:00:09          1.2.3.4  dhcp-snooping     3    0/1
00:00:00:00:00:0A          1.2.3.4  dhcp-snooping     4    0/1
```

5.27 Dynamic ARP Inspection Commands

Dynamic ARP Inspection (DAI) is a security feature that rejects invalid and malicious ARP packets. DAI prevents a class of man-in-the-middle attacks, where an unfriendly station intercepts traffic for other stations by poisoning the ARP caches of its unsuspecting neighbors. The miscreant sends ARP requests or responses mapping another station's IP address to its own MAC address.

DAI relies on DHCP snooping. DHCP snooping listens to DHCP message exchanges and builds a binding database of valid {MAC address, IP address, VLAN, and interface} tuples.

When DAI is enabled, the switch drops ARP packets whose sender MAC address and sender IP address do not match an entry in the DHCP snooping bindings database. You can optionally configure additional ARP packet validation.

5.27.0.1 ip arp inspection vlan

Use this command to enable Dynamic ARP Inspection on a list of comma-separated VLAN ranges.

Default	`disabled`
Format	`ip arp inspection vlan vlan-list`
Mode	Global Config

5.27.0.1.1 no ip arp inspection vlan

Use this command to disable Dynamic ARP Inspection on a list of comma-separated VLAN ranges.

Format	`no ip arp inspection vlan vlan-list`
Mode	Global Config

5.27.0.2 ip arp inspection validate

Use this command to enable additional validation checks like source-mac validation, destination-mac validation, and ip address validation on the received ARP packets. Each command overrides the configuration of the previous command. For example, if a command enables src-mac and dst-mac validations, and a second command enables IP validation only, the src-mac and dst-mac validations are disabled as a result of the second command.

Default	`disabled`
Format	`ip arp inspection validate {[src-mac] [dst-mac] [ip]}`
Mode	Global Config

5.27.0.2.1 no ip arp inspection validate

Use this command to disable the additional validation checks on the received ARP packets.

Format	`no ip arp inspection validate {[src-mac] [dst-mac] [ip]}`
Mode	Global Config

5.27.0.3 ip arp inspection validate interface

Use this command to enable source interface validation checks in the DHCP snooping binding database on the received ARP packets.

Default enabled
Format `ip arp inspection validate interface`
Mode Global Config

5.27.0.3.1 no ip arp inspection validate interface

Use this command to disable the source interface check against the DHCP snooping binding database entry on the received ARP packets.

Format `no ip arp inspection validate interface`
Mode Global Config

5.27.0.4 ip arp inspection vlan logging

Use this command to enable logging of invalid ARP packets on a list of comma-separated VLAN ranges.

Default `enabled`
Format `ip arp inspection vlan vlan-list logging`
Mode Global Config

5.27.0.4.1 no ip arp inspection vlan logging

Use this command to disable logging of invalid ARP packets on a list of comma-separated VLAN ranges.

Format `no ip arp inspection vlan vlan-list logging`
Mode Global Config

5.27.0.5 ip arp inspection trust

Use this command to configure an interface or range of interfaces as trusted for Dynamic ARP Inspection.

Default `disabled`
Format `ip arp inspection trust`
Mode Interface Config

5.27.0.5.1 no ip arp inspection trust

Use this command to configure an interface as untrusted for Dynamic ARP Inspection.

Format `no ip arp inspection trust`
Mode Interface Config

5.27.0.6 ip arp inspection limit

Use this command to configure the rate limit and burst interval values for an interface or range of interfaces. Configuring `none` for the limit means the interface is not rate limited for Dynamic ARP Inspections. The maximum pps value shown in the range for the rate option might be more than the hardware allowable limit. Therefore you need to understand the switch performance and configure the maximum rate pps accordingly.

NOTE: The user interface will accept a rate limit for a trusted interface, but the limit will not be enforced unless the interface is configured to be untrusted.

Default	`15 pps for rate and 1 second for burst-interval`
Format	`ip arp inspection limit {rate pps [burst interval seconds] | none}`
Mode	Interface Config

5.27.0.6.1 no ip arp inspection limit

Use this command to set the rate limit and burst interval values for an interface to the default values of 15 pps and 1 second, respectively.

Format	`no ip arp inspection limit`
Mode	Interface Config

5.27.0.7 ip arp inspection filter

Use this command to configure the ARP ACL used to filter invalid ARP packets on a list of comma-separated VLAN ranges. If the static keyword is given, packets that do not match a permit statement are dropped without consulting the DHCP snooping bindings.

Default	`No ARP ACL is configured on a VLAN`
Format	`ip arp inspection filter acl-name vlan vlan-list [static]`
Mode	Global Config

5.27.0.7.1 no ip arp inspection filter

Use this command to unconfigure the ARP ACL used to filter invalid ARP packets on a list of comma-separated VLAN ranges.

Format	`no ip arp inspection filter acl-name vlan vlan-list [static]`
Mode	Global Config

5.27.0.8 arp access-list

Use this command to create an ARP ACL.

Format	`arp access-list acl-name`
Mode	Global Config

5.27.0.8.1 no arp access-list

Use this command to delete a configured ARP ACL.

Format `no arp access-list acl-name`
Mode Global Config

5.27.0.9 deny ip host mac host

Use this command to configure an explicit deny rule for a valid IP address and MAC address combination used in ARP packet validation.

Format `deny ip {any | host` ***sender-ip***`} mac {any | host` ***sender-mac***`}`
Mode ARP Access-list Config

5.27.0.9.1 no deny ip host mac host

Use this command to delete a deny rule for a valid IP address and MAC address combination.

Format `no deny ip {any | host` ***sender-ip***`} mac {any | host` ***sender-mac***`}`
Mode ARP Access-list Config

5.27.0.10 permit ip host mac host

Use this command to configure an explicit permit rule for a valid IP address and MAC address combination used in ARP packet validation.

Format `permit ip {any | host` ***sender-ip***`} mac {any | host` ***sender-mac***`}`
Mode ARP Access-list Config

5.27.0.10.1 no permit ip host mac host

Use this command to delete an explicit permit rule for a valid IP and MAC combination.

Format `no permit ip {any | host` ***sender-ip***`} mac {any | host` ***sender-mac***`}`
Mode ARP Access-list Config

5.27.0.11 show ip arp inspection

Use this command to display the Dynamic ARP Inspection global configuration and configuration on all the VLANs. With the *vlan-list* argument (i.e. comma separated VLAN ranges), the command displays the global configuration and configuration on all the VLANs in the given VLAN list. The global configuration includes the **source mac validation**, **destination mac validation** and **invalid IP validation** information.

Format `show ip arp inspection [{interfaces` ***slot/port***`| vlan` ***vlan-list***`]`
Mode
- Privileged EXEC
- User EXEC

Parameter	Definition
Source MAC Validation	Displays whether Source MAC Validation of ARP frame is enabled or disabled.
Destination MAC Validation	Displays whether Destination MAC Validation is enabled or disabled.
IP Address Validation	Displays whether IP Address Validation is enabled or disabled.
VLAN	The VLAN ID for each displayed row.
Configuration	Displays whether DAI is enabled or disabled on the VLAN.
Log Invalid	Displays whether logging of invalid ARP packets is enabled on the VLAN.
ACL Name	The ARP ACL Name, if configured on the VLAN.
Static Flag	If the ARP ACL is configured static on the VLAN.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip arp inspection vlan 10-12

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan          Configuration    Log Invalid   ACL Name   Static flag
 ----          -------------    -----------   ---------  -----------
   10          Enabled          Enabled       H2         Enabled
   11          Disabled         Enabled
   12          Enabled          Disabled
```

5.27.0.12 show ip arp inspection statistics

Use this command to display the statistics of the ARP packets processed by Dynamic ARP Inspection. Give the vlan-list argument and the command displays the statistics on all DAI-enabled VLANs in that list. Give the single vlan argument and the command displays the statistics on that VLAN. If no argument is included, the command lists a summary of the forwarded and dropped ARP packets.

Format `show ip arp inspection statistics [vlan vlan-list]`

Mode
- Privileged EXEC
- User EXEC

Parameter	Definition
VLAN	The VLAN ID for each displayed row.
Forwarded	The total number of valid ARP packets forwarded in this VLAN.
Dropped	The total number of not valid ARP packets dropped in this VLAN.
DHCP Drops	The number of packets dropped due to DHCP snooping binding database match failure.
ACL Drops	The number of packets dropped due to ARP ACL rule match failure.
DHCP Permits	The number of packets permitted due to DHCP snooping binding database match.
ACL Permits	The number of packets permitted due to ARP ACL rule match.
ACL Denials	The number of packets denied due to ARP ACL deny rule match.
Bad Src MAC	The number of packets dropped due to Source MAC validation failure.

Parameter	Definition
Bad Dest MAC	The number of packets dropped due to Destination MAC validation failure.
Invalid IP	The number of packets dropped due to invalid IP checks.

Example: The following shows example CLI display output for the command **show ip arp inspection statistics** which lists the summary of forwarded and dropped ARP packets on all DAI-enabled VLANs.

```
(Routing) #show ip arp inspection


VLAN  Forwarded  Dropped
----  ---------  -------
  10         90       14
  20         10        3
```

Example: The following shows example CLI display output for the command `show ip arp inspection statistics vlan 10,20.`

```
VLAN    DHCP      ACL       DHCP       ACL        ACL       Bad Src   Bad Dest   Invalid
       Drops     Drops     Permits    Permits    Denials   MAC       MAC        IP
----- -------- --------- ---------- ---------  --------- ---------- ---------- ---------
10      11        1           65         25          5         1         1         0
20      1         0            8          2          3         0         1         1
```

5.27.0.13 clear ip arp inspection statistics

Use this command to reset the statistics for Dynamic ARP Inspection on all VLANs.

Default `none`

Format `clear ip arp inspection statistics`

Mode Privileged EXEC

5.27.0.14 show ip arp inspection interfaces

Use this command to display the Dynamic ARP Inspection configuration on all the DAI-enabled interfaces. An interface is said to be enabled for DAI if at least one VLAN, that the interface is a member of, is enabled for DAI. Given a *`slot/port`* interface argument, the command displays the values for that interface whether the interface is enabled for DAI or not.

Format `show ip arp inspection interfaces [`*`slot/port`*`]`

Mode
- Privileged EXEC
- User EXEC

Parameter	Definition
Interface	The interface ID for each displayed row.
Trust State	Whether the interface is trusted or untrusted for DAI.
Rate Limit	The configured rate limit value in packets per second.
Burst Interval	The configured burst interval value in seconds.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip arp inspection interfaces

 Interface        Trust State   Rate Limit   Burst Interval
                                   (pps)        (seconds)
 ---------------  -----------   ----------  ---------------
 0/1                Untrusted           15                1
 0/2                Untrusted           10               10
```

5.27.0.15 show arp access-list

Use this command to display the configured ARP ACLs with the rules. Giving an ARP ACL name as the argument will display only the rules in that ARP ACL.

Format `show arp access-list [acl-name]`

Mode
- Privileged EXEC
- User EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) #show arp access-list
ARP access list H2
permit ip host 1.1.1.1 mac host 00:01:02:03:04:05
permit ip host 1.1.1.2 mac host 00:03:04:05:06:07
deny ip host 1.1.1.3 mac host 00:08:09:0A:0B:0C
ARP access list H3
ARP access list H4
permit ip host 1.1.1.3 mac any
deny ip any mac host 00:11:11:11:11:11
ARP access list H5
permit ip host 2.1.1.2 mac host 00:03:04:05:06:08
```

5.28 IGMP Snooping Configuration Commands

This section describes the commands you use to configure IGMP snooping. EFOS software supports IGMP Versions 1, 2, and 3. The IGMP snooping feature can help conserve bandwidth because it allows the switch to forward IP multicast traffic only to connected hosts that request multicast traffic. IGMPv3 adds source filtering capabilities to IGMP versions 1 and 2.

NOTE: This note clarifies the prioritization of MGMD Snooping Configurations. Many of the IGMP Snooping commands are available both in the Interface and VLAN modes. Operationally the system chooses or prefers the VLAN configured values over the Interface configured values for most configurations when the interface participates in the VLAN.

5.28.0.1 set igmp

This command enables IGMP Snooping on the system (Global Config Mode), an interface, or a range of interfaces. This command also enables IGMP snooping on a particular VLAN (VLAN Database Mode) and can enable IGMP snooping on all interfaces participating in a VLAN.

If an interface has IGMP Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (LAG), IGMP Snooping functionality is disabled on that interface. IGMP Snooping functionality is reenabled if you disable routing or remove port-channel (LAG) membership from an interface that has IGMP Snooping enabled.

The IGMP application supports the following activities:

- Validation of the IP header checksum (as well as the IGMP header checksum) and discarding of the frame upon checksum error.
- Maintenance of the forwarding table entries based on the MAC address versus the IP address.
- Flooding of unregistered multicast data packets to all ports in the VLAN.

Default disabled

Format `set igmp [vlan_id]`

Mode
- Global Config
- Interface Config
- VLAN Database

5.28.0.1.1 no set igmp

This command disables IGMP Snooping on the system, an interface, a range of interfaces, or a VLAN.

Format `no set igmp [vlan_id]`

Mode
- Global Config
- Interface Config
- VLAN Database

5.28.0.2 set igmp header-validation

This command enables header validation for IGMP messages.

When header validation is enabled, IGMP Snooping checks:

- The time-to-live(TTL) field in the IGMP header and drops packets where TTL is not equal to 1. The TTL field should always be set to 1 in the headers of IGMP reports and queries.
- The presence of the router alert option (9404) in the IP packet header of the IGMPv2 message and drops packets that do not include this option.

- The presence of the router alert option (9404) and ToS Byte = 0xC0 (Internet Control) in the IP packet header of IGMPv3 message and drops packets that do not include these options.

Default enabled

Format `set igmp header-validation`

Mode Global Config

5.28.0.2.1 no set igmp header-validation

This command disables header validation for IGMP messages.

Format `no set igmp header-validation`

Mode Global Config

5.28.0.3 set igmp interfacemode

This command enables IGMP Snooping on all interfaces. If an interface has IGMP Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (LAG), IGMP Snooping functionality is disabled on that interface. IGMP Snooping functionality is reenabled if you disable routing or remove port-channel (LAG) membership from an interface that has IGMP Snooping enabled.

Default disabled

Format `set igmp interfacemode`

Mode Global Config

5.28.0.3.1 no set igmp interfacemode

This command disables IGMP Snooping on all interfaces.

Format `no set igmp interfacemode`

Mode Global Config

5.28.0.4 set igmp fast-leave

This command enables or disables IGMP Snooping fast-leave admin mode on a selected interface, a range of interfaces, or a VLAN. Enabling fast-leave allows the switch to immediately remove the layer 2 LAN interface from its forwarding table entry upon receiving an IGMP leave message for that multicast group without first sending out MAC-based general queries to the interface.

You should enable fast-leave admin mode only on VLANs where only one host is connected to each layer 2 LAN port. This prevents the inadvertent dropping of the other hosts that were connected to the same layer 2 LAN port but were still interested in receiving multicast traffic directed to that group. Also, fast-leave processing is supported only with IGMP version 2 hosts.

Default disabled

Format `set igmp fast-leave [vlan_id]`

Mode Interface Config
Interface Range
VLAN Database

5.28.0.4.1 no set igmp fast-leave

This command disables IGMP Snooping fast-leave admin mode on a selected interface.

Format `no set igmp fast-leave [vlan_id]`

Mode Interface Config
Interface Range
VLAN Database

5.28.0.5 set igmp groupmembership-interval

This command sets the IGMP Group Membership Interval time on a VLAN, one interface, a range of interfaces, or all interfaces. The Group Membership Interval time is the amount of time in seconds that a switch waits for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the IGMPv3 Maximum Response time value. The range is 2 to 3600 seconds.

Default 260 seconds

Format `set igmp groupmembership-interval [vlan_id] 2-3600`

Mode
- Interface Config
- Global Config
- VLAN Database

5.28.0.5.1 no set igmp groupmembership-interval

This command sets the IGMPv3 Group Membership Interval time to the default value.

Format `no set igmp groupmembership-interval [vlan_id]`

Mode
- Interface Config
- Global Config
- VLAN Database

5.28.0.6 set igmp maxresponse

This command sets the IGMP Maximum Response time for the system, on a particular interface or VLAN, or on a range of interfaces. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the IGMP Query Interval time value. The range is 1 to 25 seconds.

Default 10 seconds

Format `set igmp maxresponse [vlan_id] 1-25`

Mode
- Global Config
- Interface Config
- VLAN Database

5.28.0.6.1 no set igmp maxresponse

This command sets the max response time (on the interface or VLAN) to the default value.

Format `no set igmp maxresponse [vlan_id]`

Mode
- Global Config
- Interface Config
- VLAN Database

5.28.0.7 set igmp mcrtrexpiretime

This command sets the Multicast Router Present Expiration time. The time is set for the system, on a particular interface or VLAN, or on a range of interfaces. This is the amount of time in seconds that a switch waits for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 0 to 3600 seconds. A value of 0 indicates an infinite time-out, i.e. no expiration.

Default 0

Format `set igmp mcrtrexpiretime [vlan_id] 0-3600`

Mode
- Global Config
- Interface Config
- VLAN Database

5.28.0.7.1 no set igmp mcrtrexpiretime

This command sets the Multicast Router Present Expiration time to 0. The time is set for the system, on a particular interface or a VLAN.

Format `no set igmp mcrtrexpiretime [vlan_id]`

Mode
- Global Config
- Interface Config
- VLAN Database

Format `no set igmp mcrtrexpiretime vlan_id`

Mode VLAN Database

5.28.0.8 set igmp mrouter

This command configures the VLAN ID (*vlan_id*) that has the multicast router mode enabled.

Format `set igmp mrouter vlan_id`

Mode Interface Config

5.28.0.8.1 no set igmp mrouter

This command disables multicast router mode for a particular VLAN ID (*vlan_id*).

Format `no set igmp mrouter vlan_id`

Mode Interface Config

5.28.0.9 set igmp mrouter interface

This command configures the interface or range of interfaces as a multicast router interface. When configured as a multicast router interface, the interface is treated as a multicast router interface in all VLANs.

Default disabled

Format `set igmp mrouter interface`

Mode Interface Config

5.28.0.9.1 no set igmp mrouter interface

This command disables the status of the interface as a statically configured multicast router interface.

Format `no set igmp mrouter interface`

Mode Interface Config

5.28.0.10 set igmp report-suppression

Use this command to suppress the IGMP reports on a given VLAN ID. In order to optimize the number of reports traversing the network with no added benefits, a Report Suppression mechanism is implemented. When more than one client responds to an MGMD query for the same Multicast Group address within the max-response-time, only the first response is forwarded to the query and others are suppressed at the switch.

Default Disabled

Format `set igmp report-suppression` *`vlan-id`*

Mode VLAN Database

Parameter	Description
vlan-id	A valid VLAN ID. Range is 1 to 4093.

Example: The following shows an example of the command.

```
(Routing) #vlan database

(Routing) (Vlan)#set igmp report-suppression 1
```

5.28.0.10.1 no set igmp report-suppression

Use this command to return the system to the default.

Format `no set igmp report-suppression`

Mode VLAN Database

5.28.0.11 show igmpsnooping

This command displays IGMP Snooping information for a given *`slot/port`* or VLAN. Configured information is displayed whether or not IGMP Snooping is enabled.

Format `show igmpsnooping [`*`slot/port`* `|` *`vlan_id`*`]`

Mode Privileged EXEC

When the optional arguments *`slot/port`* or *`vlan_id`* are not used, the command displays the following information:

Term	Definition
Admin Mode	Indicates whether or not IGMP Snooping is active on the switch.
Multicast Control Frame Count	The number of multicast control frames that are processed by the CPU.
Interface Enabled for IGMP Snooping	The list of interfaces on which IGMP Snooping is enabled.
VLANS Enabled for IGMP Snooping	The list of VLANS on which IGMP Snooping is enabled.

When you specify the *slot/port* values, the following information appears:

Term	Definition
IGMP Snooping Admin Mode	Indicates whether IGMP Snooping is active on the interface.
Fast Leave Mode	Indicates whether IGMP Snooping Fast-leave is active on the interface.
Group Membership Interval	The amount of time in seconds that a switch will wait for a report from a particular group on a particular interface before deleting the interface from the entry.This value may be configured.
Maximum Response Time	The amount of time the switch waits after it sends a query on an interface because it did not receive a report for a particular group on that interface. This value may be configured.
Multicast Router Expiry Time	The amount of time to wait before removing an interface from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.

When you specify a value for *vlan_id*, the following information appears:

Term	Definition
VLAN ID	The VLAN ID.
IGMP Snooping Admin Mode	Indicates whether IGMP Snooping is active on the VLAN.
Fast Leave Mode	Indicates whether IGMP Snooping Fast-leave is active on the VLAN.
Group Membership Interval (secs)	The amount of time in seconds that a switch will wait for a report from a particular group on a particular interface, which is participating in the VLAN, before deleting the interface from the entry.This value may be configured.
Maximum Response Time (secs)	The amount of time the switch waits after it sends a query on an interface, participating in the VLAN, because it did not receive a report for a particular group on that interface. This value may be configured.
Multicast Router Expiry Time (secs)	The amount of time to wait before removing an interface that is participating in the VLAN from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.
Report Suppression Mode	Indicates whether IGMP reports (set by the command Section 5.28.0.10, set igmp report-suppression) in enabled or not.

Example: The following shows example CLI display output for the command.

```
(Routing) #show igmpsnooping 1

VLAN ID..................................... 1
IGMP Snooping Admin Mode.................... Disabled
Fast Leave Mode............................. Disabled
Group Membership Interval (secs)............ 260
Max Response Time (secs).................... 10
Multicast Router Expiry Time (secs)......... 0
Report Suppression Mode..................... Enabled
```

5.28.0.12 show igmpsnooping mrouter interface

This command displays information about statically configured ports.

Format `show igmpsnooping mrouter interface` *slot/port*

Mode Privileged EXEC

Term	Definition
Interface	The port on which multicast router information is being displayed.

Term	Definition
Multicast Router Attached	Indicates whether multicast router is statically enabled on the interface.
VLAN ID	The list of VLANs of which the interface is a member.

5.28.0.13 show igmpsnooping mrouter vlan

This command displays information about statically configured ports.

Format `show igmpsnooping mrouter vlan` *`slot/port`*
Mode Privileged EXEC

Term	Definition
Interface	The port on which multicast router information is being displayed.
VLAN ID	The list of VLANs of which the interface is a member.

5.28.0.14 show igmpsnooping ssm

This command displays information about Source Specific Multicasting (SSM) by entry, group, or statistics. SSM delivers multicast packets to receivers that originated from a source address specified by the receiver. SSM is only available with IGMPv3 and MLDv2.

Format `show igmpsnooping ssm {entries | groups | stats}`
Mode Privileged EXEC

5.28.0.15 show mac-address-table igmpsnooping

This command displays the IGMP Snooping entries in the MFDB table.

Format `show mac-address-table igmpsnooping`
Mode Privileged EXEC

Term	Definition
VLAN ID	The VLAN in which the MAC address is learned.
MAC Address	A multicast MAC address for which the switch has forwarding or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Type	The type of the entry, which is either static (added by the user) or dynamic (added to the table as a result of a learning process or protocol).
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

5.29 IGMP Snooping Querier Commands

IGMP Snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the “IGMP Querier”. The IGMP query responses, known as IGMP reports, keep the switch updated with the current multicast group membership on a port-by-port basis. If the switch does not receive updated membership information in a timely fashion, it will stop forwarding multicasts to the port where the end device is located.

This section describes commands used to configure and display information on IGMP Snooping Queriers on the network and, separately, on VLANs.

NOTE: This note clarifies the prioritization of MGMD Snooping Configurations. Many of the IGMP/MLD Snooping commands are available both in the Interface and VLAN modes. Operationally the system chooses or prefers the VLAN configured values over the Interface configured values for most configurations when the interface participates in the VLAN.

5.29.0.1 set igmp querier

Use this command to enable IGMP Snooping Querier on the system, using Global Config mode, or on a VLAN. Using this command, you can specify the IP Address that the Snooping Querier switch should use as the source address while generating periodic queries.

If a VLAN has IGMP Snooping Querier enabled and IGMP Snooping is operationally disabled on it, IGMP Snooping Querier functionality is disabled on that VLAN. IGMP Snooping functionality is reenabled if IGMP Snooping is operational on the VLAN.

NOTE: The Querier IP Address assigned for a VLAN takes preference over global configuration.

The IGMP Snooping Querier application supports sending periodic general queries on the VLAN to solicit membership reports.

Default disabled

Format `set igmp querier [vlan-id] [address ipv4_address]`

Mode
- Global Config
- VLAN Mode

5.29.0.1.1 no set igmp querier

Use this command to disable IGMP Snooping Querier on the system. Use the optional `address` parameter to reset the querier address to 0.0.0.0.

Format `no set igmp querier [vlan-id] [address]`

Mode
- Global Config
- VLAN Mode

5.29.0.2 set igmp querier query-interval

Use this command to set the IGMP Querier Query Interval time. It is the amount of time in seconds that the switch waits before sending another general query.

Default disabled

Format `set igmp querier query-interval 1-1800`

Mode Global Config

5.29.0.2.1 no set igmp querier query-interval

Use this command to set the IGMP Querier Query Interval time to its default value.

Format `no set igmp querier query-interval`

Mode Global Config

5.29.0.3 set igmp querier timer expiry

Use this command to set the IGMP Querier timer expiration period. It is the time period that the switch remains in Non-Querier mode once it has discovered that there is a Multicast Querier in the network.

Default 60 seconds

Format `set igmp querier timer expiry` *`60-300`*

Mode Global Config

5.29.0.3.1 no set igmp querier timer expiry

Use this command to set the IGMP Querier timer expiration period to its default value.

Format `no set igmp querier timer expiry`

Mode Global Config

5.29.0.4 set igmp querier version

Use this command to set the IGMP version of the query that the snooping switch is going to send periodically.

Default 1

Format `set igmp querier version` *`1-2`*

Mode Global Config

5.29.0.4.1 no set igmp querier version

Use this command to set the IGMP Querier version to its default value.

Format `no set igmp querier version`

Mode Global Config

5.29.0.5 set igmp querier election participate

Use this command to enable the Snooping Querier to participate in the Querier Election process when it discovers the presence of another Querier in the VLAN. When this mode is enabled, if the Snooping Querier finds that the other Querier's source address is better (less) than the Snooping Querier's address, it stops sending periodic queries. If the Snooping Querier wins the election, then it will continue sending periodic queries.

Default disabled

Format `set igmp querier election participate`

Mode VLAN Database

5.29.0.5.1 no set igmp querier election participate

Use this command to set the Snooping Querier not to participate in querier election but go into non-querier mode as soon as it discovers the presence of another querier in the same VLAN.

Format `no set igmp querier election participate`
Mode VLAN Database

5.29.0.6 show igmpsnooping querier

Use this command to display IGMP Snooping Querier information. Configured information is displayed whether or not IGMP Snooping Querier is enabled.

Format `show igmpsnooping querier [{detail | vlan` *`vlanid`*`}]`
Mode Privileged EXEC

When the optional argument *`vlanid`* is not used, the command displays the following information.

Field	Description
Admin Mode	Indicates whether or not IGMP Snooping Querier is active on the switch.
Admin Version	The version of IGMP that will be used while sending out the queries.
Querier Address	The IP Address which will be used in the IPv4 header while sending out IGMP queries. It can be configured using the appropriate command.
Query Interval	The amount of time in seconds that a Snooping Querier waits before sending out the periodic general query.
Querier Timeout	The amount of time to wait in the Non-Querier operational state before moving to a Querier state.

When you specify a value for *vlanid*, the following additional information appears.

Field	Description
VLAN Admin Mode	Indicates whether iGMP Snooping Querier is active on the VLAN.
VLAN Operational State	Indicates whether IGMP Snooping Querier is in “Querier” or “Non-Querier” state. When the switch is in *Querier* state, it will send out periodic general queries. When in *Non-Querier* state, it will wait for moving to Querier state and does not send out any queries.
VLAN Operational Max Response Time	Indicates the time to wait before removing a Leave from a host upon receiving a Leave request. This value is calculated dynamically from the Queries received from the network. If the Snooping Switch is in Querier state, then it is equal to the configured value.
Querier Election Participation	Indicates whether the IGMP Snooping Querier participates in querier election if it discovers the presence of a querier in the VLAN.
Querier VLAN Address	The IP address will be used in the IPv4 header while sending out IGMP queries on this VLAN. It can be configured using the appropriate command.
Operational Version	The version of IPv4 will be used while sending out IGMP queries on this VLAN.
Last Querier Address	Indicates the IP address of the most recent Querier from which a Query was received.
Last Querier Version	Indicates the IGMP version of the most recent Querier from which a Query was received on this VLAN.

When the optional argument `detail` is used, the command shows the global information and the information for all Querier-enabled VLANs.

5.30 MLD Snooping Commands

This section describes commands used for MLD Snooping. In IPv4, Layer 2 switches can use IGMP Snooping to limit the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded only to those interfaces associated with IP multicast addresses. In IPv6, MLD Snooping performs a similar function. With MLD Snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets.

NOTE: This note clarifies the prioritization of MGMD Snooping Configurations. Many of the IGMP/MLD Snooping commands are available both in the Interface and VLAN modes. Operationally the system chooses or prefers the VLAN configured values over the Interface configured values for most configurations when the interface participates in the VLAN.

5.30.0.1 set mld

This command enables MLD Snooping on the system (Global Config Mode) or an Interface (Interface Config Mode). This command also enables MLD Snooping on a particular VLAN and enables MLD Snooping on all interfaces participating in a VLAN.

If an interface has MLD Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (LAG), MLD Snooping functionality is disabled on that interface. MLD Snooping functionality is re-enabled if you disable routing or remove port channel (LAG) membership from an interface that has MLD Snooping enabled.

MLD Snooping supports the following activities:

- Validation of address version, payload length consistencies and discarding of the frame upon error.
- Maintenance of the forwarding table entries based on the MAC address versus the IPv6 address.
- Flooding of unregistered multicast data packets to all ports in the VLAN.

Default disabled

Format `set mld` *`vlanid`*

Mode
- Global Config
- Interface Config
- VLAN Mode

5.30.0.1.1 no set mld

Use this command to disable MLD Snooping on the system.

Format `set mld` *`vlanid`*

Mode
- Global Config
- Interface Config
- VLAN Mode

5.30.0.2 set mld interfacemode

Use this command to enable MLD Snooping on all interfaces. If an interface has MLD Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (LAG), MLD Snooping functionality is disabled on that interface. MLD Snooping functionality is re-enabled if you disable routing or remove port-channel (LAG) membership from an interface that has MLD Snooping enabled.

Default	disabled
Format	`set mld interfacemode`
Mode	Global Config

5.30.0.2.1 no set mld interfacemode

Use this command to disable MLD Snooping on all interfaces.

Format	`no set mld interfacemode`
Mode	Global Config

5.30.0.3 set mld fast-leave

Use this command to enable MLD Snooping fast-leave admin mode on a selected interface or VLAN. Enabling fast-leave allows the switch to immediately remove the Layer 2 LAN interface from its forwarding table entry upon receiving and MLD done message for that multicast group without first sending out MAC-based general queries to the interface.

NOTE: Note the following:

- You should enable fast-leave admin mode only on VLANs where only one host is connected to each Layer 2 LAN port. This prevents the inadvertent dropping of the other hosts that were connected to the same layer 2 LAN port but were still interested in receiving multicast traffic directed to that group.
- Fast-leave processing is supported only with MLD version 1 hosts.

Default	disabled
Format	`set mld fast-leave` *`vlanid`*
Mode	■ Interface Config ■ VLAN Mode

5.30.0.3.1 no set mld fast-leave

Use this command to disable MLD Snooping fast-leave admin mode on a selected interface.

Format	`no set mld fast-leave` *`vlanid`*
Mode	■ Interface Config ■ VLAN Mode

5.30.0.4 set mld groupmembership-interval

Use this command to set the MLD Group Membership Interval time on a VLAN, one interface or all interfaces. The Group Membership Interval time is the amount of time in seconds that a switch waits for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the MLDv2 Maximum Response time value. The range is 2 to 3600 seconds.

Default	260 seconds
Format	`set mld groupmembership-interval` *`vlanid 2-3600`*

Mode
- Interface Config
- Global Config
- VLAN Mode

5.30.0.4.1 no set groupmembership-interval

Use this command to set the MLDv2 Group Membership Interval time to the default value.

Format `no set mld groupmembership-interval`

Mode
- Interface Config
- Global Config
- VLAN Mode

5.30.0.5 set mld maxresponse

Use this command to set the MLD Maximum Response time for the system, on a particular interface or VLAN. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the MLD Query Interval time value. The range is 1 to 65 seconds.

Default 10 seconds

Format `set mld maxresponse` *`1-65`*

Mode
- Global Config
- Interface Config
- VLAN Mode

5.30.0.5.1 no set mld maxresponse

Use this command to set the max response time (on the interface or VLAN) to the default value.

Format `no set mld maxresponse`

Mode
- Global Config
- Interface Config
- VLAN Mode

5.30.0.6 set mld mcrtexpiretime

Use this command to set the Multicast Router Present Expiration time. The time is set for the system, on a particular interface or VLAN. This is the amount of time in seconds that a switch waits for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 0 to 3600 seconds. A value of 0 indicates an infinite timeout, i.e. no expiration.

Default 0

Format `set mld mcrtexpiretime` *`vlanid 0-3600`*

Mode
- Global Config
- Interface Config

5.30.0.6.1 no set mld mcrtexpiretime

Use this command to set the Multicast Router Present Expiration time to 0. The time is set for the system, on a particular interface or a VLAN.

Format `no set mld mcrtexpiretime` *`vlanid`*

Mode
- Global Config
- Interface Config

5.30.0.7 set mld mrouter

Use this command to configure the VLAN ID for the VLAN that has the multicast router attached mode enabled.

Format `set mld mrouter` *`vlanid`*

Mode Interface Config

5.30.0.7.1 no set mld mrouter

Use this command to disable multicast router attached mode for a VLAN with a particular VLAN ID.

Format `no set mld mrouter` *`vlanid`*

Mode Interface Config

5.30.0.8 set mld mrouter interface

Use this command to configure the interface as a multicast router-attached interface. When configured as a multicast router interface, the interface is treated as a multicast router-attached interface in all VLANs.

Default disabled

Format `set mld mrouter interface`

Mode Interface Config

5.30.0.8.1 no set mld mrouter interface

Use this command to disable the status of the interface as a statically configured multicast router-attached interface.

Format `no set mld mrouter interface`

Mode Interface Config

5.30.0.9 show mldsnooping

Use this command to display MLD Snooping information. Configured information is displayed whether or not MLD Snooping is enabled.

Format `show mldsnooping` *`[slot/port | vlanid]`*

Mode Privileged EXEC

When the optional arguments *`slot/port`* or *`vlanid`* are not used, the command displays the following information.

Term	Definition
Admin Mode	Indicates whether or not MLD Snooping is active on the switch.
Interfaces Enabled for MLD Snooping	Interfaces on which MLD Snooping is enabled.
MLD Control Frame Count	Displays the number of MLD Control frames that are processed by the CPU.
VLANs Enabled for MLD Snooping	VLANs on which MLD Snooping is enabled.

When you specify the *slot/port* values, the following information displays.

Term	Definition
MLD Snooping Admin Mode	Indicates whether MLD Snooping is active on the interface.
Fast Leave Mode	Indicates whether MLD Snooping Fast Leave is active on the VLAN.
Group Membership Interval	Shows the amount of time in seconds that a switch will wait for a report from a particular group on a particular interface, which is participating in the VLAN, before deleting the interface from the entry. This value may be configured.
Max Response Time	Displays the amount of time the switch waits after it sends a query on an interface, participating in the VLAN, because it did not receive a report for a particular group on that interface. This value may be configured.
Multicast Router Present Expiration Time	Displays the amount of time to wait before removing an interface that is participating in the VLAN from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.

When you specify a value for *vlanid*, the following information appears.

Term	Definition
VLAN Admin Mode	Indicates whether MLD Snooping is active on the VLAN.

5.30.0.10 show mldsnooping mrouter interface

Use this command to display information about statically configured multicast router attached interfaces.

Format `show mldsnooping mrouter interface` *slot/port*

Mode Privileged EXEC

Term	Definition
Interface	Shows the interface on which multicast router information is being displayed.
Multicast Router Attached	Indicates whether multicast router is statically enabled on the interface.
VLAN ID	Displays the list of VLANs of which the interface is a member.

5.30.0.11 show mldsnooping mrouter vlan

Use this command to display information about statically configured multicast router-attached interfaces.

Format `show mldsnooping mrouter vlan` *slot/port*

Mode Privileged EXEC

Term	Definition
Interface	Shows the interface on which multicast router information is being displayed.
VLAN ID	Displays the list of VLANs of which the interface is a member.

5.30.0.12 show mldsnooping ssm entries

Use this command to display the source specific multicast forwarding database built by MLD snooping.

Format `show mldsnooping ssm entries`

Mode Privileged EXEC

Term	Definition
VLAN	The VLAN on which the entry is learned.
Group	The IPv6 multicast group address.
Source	The IPv6 source address.
Source Filter Mode	The source filter mode (Include/Exclude) for the specified group.
Interfaces	1)If Source Filter Mode is “Include,” specifies the list of interfaces on which a incoming packet is forwarded. If it’s source IP address is equal to the current entry’s Source, the destination IP address is equal to the current entry’s Group and the VLAN ID on which it arrived is current entry’s VLAN. 2) If Source Filter Mode is “Exclude,” specifies the list of interfaces on which a incoming packet is forwarded. If it’s source IP address is *not* equal to the current entry’s Source, the destination IP address is equal to current entry’s Group and VLAN ID on which it arrived is current entry’s VLAN.

5.30.0.13 show mldsnooping ssm stats

Use this command to display the statistics of MLD snooping’s SSMFDB. This command takes no options.

Format `show mldsnooping ssm stats`

Mode Privileged EXEC

Term	Definition
Total Entries	The total number of entries that can possibly be in the MLD snooping’s SSMFDB.
Most SSMFDB Entries Ever Used	The largest number of entries that have been present in the MLD snooping’s SSMFDB.
Current Entries	The current number of entries in the MLD snooping’s SSMFDB.

5.30.0.14 show mldsnooping ssm groups

Use this command to display the MLD SSM group membership information.

Format `show mldsnooping ssm groups`

Mode Privileged EXEC

Term	Definition
VLAN	VLAN on which the MLD v2 report is received.
Group	The IPv6 multicast group address.
Interface	The interface on which the MLD v2 report is received.
Reporter	The IPv6 address of the host that sent the MLDv2 report.
Source Filter Mode	The source filter mode (Include/Exclude) for the specified group.
Source Address List	List of source IP addresses for which source filtering is requested.

5.30.0.15 show mac-address-table mldsnooping

Use this command to display the MLD Snooping entries in the Multicast Forwarding Database (MFDB) table.

Format `show mac-address-table mldsnooping`

Mode Privileged EXEC

Term	Definition
VLAN ID	The VLAN in which the MAC address is learned.
MAC Address	A multicast MAC address for which the switch has forwarding or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Type	The type of entry, which is either static (added by the user) or dynamic (added to the table as a result of a learning process or protocol.)
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

5.30.0.16 clear mldsnooping

Use this command to delete all MLD snooping entries from the MFDB table.

Format `clear mldsnooping`

Mode Privileged EXEC

5.31 MLD Snooping Querier Commands

In an IPv6 environment, MLD Snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the MLD Querier. The MLD query responses, known as MLD reports, keep the switch updated with the current multicast group membership on a port-by-port basis. If the switch does not receive updated membership information in a timely fashion, it will stop forwarding multicasts to the port where the end device is located.

This section describes the commands you use to configure and display information on MLD Snooping queries on the network and, separately, on VLANs.

NOTE: This note clarifies the prioritization of MGMD Snooping Configurations. Many of the IGMP/MLD Snooping commands are available both in the Interface and VLAN modes. Operationally the system chooses or prefers the VLAN configured values over the Interface configured values for most configurations when the interface participates in the VLAN.

5.31.0.1 set mld querier

Use this command to enable MLD Snooping Querier on the system (Global Config Mode) or on a VLAN. Using this command, you can specify the IP address that the snooping querier switch should use as a source address while generating periodic queries.

If a VLAN has MLD Snooping Querier enabled and MLD Snooping is operationally disabled on it, MLD Snooping Querier functionality is disabled on that VLAN. MLD Snooping functionality is re-enabled if MLD Snooping is operational on the VLAN.

The MLD Snooping Querier sends periodic general queries on the VLAN to solicit membership reports.

Default disabled

Format `set mld querier [vlan-id] [address ipv6_address]`

Mode
- Global Config
- VLAN Mode

5.31.0.1.1 no set mld querier

Use this command to disable MLD Snooping Querier on the system. Use the optional parameter `address` to reset the querier address.

Format `no set mld querier [vlan-id][address]`

Mode
- Global Config
- VLAN Mode

5.31.0.2 set mld querier query_interval

Use this command to set the MLD Querier Query Interval time. It is the amount of time in seconds that the switch waits before sending another general query.

Default 60 seconds

Format `set mld querier query_interval 1-1800`

Mode Global Config

5.31.0.2.1 no set mld querier query_interval

Use this command to set the MLD Querier Query Interval time to its default value.

Format `no set mld querier query_interval`
Mode Global Config

5.31.0.3 set mld querier timer expiry

Use this command to set the MLD Querier timer expiration period. It is the time period that the switch remains in Non-Querier mode once it has discovered that there is a Multicast Querier in the network.

Default 60 seconds
Format `set mld querier timer expiry` *`60-300`*
Mode Global Config

5.31.0.3.1 no set mld querier timer expiry

Use this command to set the MLD Querier timer expiration period to its default value.

Format `no set mld querier timer expiry`
Mode Global Config

5.31.0.4 set mld querier election participate

Use this command to enable the Snooping Querier to participate in the Querier Election process when it discovers the presence of another Querier in the VLAN. When this mode is enabled, if the Snooping Querier finds that the other Querier's source address is better (less) than the Snooping Querier's address, it stops sending periodic queries. If the Snooping Querier wins the election, then it will continue sending periodic queries.

Default disabled
Format `set mld querier election participate`
Mode VLAN Database

5.31.0.4.1 no set mld querier election participate

Use this command to set the snooping querier not to participate in querier election but go into a non-querier mode as soon as it discovers the presence of another querier in the same VLAN.

Format `no set mld querier election participate`
Mode VLAN Database

5.31.0.5 show mldsnooping querier

Use this command to display MLD Snooping Querier information. Configured information is displayed whether or not MLD Snooping Querier is enabled.

Format `show mldsnooping querier [{detail | vlan` *`vlanid`*`}]`

Mode Privileged EXEC

When the optional arguments *vlandid* are not used, the command displays the following information.

Field	Description
Admin Mode	Indicates whether or not MLD Snooping Querier is active on the switch.
Admin Version	Indicates the version of MLD that will be used while sending out the queries. This is defaulted to `MLD v1` and it cannot be changed.
Querier Address	Shows the IP address which will be used in the IPv6 header while sending out MLD queries. It can be configured using the appropriate command.
Query Interval	Shows the amount of time in seconds that a Snooping Querier waits before sending out the periodic general query.
Querier Timeout	Displays the amount of time to wait in the Non-Querier operational state before moving to a Querier state.

When you specify a value for *vlanid*, the following information appears.

Field	Description
VLAN Admin Mode	Indicates whether MLD Snooping Querier is active on the VLAN.
VLAN Operational State	Indicates whether MLD Snooping Querier is in "*Querier*" or "*Non-Querier*" state. When the switch is in *Querier* state, it will send out periodic general queries. When in *Non-Querier* state, it will wait for moving to *Querier* state and does not send out any queries.
VLAN Operational Max Response Time	Indicates the time to wait before removing a Leave from a host upon receiving a Leave request. This value is calculated dynamically from the Queries received from the network. If the Snooping Switch is in Querier state, then it is equal to the configured value.
Querier Election Participate	Indicates whether the MLD Snooping Querier participates in querier election if it discovers the presence of a querier in the VLAN.
Querier VLAN Address	The IP address will be used in the IPv6 header while sending out MLD queries on this VLAN. It can be configured using the appropriate command.
Operational Version	This version of IPv6 will be used while sending out MLD queriers on this VLAN.
Last Querier Address	Indicates the IP address of the most recent Querier from which a Query was received.
Last Querier Version	Indicates the MLD version of the most recent Querier from which a Query was received on this VLAN.

When the optional argument `detail` is used, the command shows the global information and the information for all Querier-enabled VLANs.

5.32 Port Security Commands

This section describes the command you use to configure Port Security on the switch. Port security, which is also known as port MAC locking, allows you to secure the network by locking allowable MAC addresses on a given port. Packets with a matching source MAC address are forwarded normally, and all other packets are discarded.

NOTE: To enable the SNMP trap specific to port security, see Section 3.10.0.4, snmp-server enable traps violation.

5.32.0.1 port-security

This command enables port locking on an interface, a range of interfaces, or at the system level.

Default disabled

Format `port-security`

Mode
- Global Config (to enable port locking globally)
- Interface Config (to enable port locking on an interface or range of interfaces)

5.32.0.1.1 no port-security

This command disables port locking for one (Interface Config) or all (Global Config) ports.

Format `no port-security`

Mode
- Global Config
- Interface Config

5.32.0.2 port-security max-dynamic

This command sets the maximum number of dynamically locked MAC addresses allowed on a specific port.

Default 600

Format `port-security max-dynamic` *`maxvalue`*

Mode Interface Config

5.32.0.2.1 no port-security max-dynamic

This command resets the maximum number of dynamically locked MAC addresses allowed on a specific port to its default value.

Format `no port-security max-dynamic`

Mode Interface Config

5.32.0.3 port-security max-static

This command sets the maximum number of statically locked MAC addresses allowed on a port.

Default 1

Format `port-security max-static` *`maxvalue`*

Mode Interface Config

5.32.0.3.1 no port-security max-static

This command sets maximum number of statically locked MAC addresses to the default value.

Format `no port-security max-static`

Mode Interface Config

5.32.0.4 port-security mac-address

This command adds a MAC address to the list of statically locked MAC addresses for an interface or range of interfaces. The `vid` is the VLAN ID.

Format `port-security mac-address` *`mac-address vid`*

Mode Interface Config

5.32.0.4.1 no port-security mac-address

This command removes a MAC address from the list of statically locked MAC addresses.

Format `no port-security mac-address` *`mac-address vid`*

Mode Interface Config

5.32.0.5 port-security mac-address move

This command converts dynamically locked MAC addresses to statically locked addresses for an interface or range of interfaces.

Format `port-security mac-address move`

Mode Interface Config

5.32.0.6 port-security mac-address sticky

This command enables sticky mode Port MAC Locking on a port. If accompanied by a MAC address and a VLAN id (for interface config mode only), it adds a sticky MAC address to the list of statically locked MAC addresses. These sticky addresses are converted back to dynamically locked addresses if sticky mode is disabled on the port. The <vid> is the VLAN ID. The Global command applies the “sticky” mode to all valid interfaces (physical and LAG). There is no global sticky mode as such.

Sticky addresses that are dynamically learned will appear in **show running config** as “port-security mac-address sticky <mac> <vid>” entries. This distinguishes them from static entries.

Format `port-security mac-address sticky [<mac-address> <vid>]`

Mode
- Global Config
- Interface Config

Example: The following shows an example of the command.

```
(Routing)(Config)# port-security mac-address sticky

(Routing)(Interface 0/1)# port-security mac-address sticky
(Routing)(Interface 0/1)# port-security mac-address sticky
  00:00:00:00:00:01 2
```

5.32.0.6.1 no port-security mac-address sticky

The **no** form removes the sticky mode. The sticky MAC address can be deleted by using the command “no port-security mac-address <mac-address> <vid>”.

Format `no port-security mac-address sticky [<mac-address> <vid>]`

Mode
- Global Config
- Interface Config

5.32.0.7 mac-address-table limit

This command enables VLAN port security. VLAN MAC locking allows you to secure the network by locking down allowable MAC addresses on a given VLAN. Packets with a matching source MAC address can be forwarded normally. All other packets will be discarded. VLAN MAC locking will lock the dynamic MAC entries.

If VLAN and port MAC locking are enabled, VLAN MAC locking will be given precedence over port MAC locking.

Default Disabled

Format `mac-address-table limit [action shutdown] [notification trap ] [`*`maximum-num`*`] [vlan `*`vlan-id`*`]`

Mode Global Config

Parameter	Description
[action shutdown]	After the MAC limit has been reached, the action will shut down the ports participating in the VLAN.
[notification trap]	Enables `snmp-server enable traps` violation on the ports participating in the VLAN. After the MAC limit has been reached, log message will be generated with the violation MAC address details.
[*maximum-num*]	MAC limit to be configured.
[vlan *vlan*]	VLAN on which the MAC limit is to be applied. **NOTE:** Packets on all other VLAN will be discarded.

Example: The following shows an example of the command.

```
(Routing) (Config)#mac-address-table limit 3 vlan 10
(Routing) (Config)#mac-address-table limit action shutdown 5 vlan 20
(Routing) (Config)#mac-address-table limit notification trap 4 vlan 30
(Routing) (Config)#mac-address-table limit action shutdown notification trap 6 vlan 100
```

5.32.0.7.1 no mac-address-table limit

This command disables VLAN port security on the specified VLAN.

Default Disabled

Format `no mac-address-table limit [action shutdown] [notification trap ] [`*`maximum-num`*`] [vlan `*`vlan-id`*`]`

Mode Global Config

5.32.0.8 show port-security

This command displays the port-security settings for the port(s). If you do not use a parameter, the command displays the Port Security Administrative mode. Use the optional parameters to display the settings on a specific interface, LAG, or on all interfaces.

Format `show port-security [{`*`slot/port`* `| lag` *`lag-id`* `| all}]`

Mode Privileged EXEC

Parameter	Definition
Admin Mode	Port Locking mode for the entire system. This field displays if you do not supply any parameters.

For each interface, or for the interface you specify, the following information appears:

Parameter	Definition
Admin Mode	Port Locking mode for the Interface.
Dynamic Limit	Maximum dynamically allocated MAC Addresses.
Static Limit	Maximum statically allocated MAC Addresses.
Violation Trap Mode	Whether violation traps are enabled.

Example: The following shows example CLI display output for the command.

```
(Routing) #show port-security 0/1

        Admin    Dynamic     Static     Violation  Sticky
Intf    Mode      Limit      Limit      Trap Mode  Mode
------  -------  ----------  ---------  ---------  --------
0/1     Disabled 1           1          Disabled   Enabled
```

5.32.0.9 show port-security dynamic

This command displays the dynamically locked MAC addresses for the port.

Format `show port-security dynamic {`*`slot/port | lag lag-id}`*

Mode Privileged EXEC

Parameter	Definition
MAC Address	MAC Address of dynamically locked MAC.

5.32.0.10 show port-security static

This command displays the statically locked MAC addresses for port. Instead of `slot/port`, `lag lag-intf-num` can be used as an alternate way to specify the LAG interface. `lag lag-intf-num` can also be used to specify the LAG interface where `lag-intf-num` is the LAG port number.

Format `show port-security static {`*`slot/port | lag lag-id}`*

Mode Privileged EXEC

Term	Definition
Statically Configured MAC Address	The statically configured MAC address.
VLAN ID	The ID of the VLAN that includes the host with the specified MAC address.
Sticky	Indicates whether the static MAC address entry is added in sticky mode.

Example: The following shows example CLI display output for the command.

```
(Routing) #show port-security static 0/1

 Number of static MAC addresses configured: 2

 Statically configured MAC Address    VLAN ID    Sticky
 ---------------------------------    -------    ------
 00:00:00:00:00:01                    2            Yes
 00:00:00:00:00:02                    2            No
```

5.32.0.11 show port-security violation

This command displays the source MAC address of the last packet discarded on a locked port. Instead of `slot/port`, `lag lag-intf-num` can be used as an alternate way to specify the LAG interface. `lag lag-intf-num` can also be used to specify the LAG interface where `lag-intf-num` is the LAG port number.

Format `show port-security violation {slot/port | lag lag-id}`

Mode Privileged EXEC

Term	Definition
MAC Address	The source MAC address of the last frame that was discarded at a locked port.
VLAN ID	The VLAN ID, if applicable, associated with the MAC address of the last frame that was discarded at a locked port.

5.32.0.12 show mac-address-table limit

This command displays the VLAN port security configuration.

Format *show mac-address-table limit [vlan-id]*

Mode Privileged EXEC

Term	Definition
VLAN ID	The VLAN ID on which MAC locking has been configured.

Example:

```
(Routing) #show mac-address-table limit

Vlan MAC Locking Administration Mode:  Enabled

For Vlan 10
Configured mac limit 3
Operational mac limit 3
```

```
Violation trap mode  Enabled
Violation shutdown mode  Disabled

vlan    Interface Mac-Address
------- --------- -----------------
10      0/2       00:00:00:00:44:44
10      0/2       00:00:00:00:44:45
10      0/2       00:00:00:00:44:46

For Vlan 20
Configured mac limit 3
Operational mac limit 3
Violation trap mode  Enabled
Violation shutdown mode  Disabled

vlan    Interface Mac-Address
------- --------- -----------------
20      0/28      00:00:00:00:00:11
20      0/28      00:00:00:00:00:12
20      0/28      00:00:00:00:00:13

(Routing) #show mac-address-table limit 10

Vlan MAC Locking Administration Mode:  Enabled

For Vlan 10
Configured mac limit 3
Operational mac limit 3

vlan    Interface Mac-Address
------- --------- -----------------
10      0/2       00:00:00:00:44:44
10      0/2       00:00:00:00:44:45
10      0/2       00:00:00:00:44:46
```

5.33 LLDP (802.1AB) Commands

This section describes the command you use to configure Link Layer Discovery Protocol (LLDP), which is defined in the IEEE 802.1AB specification. LLDP allows stations on an 802 LAN to advertise major capabilities and physical descriptions. The advertisements allow a network management system (NMS) to access and display this information.

5.33.0.1 lldp transmit

Use this command to enable the LLDP advertise capability on an interface or a range of interfaces.

Default disabled

Format `lldp transmit`

Mode Interface Config

5.33.0.1.1 no lldp transmit

Use this command to return the local data transmission capability to the default.

Format `no lldp transmit`

Mode Interface Config

5.33.0.2 lldp receive

Use this command to enable the LLDP receive capability on an interface or a range of interfaces.

Default disabled

Format `lldp receive`

Mode Interface Config

5.33.0.2.1 no lldp receive

Use this command to return the reception of LLDPDUs to the default value.

Format `no lldp receive`

Mode Interface Config

5.33.0.3 lldp timers

Use this command to set the timing parameters for local data transmission on ports enabled for LLDP. The `interval-seconds` determines the number of seconds to wait between transmitting local data LLDPDUs. The range is 1-32768 seconds. The `hold-value` is the multiplier on the transmit interval that sets the TTL in local data LLDPDUs. The multiplier range is 2-10. The `reinit-seconds` is the delay before reinitialization, and the range is 1-0 seconds.

Default
- interval—30 seconds
- hold—4
- reinit—2 seconds

Format `lldp timers [interval` *`interval-seconds`*`] [hold` *`hold-value`*`] [reinit` *`reinit-seconds`*]

Mode Global Config

5.33.0.3.1 no lldp timers

Use this command to return any or all timing parameters for local data transmission on ports enabled for LLDP to the default values.

Format `no lldp timers [interval] [hold] [reinit]`

Mode Global Config

5.33.0.4 lldp transmit-tlv

Use this command to specify which optional type length values (TLVs) in the 802.1AB basic management set are transmitted in the LLDPDUs from an interface or range of interfaces. Use `sys-name` to transmit the system name TLV. To configure the system name, see Section 3.10.0.1, snmp-server. Use `sys-desc` to transmit the system description TLV. Use `sys-cap` to transmit the system capabilities TLV. Use `port-desc` to transmit the port description TLV.

Default no optional TLVs are included

Format `lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]`

Mode Interface Config

5.33.0.4.1 no lldp transmit-tlv

Use this command to remove an optional TLV from the LLDPDUs. Use the command without parameters to remove all optional TLVs from the LLDPDU.

Format `no lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]`

Mode Interface Config

5.33.0.5 lldp transmit-mgmt

Use this command to include transmission of the local system management address information in the LLDPDUs. This command can be used to configure a single interface or a range of interfaces.

Format `lldp transmit-mgmt`

Mode Interface Config

5.33.0.5.1 no lldp transmit-mgmt

Use this command to include transmission of the local system management address information in the LLDPDUs. Use this command to cancel inclusion of the management information in LLDPDUs.

Format `no lldp transmit-mgmt`

Mode Interface Config

5.33.0.6 lldp notification

Use this command to enable remote data change notifications on an interface or a range of interfaces.

Default disabled

Format `lldp notification`

Mode Interface Config

5.33.0.6.1 no lldp notification

Use this command to disable notifications.

Default disabled
Format `no lldp notification`
Mode Interface Config

5.33.0.7 lldp notification-interval

Use this command to configure how frequently the system sends remote data change notifications. The `interval` parameter is the number of seconds to wait between sending notifications. The valid interval range is 5-3600 seconds.

Default 5
Format `lldp notification-interval` *`interval`*
Mode Global Config

5.33.0.7.1 no lldp notification-interval

Use this command to return the notification interval to the default value.

Format `no lldp notification-interval`
Mode Global Config

5.33.0.8 clear lldp statistics

Use this command to reset all LLDP statistics, including MED-related information.

Format `clear lldp statistics`
Mode Privileged EXEC

5.33.0.9 clear lldp remote-data

Use this command to delete all information from the LLDP remote data table, including MED-related information.

Format `clear lldp remote-data`
Mode Global Config

5.33.0.10 show lldp

Use this command to display a summary of the current LLDP configuration.

Format `show lldp`
Mode Privileged EXEC

Parameter	Definition
Transmit Interval	How frequently the system transmits local data LLDPDUs, in seconds.
Transmit Hold Multiplier	The multiplier on the transmit interval that sets the TTL in local data LLDPDUs.
Re-initialization Delay	The delay before reinitialization, in seconds.
Notification Interval	How frequently the system sends remote data change notifications, in seconds.

5.33.0.11 show lldp interface

Use this command to display a summary of the current LLDP configuration for a specific interface or for all interfaces.

Format `show lldp interface {`*`slot/port`* `| all}`

Mode Privileged EXEC

Parameter	Definition
Interface	The interface in a *`slot/port`* format.
Link	Shows whether the link is up or down.
Transmit	Shows whether the interface transmits LLDPDUs.
Receive	Shows whether the interface receives LLDPDUs.
Notify	Shows whether the interface sends remote data change notifications.
TLVs	Shows whether the interface sends optional TLVs in the LLDPDUs. The TLV codes can be 0 (Port Description), 1 (System Name), 2 (System Description), or 3 (System Capability).
Mgmt	Shows whether the interface transmits system management address information in the LLDPDUs.

5.33.0.12 show lldp statistics

Use this command to display the current LLDP traffic and remote table statistics for a specific interface or for all interfaces.

Format `show lldp statistics {`*`slot/port`* `| all}`

Mode Privileged EXEC

Parameter	Definition
Last Update	The amount of time since the last update to the remote table in days, hours, minutes, and seconds.
Total Inserts	Total number of inserts to the remote data table.
Total Deletes	Total number of deletes from the remote data table.
Total Drops	Total number of times the complete remote data received was not inserted due to insufficient resources.
Total Ageouts	Total number of times a complete remote data entry was deleted because the Time to Live interval expired.

The table contains the following column headings:

Term	Definition
Interface	The interface in *`slot/port`* format.
TX Total	Total number of LLDP packets transmitted on the port.

Term	Definition
RX Total	Total number of LLDP packets received on the port.
Discards	Total number of LLDP frames discarded on the port for any reason.
Errors	The number of invalid LLDP frames received on the port.
Ageouts	Total number of times a complete remote data entry was deleted for the port because the Time to Live interval expired.
TVL Discards	The number of TLVs discarded.
TVL Unknowns	Total number of LLDP TLVs received on the port where the type value is in the reserved range, and not recognized.
TLV MED	The total number of LLDP-MED TLVs received on the interface.
TLV 802.1	The total number of LLDP TLVs received on the interface which are of type 802.1.
TLV 802.3	The total number of LLDP TLVs received on the interface which are of type 802.3.

5.33.0.13 show lldp remote-device

Use this command to display summary information about remote devices that transmit current LLDP data to the system. You can show information about LLDP remote data received on all ports or on a specific port.

Format `show lldp remote-device {`*`slot/port`* `| all}`

Mode Privileged EXEC

Parameter	Definition
Local Interface	The interface that received the LLDPDU from the remote device.
RemID	An internal identifier to the switch to mark each remote device to the system.
Chassis ID	The ID that is sent by a remote device as part of the LLDP message, it is usually a MAC address of the device.
Port ID	The port number that transmitted the LLDPDU.
System Name	The system name of the remote device.

Example: The following shows example CLI display output for the command.

```
(Switching) #show lldp remote-device all

LLDP Remote Device Summary

Local
Interface RemID    Chassis ID            Port ID             System Name
-------  -------   --------------------  ------------------  ------------------
0/1
0/2
0/3
0/4
0/5
0/6
0/7         2      00:FC:E3:90:01:0F     00:FC:E3:90:01:11
0/7         3      00:FC:E3:90:01:0F     00:FC:E3:90:01:12
0/7         4      00:FC:E3:90:01:0F     00:FC:E3:90:01:13
0/7         5      00:FC:E3:90:01:0F     00:FC:E3:90:01:14
0/7         1      00:FC:E3:90:01:0F     00:FC:E3:90:03:11
0/7         6      00:FC:E3:90:01:0F     00:FC:E3:90:04:11
0/8
```

```
0/9
0/10
0/11
0/12
--More-- or (q)uit
```

5.33.0.14 show lldp remote-device detail

Use this command to display detailed information about remote devices that transmit current LLDP data to an interface on the system.

Format `show lldp remote-device detail` *`slot/port`*

Mode Privileged EXEC

Parameter	Definition
Local Interface	The interface that received the LLDPDU from the remote device.
Remote Identifier	An internal identifier to the switch to mark each remote device to the system.
Chassis ID Subtype	The type of identification used in the Chassis ID field.
Chassis ID	The chassis of the remote device.
Port ID Subtype	The type of port on the remote device.
Port ID	The port number that transmitted the LLDPDU.
System Name	The system name of the remote device.
System Description	Describes the remote system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.
Port Description	Describes the port in an alpha-numeric format. The port description is configurable.
System Capabilities Supported	Indicates the primary function(s) of the device.
System Capabilities Enabled	Shows which of the supported system capabilities are enabled.
Management Address	For each interface on the remote device with an LLDP agent, lists the type of address the remote LLDP agent uses and specifies the address used to obtain information related to the device.
Time To Live	The amount of time (in seconds) the remote device's information received in the LLDPDU should be treated as valid information.

Example: The following shows example CLI display output for the command.

```
(Switching) #show lldp remote-device detail 0/7

LLDP Remote Device Detail

Local Interface: 0/7

Remote Identifier: 2
Chassis ID Subtype: MAC Address
Chassis ID: 00:FC:E3:90:01:0F
Port ID Subtype: MAC Address
Port ID: 00:FC:E3:90:01:11
System Name:
System Description:
Port Description:
System Capabilities Supported:
System Capabilities Enabled:
Time to Live: 24 seconds
```

5.33.0.15 show lldp local-device

Use this command to display summary information about the advertised LLDP local data. This command can display summary information or detail for each interface.

Format `show lldp local-device {`*`slot/port`* `| all}`
Mode Privileged EXEC

Parameter	Definition
Interface	The interface in a *slot/port* format.
Port ID	The port ID associated with this interface.
Port Description	The port description associated with the interface.

5.33.0.16 show lldp local-device detail

Use this command to display detailed information about the LLDP data a specific interface transmits.

Format `show lldp local-device detail` *`slot/port`*
Mode Privileged EXEC

Parameter	Definition
Interface	The interface that sends the LLDPDU.
Chassis ID Subtype	The type of identification used in the Chassis ID field.
Chassis ID	The chassis of the local device.
Port ID Subtype	The type of port on the local device.
Port ID	The port number that transmitted the LLDPDU.
System Name	The system name of the local device.
System Description	Describes the local system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.
Port Description	Describes the port in an alpha-numeric format.
System Capabilities Supported	Indicates the primary function(s) of the device.
System Capabilities Enabled	Shows which of the supported system capabilities are enabled.
Management Address	The type of address and the specific address the local LLDP agent uses to send and receive information.

5.34 LLDP-MED Commands

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) (ANSI-TIA-1057) provides an extension to the LLDP standard. Specifically, LLDP-MED provides extensions for network configuration and policy, device location, Power over Ethernet (PoE) management, and inventory management.

5.34.0.1 lldp med

Use this command to enable MED on an interface or a range of interfaces. By enabling MED, you will be effectively enabling the transmit and receive function of LLDP.

Default	disabled
Format	`lldp med`
Mode	Interface Config

5.34.0.1.1 no lldp med

Use this command to disable MED.

Format	`no lldp med`
Mode	Interface Config

5.34.0.2 lldp med confignotification

Use this command to configure an interface or a range of interfaces to send the topology change notification.

Default	disabled
Format	`lldp med confignotification`
Mode	Interface Config

5.34.0.2.1 no lldp med confignotification

Use this command to disable notifications.

Format	`no lldp med confignotification`
Mode	Interface Config

5.34.0.3 lldp med transmit-tlv

Use this command to specify which optional Type Length Values (TLVs) in the LLDP MED set will be transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs) from this interface or a range of interfaces.

Default	By default, the capabilities and network policy TLVs are included.
Format	`lldp med transmit-tlv [capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]`
Mode	Interface Config

Parameter	Definition
capabilities	Transmit the LLDP capabilities TLV.
ex-pd	Transmit the LLDP extended PD TLV.
ex-pse	Transmit the LLDP extended PSE TLV.
inventory	Transmit the LLDP inventory TLV.
location	Transmit the LLDP location TLV.
network-policy	Transmit the LLDP network policy TLV.

5.34.0.3.1 no lldp med transmit-tlv

Use this command to remove a TLV.

Format `no lldp med transmit-tlv [capabilities] [network-policy] [ex-pse] [ex-pd] [location] [inventory]`

Mode Interface Config

5.34.0.4 lldp med all

Use this command to configure LLDP-MED on all the ports.

Format `lldp med all`

Mode Global Config

5.34.0.5 lldp med confignotification all

Use this command to configure all the ports to send the topology change notification.

Format `lldp med confignotification all`

Mode Global Config

5.34.0.6 lldp med faststartrepeatcount

Use this command to set the value of the fast start repeat count. `[count]` is the number of LLDP PDUs that will be transmitted when the product is enabled. The range is 1 to 10.

Default 3

Format `lldp med faststartrepeatcount` *`[count]`*

Mode Global Config

5.34.0.6.1 no lldp med faststartrepeatcount

Use this command to return to the factory default value.

Format `no lldp med faststartrepeatcount`

Mode Global Config

5.34.0.7 lldp med transmit-tlv all

Use this command to specify which optional Type Length Values (TLVs) in the LLDP MED set will be transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs).

Default By default, the capabilities and network policy TLVs are included.

Format `lldp med transmit-tlv all [capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]`

Mode Global Config

Parameter	Definition
capabilities	Transmit the LLDP capabilities TLV.
ex-pd	Transmit the LLDP extended PD TLV.
ex-pse	Transmit the LLDP extended PSE TLV.
inventory	Transmit the LLDP inventory TLV.
location	Transmit the LLDP location TLV.
network-policy	Transmit the LLDP network policy TLV.

5.34.0.7.1 no lldp med transmit-tlv

Use this command to remove a TLV.

Format `no lldp med transmit-tlv [capabilities] [network-policy] [ex-pse] [ex-pd] [location] [inventory]`

Mode Global Config

5.34.0.8 show lldp med

Use this command to display a summary of the current LLDP MED configuration.

Format `show lldp med`

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) #show lldp med
LLDP MED Global Configuration

Fast Start Repeat Count: 3
Device Class: Network Connectivity

(Routing) #
```

5.34.0.9 show lldp med interface

Use this command to display a summary of the current LLDP MED configuration for a specific interface. Slot/Port indicates a specific physical interface. `all` indicates all valid LLDP interfaces.

Format `show lldp med interface {slot/port | all}`

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) #show lldp med interface all

Interface  Link    configMED operMED   ConfigNotify TLVsTx
---------  ------  --------- --------  ------------ -----------
0/1      Down    Disabled  Disabled  Disabled     0,1
0/2      Up      Disabled  Disabled  Disabled     0,1
0/3      Down    Disabled  Disabled  Disabled     0,1
0/4      Down    Disabled  Disabled  Disabled     0,1
0/5      Down    Disabled  Disabled  Disabled     0,1
0/6      Down    Disabled  Disabled  Disabled     0,1
0/7      Down    Disabled  Disabled  Disabled     0,1
0/8      Down    Disabled  Disabled  Disabled     0,1
0/9      Down    Disabled  Disabled  Disabled     0,1
0/10     Down    Disabled  Disabled  Disabled     0,1
0/11     Down    Disabled  Disabled  Disabled     0,1
0/12     Down    Disabled  Disabled  Disabled     0,1
0/13     Down    Disabled  Disabled  Disabled     0,1
0/14     Down    Disabled  Disabled  Disabled     0,1

TLV Codes: 0- Capabilities,       1- Network Policy
           2- Location,           3- Extended PSE
           4- Extended Pd,        5- Inventory
--More-- or (q)uit
(Routing) #show lldp med interface 0/2

Interface  Link    configMED operMED   ConfigNotify TLVsTx
---------  ------  --------- --------  ------------ -----------
0/2       Up      Disabled  Disabled  Disabled     0,1

TLV Codes: 0- Capabilities,       1- Network Policy
           2- Location,           3- Extended PSE
           4- Extended Pd,        5- Inventory

(Routing) #
```

5.34.0.10 show lldp med local-device detail

Use this command to display detailed information about the LLDP MED data that a specific interface transmits. *slot/port* indicates a specific physical interface.

Format `show lldp med local-device detail` *slot/port*

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) #show lldp med local-device detail 0/8
LLDP MED Local Device Detail

Interface: 0/8

Network Policies
Media Policy Application Type : voice
```

```
Vlan ID: 10
Priority: 5
DSCP: 1
Unknown: False
Tagged: True

Media Policy Application Type : streamingvideo
Vlan ID: 20
Priority: 1
DSCP: 2
Unknown: False
Tagged: True

Inventory
Hardware Rev: xxx xxx xxx
Firmware Rev: xxx xxx xxx
Software Rev: xxx xxx xxx
Serial Num: xxx xxx xxx
Mfg Name: xxx xxx xxx
Model Name: xxx xxx xxx
Asset ID: xxx xxx xxx

Location
Subtype: elin
Info: xxx xxx xxx

Extended POE
Device Type: pseDevice

Extended POE PSE
Available: 0.3 Watts
Source: primary
Priority: critical

Extended POE PD

Required: 0.2 Watts
Source: local
Priority: low
```

5.34.0.11 show lldp med remote-device

Use this command to display the summary information about remote devices that transmit current LLDP MED data to the system. You can show information about LLDP MED remote data received on all valid LLDP interfaces or on a specific physical interface.

Format `show lldp med remote-device {`*`slot/port`* `| all}`

Mode Privileged EXEC

Parameter	Definition
Local Interface	The interface that received the LLDPDU from the remote device.
Remote ID	An internal identifier to the switch to mark each remote device to the system.
Device Class	Device classification of the remote device.

Example: The following shows example CLI display output for the command.

```
(Routing) #show lldp med remote-device all

LLDP MED Remote Device Summary

Local
Interface  Remote ID  Device Class
---------  ---------  ------------
0/8          1         Class I
0/9          2         Not Defined
0/10         3         Class II
0/11         4         Class III
0/12         5         Network Con
```

5.34.0.12 show lldp med remote-device detail

Use this command to display detailed information about remote devices that transmit current LLDP MED data to an interface on the system.

Format `show lldp med remote-device detail` *`slot/port`*

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) #show lldp med remote-device detail 0/8

LLDP MED Remote Device Detail

Local Interface: 0/8
Remote Identifier: 18
Capabilities
MED Capabilities Supported: capabilities, networkpolicy, location, extendedpse
MED Capabilities Enabled: capabilities, networkpolicy
Device Class: Endpoint Class I

Network Policies
Media Policy Application Type : voice
Vlan ID: 10
Priority: 5
DSCP: 1
Unknown: False
Tagged: True

Media Policy Application Type : streamingvideo
Vlan ID: 20
Priority: 1
DSCP: 2
Unknown: False
Tagged: True

Inventory
Hardware Rev: xxx xxx xxx
Firmware Rev: xxx xxx xxx
Software Rev: xxx xxx xxx
Serial Num: xxx xxx xxx
Mfg Name: xxx xxx xxx
```

```
Model Name: xxx xxx xxx
Asset ID: xxx xxx xxx

Location
Subtype: elin
Info: xxx xxx xxx

Extended POE
Device Type: pseDevice

Extended POE PSE
Available: 0.3 Watts
Source: primary
Priority: critical

Extended POE PD

Required: 0.2 Watts
Source: local
Priority: low
```

5.35 Denial of Service Commands

NOTE: Denial of Service (Data Plane) is supported on XGS-III and later platforms only.

This section describes the commands you use to configure Denial of Service (DoS) Control. EFOS software provides support for classifying and blocking specific types of Denial of Service attacks. You can configure your system to monitor and block these types of attacks:

- **SIP = DIP:** Source IP address = Destination IP address.
- **First Fragment:**TCP Header size smaller then configured value.
- **TCP Fragment:** Allows the device to drop packets that have a TCP payload where the IP payload length minus the IP header size is less than the minimum allowed TCP header size.
- **TCP Flag:** TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- **L4 Port:** Source TCP/UDP Port = Destination TCP/UDP Port.
- **ICMP:** Limiting the size of ICMP Ping packets.

NOTE: Monitoring and blocking of the types of attacks listed below are only supported on the BCM56538, BCM56840, BCM56843, BCM56845, BCM56846, and BCM5685x platforms.

- **SMAC = DMAC:** Source MAC address = Destination MAC address.
- **TCP Port:** Source TCP Port = Destination TCP Port.
- **UDP Port:** Source UDP Port = Destination UDP Port.
- **TCP Flag & Sequence:** TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- **TCP Offset:** Allows the device to drop packets that have a TCP header Offset set to 1.
- **TCP SYN:** TCP Flag SYN set.
- **TCP SYN & FIN:** TCP Flags SYN and FIN set.
- **TCP FIN & URG & PSH:** TCP Flags FIN and URG and PSH set and TCP Sequence Number = 0.
- **ICMP V6**: Limiting the size of ICMPv6 Ping packets.
- **ICMP Fragment**: Checks for fragmented ICMP packets.

5.35.0.1 dos-control all

This command enables Denial of Service protection checks globally.

Default	disabled
Format	`dos-control all`
Mode	Global Config

5.35.0.1.1 no dos-control all

This command disables Denial of Service prevention checks globally.

Format	`no dos-control all`
Mode	Global Config

5.35.0.2 dos-control sipdip

This command enables Source IP address = Destination IP address (SIP = DIP) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with SIP = DIP, the packets will be dropped if the mode is enabled.

Default disabled

Format `dos-control sipdip`

Mode Global Config

5.35.0.2.1 no dos-control sipdip

This command disables Source IP address = Destination IP address (SIP = DIP) Denial of Service prevention.

Format `no dos-control sipdip`

Mode Global Config

5.35.0.3 dos-control firstfrag

This command enables Minimum TCP Header Size Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having a TCP Header Size smaller then the configured value, the packets will be dropped if the mode is enabled.The default is `disabled`. If you enable dos-control firstfrag, but do not provide a Minimum TCP Header Size, the system sets that value to `20`.

Default disabled (20)

Format `dos-control firstfrag [`*`0-255`*`]`

Mode Global Config

5.35.0.3.1 no dos-control firstfrag

This command sets Minimum TCP Header Size Denial of Service protection to the default value of `disabled`.

Format `no dos-control firstfrag`

Mode Global Config

5.35.0.4 dos-control tcpfrag

This command enables TCP Fragment Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack and packets that have a TCP payload in which the IP payload length minus the IP header size is less than the minimum allowed TCP header size are dropped.

Default disabled

Format `dos-control tcpfrag`

Mode Global Config

5.35.0.4.1 no dos-control tcpfrag

This command disables TCP Fragment Denial of Service protection.

Format `no dos-control tcpfrag`
Mode Global Config

5.35.0.5 dos-control tcpflag

This command enables TCP Flag Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attacks and packets will be dropped, as follows:

- Packets ingress have the TCP Flag SYN set and a source port less than 1024.
- The TCP Control Flags are set to 0 and the TCP Sequence Number is set to 0.
- The TCP Flags FIN, URG, and PSH are set and the TCP Sequence Number is set to 0.
- The TCP Flags SYN and FIN are both set.

Default disabled
Format `dos-control tcpflag`
Mode Global Config

5.35.0.5.1 no dos-control tcpflag

This command sets disables TCP Flag Denial of Service protections.

Format `no dos-control tcpflag`
Mode Global Config

5.35.0.6 dos-control l4port

This command enables L4 Port Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having Source TCP/UDP Port Number equal to Destination TCP/UDP Port Number, the packets will be dropped if the mode is enabled.

NOTE: Some applications mirror source and destination L4 ports.

Default disabled
Format `dos-control l4port`
Mode Global Config

5.35.0.6.1 no dos-control l4port

This command disables L4 Port Denial of Service protections.

Format `no dos-control l4port`
Mode Global Config

5.35.0.7 dos-control icmp

This command enables Maximum ICMP Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMP Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Default	disabled (512)
Format	`dos-control icmp` *`0-1023`*
Mode	Global Config

5.35.0.7.1 no dos-control icmp

This command disables Maximum ICMP Packet Size Denial of Service protections.

Format	`no dos-control icmp`
Mode	Global Config

5.35.0.8 dos-control smacdmac

NOTE: This command is only supported on the BCM56538, BCM56840, BCM56843, BCM56845, BCM56846, and BCM5685x platforms.

This command enables Source MAC address = Destination MAC address (SMAC = DMAC) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with SMAC = DMAC, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control smacdmac`
Mode	Global Config

5.35.0.8.1 no dos-control smacdmac

This command disables Source MAC address = Destination MAC address (SMAC = DMAC) DoS protection.

Format	`no dos-control smacdmac`
Mode	Global Config

5.35.0.9 dos-control tcpport

NOTE: This command is only supported on the BCM56538, BCM56840, BCM56843, BCM56845, BCM56846, and BCM5685x platforms.

This command enables TCP L4 source = destination port number (Source TCP Port = Destination TCP Port) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with Source TCP Port = Destination TCP Port, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpport`
Mode	Global Config

5.35.0.9.1 no dos-control tcpport

This command disables TCP L4 source = destination port number (Source TCP Port = Destination TCP Port) Denial of Service protection.

Format	`no dos-control smacdmac`
Mode	Global Config

5.35.0.10 dos-control udpport

NOTE: This command is only supported on the BCM56538, BCM56840, BCM56843, BCM56845, BCM56846, and BCM5685x platforms.

This command enables UDP L4 source = destination port number (Source UDP Port = Destination UDP Port) DoS protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with Source UDP Port = Destination UDP Port, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control udpport`
Mode	Global Config

5.35.0.10.1 no dos-control udpport

This command disables UDP L4 source = destination port number (Source UDP Port = Destination UDP Port) Denial of Service protection.

Format	`no dos-control udpport`
Mode	Global Config

5.35.0.11 dos-control tcpflagseq

NOTE: This command is only supported on the BCM56538, BCM56840, BCM56843, BCM56845, BCM56846, and BCM5685x platforms.

This command enables TCP Flag and Sequence Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack and packets will be dropped if the TCP Control Flags are set to 0 and the TCP Sequence Number is set to 0

Default	disabled
Format	`dos-control tcpflagseq`
Mode	Global Config

5.35.0.11.1 no dos-control tcpflagseq

This command sets disables TCP Flag and Sequence Denial of Service protection.

Format	`no dos-control tcpflagseq`
Mode	Global Config

5.35.0.12 dos-control tcpoffset

NOTE: This command is only supported on the BCM56538, BCM56840, BCM56843, BCM56845, BCM56846, and BCM5685x platforms.

This command enables TCP Offset Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP Header Offset equal to one (1), the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpoffset`
Mode	Global Config

5.35.0.12.1 no dos-control tcpoffset

This command disabled TCP Offset Denial of Service protection.

Format	`no dos-control tcpoffset`
Mode	Global Config

5.35.0.13 dos-control tcpsyn

NOTE: This command is only supported on the BCM56538, BCM56840, BCM56843, BCM56845, BCM56846, and BCM5685x platforms.

This command enables TCP SYN and L4 source = 0-1023 Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP flag SYN set and an L4 source port from 0 to 1023, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpsyn`
Mode	Global Config

5.35.0.13.1 no dos-control tcpsyn

This command sets disables TCP SYN and L4 source = 0-1023 Denial of Service protection.

Format	`no dos-control tcpsyn`
Mode	Global Config

5.35.0.14 dos-control tcpsynfin

NOTE: This command is only supported on the BCM56538, BCM56840, BCM56843, BCM56845, BCM56846, and BCM5685x platforms.

This command enables TCP SYN and FIN Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP flags SYN and FIN set, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpsynfin`
Mode	Global Config

5.35.0.14.1 no dos-control tcpsynfin

This command sets disables TCP SYN & FIN Denial of Service protection.

Format	`no dos-control tcpsynfin`
Mode	Global Config

5.35.0.15 dos-control tcpfinurgpsh

NOTE: This command is only supported on the BCM56538, BCM56840, BCM56843, BCM56845, BCM56846, and BCM5685x platforms.

This command enables TCP FIN and URG and PSH and SEQ = 0 checking Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP FIN, URG, and PSH all set and TCP Sequence Number set to 0, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpfinurgpsh`
Mode	Global Config

5.35.0.15.1 no dos-control tcpfinurgpsh

This command sets disables TCP FIN and URG and PSH and SEQ = 0 checking Denial of Service protections.

Format	`no dos-control tcpfinurgpsh`
Mode	Global Config

5.35.0.16 dos-control icmpv4

NOTE: This command is only supported on the BCM56538, BCM56840, BCM56843, BCM56845, BCM56846, and BCM5685x platforms.

This command enables Maximum ICMPv4 Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMPv4 Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Default	disabled (512)
Format	`dos-control icmpv4` *`0-16376`*
Mode	Global Config

5.35.0.16.1 no dos-control icmpv4

This command disables Maximum ICMP Packet Size Denial of Service protections.

Format	`no dos-control icmpv4`
Mode	Global Config

5.35.0.17 dos-control icmpv6

NOTE: This command is only supported on the BCM56538, BCM56840, BCM56843, BCM56845, BCM56846, and BCM5685x platforms.

This command enables Maximum ICMPv6 Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMPv6 Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Default	disabled (512)
Format	`dos-control icmpv6 0-16376`
Mode	Global Config

5.35.0.17.1 no dos-control icmpv6

This command disables Maximum ICMP Packet Size Denial of Service protections.

Format	`no dos-control icmpv6`
Mode	Global Config

5.35.0.18 dos-control icmpfrag

NOTE: This command is only supported on the BCM56538, BCM56840, BCM56843, BCM56845, BCM56846, and BCM5685x platforms.

This command enables ICMP Fragment Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having fragmented ICMP packets, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control icmpfrag`
Mode	Global Config

5.35.0.18.1 no dos-control icmpfrag

This command disabled ICMP Fragment Denial of Service protection.

Format	`no dos-control icmpfrag`
Mode	Global Config

5.35.0.19 show dos-control

This command displays Denial of Service configuration information.

Format	`show dos-control`
Mode	Privileged EXEC

NOTE: Some of the information below displays only if you are using the BCM56538, BCM56840, BCM56843, BCM56845, BCM56846, and BCM5685x platforms.

Parameter	Definition
First Fragment Mode	May be enabled or disabled. The factory default is disabled.
Min TCP Hdr Size <0-255>	The factory default is 20.
ICMP Mode	May be enabled or disabled. The factory default is disabled.
Max ICMPv4 Pkt Size	The range is 0-16376. The factory default is 512.
Max ICMPv6 Pkt Size	The range is 0-16376. The factory default is 512.
ICMP Fragment Mode	May be enabled or disabled. The factory default is disabled.
L4 Port Mode	May be enabled or disabled. The factory default is disabled.
TCP Port Mode	May be enabled or disabled. The factory default is disabled.
UDP Port Mode	May be enabled or disabled. The factory default is disabled.
SIPDIP Mode	May be enabled or disabled. The factory default is disabled.
SMACDMAC Mode	May be enabled or disabled. The factory default is disabled.
TCP Flag Mode	May be enabled or disabled. The factory default is disabled.
TCP FIN&URG& PSH Mode	May be enabled or disabled. The factory default is disabled.
TCP Flag & Sequence Mode	May be enabled or disabled. The factory default is disabled.
TCP SYN Mode	May be enabled or disabled. The factory default is disabled.
TCP SYN & FIN Mode	May be enabled or disabled. The factory default is disabled.
TCP Fragment Mode	May be enabled or disabled. The factory default is disabled.
TCP Offset Mode	May be enabled or disabled. The factory default is disabled.

5.36 MAC Database Commands

This section describes the commands you use to configure and view information about the MAC databases.

5.36.0.1 bridge aging-time

This command configures the forwarding database address aging timeout in seconds. The `seconds` parameter must be within the range of 10 to 1,000,000 seconds.

Default 300
Format `bridge aging-time` *`10-1,000,000`*
Mode Global Config

5.36.0.1.1 no bridge aging-time

This command sets the forwarding database address aging timeout to the default value.

Format `no bridge aging-time`
Mode Global Config

5.36.0.2 show forwardingdb agetime

This command displays the timeout for address aging.

Default all
Format `show forwardingdb agetime`
Mode Privileged EXEC

Term	Definition
Address Aging Timeout	Displays the system's address aging timeout value in seconds.

5.36.0.3 show mac-address-table multicast

This command displays the Multicast Forwarding Database (MFDB) information. If you enter the command with no parameter, the entire table is displayed. You can display the table entry for one MAC Address by specifying the MAC address as an optional parameter.

Format `show mac-address-table multicast` *`macaddr`*
Mode Privileged EXEC

Term	Definition
VLAN ID	The VLAN in which the MAC address is learned.
MAC Address	A multicast MAC address for which the switch has forwarding or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.

Term	Definition
Source	The component that is responsible for this entry in the Multicast Forwarding Database. The source can be IGMP Snooping, GMRP, and Static Filtering.
Type	The type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).
Fwd Interface	The resultant forwarding list is derived from combining all the component's forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.

Example: If one or more entries exist in the multicast forwarding table, the command output looks similar to the following:

```
(Routing) #show mac-address-table multicast

                                                                    Fwd
VLAN ID MAC Address       Source  Type    Description     Interface Interface
------- ----------------- ------- ------- --------------- --------- ---------
1       01:00:5E:01:02:03 Filter  Static  Mgmt Config     Fwd:      Fwd:
                                                          1/0/1,    1/0/1,
                                                          1/0/2,    1/0/2,
                                                          1/0/3,    1/0/3,
                                                          1/0/4,    1/0/4,
                                                          1/0/5,    1/0/5,
                                                          1/0/6,    1/0/6,
                                                          1/0/7,    1/0/7,
                                                          1/0/8,    1/0/8,
                                                          1/0/9,    1/0/9,
                                                          1/0/10,   1/0/10,
--More-- or (q)uit
```

5.36.0.4 show mac-address-table stats

This command displays the Multicast Forwarding Database (MFDB) statistics.

Format `show mac-address-table stats`

Mode Privileged EXEC

Parameter	Definition
Total Entries	The total number of entries that can possibly be in the Multicast Forwarding Database table.
Most MFDB Entries Ever Used	The largest number of entries that have been present in the Multicast Forwarding Database table. This value is also known as the MFDB high-water mark.
Current Entries	The current number of entries in the MFDB.

5.37 ISDP Commands

This section describes the commands you use to configure the industry standard Discovery Protocol (ISDP).

5.37.0.1 isdp run

This command enables ISDP on the switch.

Default Enabled

Format `isdp run`

Mode Global Config

5.37.0.1.1 no isdp run

This command disables ISDP on the switch.

Format `no isdp run`

Mode Global Config

5.37.0.2 isdp holdtime

This command configures the hold time for ISDP packets that the switch transmits. The hold time specifies how long a receiving device should store information sent in the ISDP packet before discarding it. The range is given in seconds.

Default 180 seconds

Format `isdp holdtime` *`10-255`*

Mode Global Config

5.37.0.3 isdp timer

This command sets the period of time between sending new ISDP packets. The range is given in seconds.

Default 30 seconds

Format `isdp timer` *`5-254`*

Mode Global Config

5.37.0.4 isdp advertise-v2

This command enables the sending of ISDP version 2 packets from the device.

Default Enabled

Format `isdp advertise-v2`

Mode Global Config

5.37.0.4.1 no isdp advertise-v2

This command disables the sending of ISDP version 2 packets from the device.

Format `no isdp advertise-v2`

Mode Global Config

5.37.0.5 isdp enable

This command enables ISDP on an interface or range of interfaces.

NOTE: ISDP must be enabled both globally and on the interface in order for the interface to transmit ISDP packets. If ISDP is globally disabled on the switch, the interface will not transmit ISDP packets, regardless of the ISDP status on the interface. To enable ISDP globally, use the command Section 5.37.0.1, isdp run.

Default Enabled
Format `isdp enable`
Mode Interface Config

5.37.0.5.1 no isdp enable

This command disables ISDP on the interface.
Format `no isdp enable`
Mode Interface Config

5.37.0.6 clear isdp counters

This command clears ISDP counters.
Format `clear isdp counters`
Mode Privileged EXEC

5.37.0.7 clear isdp table

This command clears entries in the ISDP table.
Format `clear isdp table`
Mode Privileged EXEC

5.37.0.8 show isdp

This command displays global ISDP settings.

Format `show isdp`
Mode Privileged EXEC

Parameter	Definition
Timer	The frequency with which this device sends ISDP packets. This value is given in seconds.
Hold Time	The length of time the receiving device should save information sent by this device. This value is given in seconds.
ISDPv2 Advertisements	The setting for sending ISDPv2 packets. If disabled, version 1 packets are transmitted.
Device ID	The Device ID advertised by this device. The format of this Device ID is characterized by the value of the Device ID Format object.

Parameter	Definition
Device ID Format Capability	Indicates the Device ID format capability of the device. ■ `serialNumber` indicates that the device uses a serial number as the format for its Device ID. ■ `macAddress` indicates that the device uses a Layer 2 MAC address as the format for its Device ID. ■ `other` indicates that the device uses its platform-specific format as the format for its Device ID.
Device ID Format	Indicates the Device ID format of the device. ■ `serialNumber` indicates that the value is in the form of an ASCII string containing the device serial number. ■ `macAddress` indicates that the value is in the form of a Layer 2 MAC address. ■ `other` indicates that the value is in the form of a platform specific ASCII string containing info that identifies the device. For example, ASCII string contains serialNumber appended/prepended with system name.

5.37.0.9 show isdp interface

This command displays ISDP settings for the specified interface.

Format `show isdp interface {all | slot/port}`

Mode Privileged EXEC

Parameter	Definition
Mode	ISDP mode enabled/disabled status for the interface(s).

5.37.0.10 show isdp entry

This command displays ISDP entries. If the device id is specified, then only entries for that device are shown.

Format `show isdp entry {all | deviceid}`

Mode Privileged EXEC

Parameter	Definition
Device ID	The device ID associated with the neighbor which advertised the information.
IP Addresses	The IP address(es) associated with the neighbor.
Platform	The hardware platform advertised by the neighbor.
Interface	The interface (slot/port) on which the neighbor's advertisement was received.
Port ID	The port ID of the interface from which the neighbor sent the advertisement.
Hold Time	The hold time advertised by the neighbor.
Version	The software version that the neighbor is running.
Advertisement Version	The version of the advertisement packet received from the neighbor.
Capability	ISDP Functional Capabilities advertised by the neighbor.

5.37.0.11 show isdp neighbors

This command displays the list of neighboring devices.

Format `show isdp neighbors [{slot/port | detail}]`

Mode Privileged EXEC

Parameter	Definition
Device ID	The device ID associated with the neighbor which advertised the information.
IP Address(es)	The IP addresses associated with the neighbor.
Capability	ISDP functional capabilities advertised by the neighbor.
Platform	The hardware platform advertised by the neighbor.
Interface	The interface (*slot/port*) on which the neighbor's advertisement was received.
Port ID	The port ID of the interface from which the neighbor sent the advertisement.
Hold Time	The hold time advertised by the neighbor.
Advertisement Version	The version of the advertisement packet received from the neighbor.
Time when last changed	Displays when the entry was last modified.
Version	The software version that the neighbor is running.

Example: The following shows example CLI display output for the command.

```
(Switching) #show isdp neighbors detail

(Routing) #show isdp  neighbors detail

Device ID                       none
Address(es):
Capability                      Router
Platform                        BCM-56846
Interface                       0/33
Port ID                         0/37
Holdtime                        180
Advertisement Version           2
Time when last changed          2 days 05:47:33
Version :
1.2.0.3
```

5.37.0.12 show isdp traffic

This command displays ISDP statistics.

Format show isdp traffic

Mode Privileged EXEC

Parameter	Definition
ISDP Packets Received	Total number of ISDP packets received
ISDP Packets Transmitted	Total number of ISDP packets transmitted
ISDPv1 Packets Received	Total number of ISDPv1 packets received
ISDPv1 Packets Transmitted	Total number of ISDPv1 packets transmitted
ISDPv2 Packets Received	Total number of ISDPv2 packets received
ISDPv2 Packets Transmitted	Total number of ISDPv2 packets transmitted
ISDP Bad Header	Number of packets received with a bad header
ISDP Checksum Error	Number of packets received with a checksum error
ISDP Transmission Failure	Number of packets which failed to transmit

Parameter	Definition
ISDP Invalid Format	Number of invalid packets received
ISDP Table Full	Number of times a neighbor entry was not added to the table due to a full database
ISDP IP Address Table Full	Displays the number of times a neighbor entry was added to the table without an IP address.

5.38 Unidirectional Link Detection Commands

The Unidirectional Link Detection (UDLD) feature detects unidirectional links' physical ports. UDLD must be enabled on both sides of the link in order to detect a unidirectional link. The UDLD protocol operates by exchanging packets containing information about neighboring devices.

The purpose of the UDLD feature is to detect and avoid unidirectional links. A unidirectional link is a forwarding anomaly in a Layer 2 communication channel in which a bi-directional link stops passing traffic in one direction.

5.38.0.1 udld enable (Global Config)

Use the `udld enable` command in Global Config mode to enable UDLD globally on the switch.

Default disable
Format `udld enable`
Mode Global Config

5.38.0.1.1 no udld enable (Global Config)

Use the `no udld enable` command in Global Config mode to disable UDLD globally on the switch.

Format `no udld enable`
Mode Global Config

5.38.0.2 udld message time

Use the `udld message time` command in Global Config mode to configure the interval between UDLD probe messages on ports that are in the advertisement phase. The *interval* range is from 1 to 90 seconds.

Default 15
Format `udld message time interval`
Mode Global Config

5.38.0.3 udld timeout interval

Use the `udld timeout interval` command in Global Config mode to configure the time interval after which the UDLD link is considered to be unidirectional. The *interval* range is from 3 to 60 seconds.

Default 5
Format `udld timeout interval interval`
Mode Global Config

5.38.0.4 udld enable (Interface Config)

Use the `udld enable` command in Interface Config mode to enable UDLD on the specified interface.

Default disable
Format `udld enable`

Mode Interface Config

5.38.0.4.1 no udld enable (Interface Config)

Use the `no udld enable` command in Interface Config mode to disable UDLD on the specified interface.

Format `no udld enable`
Mode Interface Config

5.38.0.5 udld port

Use the `udld port` command in Interface Config mode to select the UDLD mode operating on this interface. If the keyword `aggressive` is not entered, the port operates in normal mode.

Default normal
Format `udld port [aggressive]`
Mode Interface Config

5.38.0.6 udld reset

Use the `udld reset` command in Privileged EXEC mode to reset all interfaces that have been shutdown by UDLD.

Format `udld reset`
Mode Privileged EXEC

5.38.0.7 show udld

Use the `show udld` command in Privileged EXEC or User EXEC modes to display the global settings of UDLD.

Format `show udld`
Mode
- Privileged EXEC
- User EXEC

Parameter	Description
Admin Mode	The global administrative mode of UDLD.
Message Interval	The time period (in seconds) between the transmission of UDLD probe packets.
Timeout Interval	The time period (in seconds) before making the decision that the link is unidirectional.

Example: The following shows example CLI display output for the command.

```
(Routing) #show udld

Admin Mode.....................Enabled
Message Interval.................15 seconds
Timeout Interval.................5 seconds
```

5.38.0.8 show udld slot/port

Use the `show udld slot/port` command in Privileged EXEC or User EXEC modes to display the UDLD settings for the specified *`slot/port`*.

Format `show udld {`*`slot/port`* `| all}`

Mode
- Privileged EXEC
- User EXEC

Parameter	Description
Port	The identifying port of the interface.
Admin Mode	The administrative mode of UDLD configured on this interface. The mode is either `Enabled` or `Disabled`.
UDLD Mode	The UDLD mode configured on this interface. The mode is either `Normal` or `Aggressive`.
UDLD Status	The status of the link as determined by UDLD. The options are: ■ Undetermined – UDLD has not collected enough information to determine the state of the link ■ Not applicable – UDLD is disabled, either globally or on the port. ■ Shutdown – UDLD has detected a unidirectional link and shutdown the port. That is, the port is in an errDisabled state. ■ Bidirectional – UDLD has detected a bidirectional link. ■ Undetermined (Link Down) – The port would transition into this state when the port link physically goes down due to any reasons other than the port has been put into D-Disable mode by the UDLD protocol on the switch.

Example: The following shows example CLI display output for the command.

```
(Routing) #show udld 0/2
Port   Admin     UDLD      UDLD
Port   Mode      Mode      Status
----   --------- ----      ------
0/2    Enabled   AggressiveBidirectional
```

5.39 Interface Error Disable and Auto Recovery

Interface error disable automatically disables an interface when an error is detected; no traffic is allowed until the interface is either manually re-enabled or, if auto recovery is configured, the configured auto recovery time interval has passed.

For interface error disable and auto recovery, an error condition is detected for an interface, the interface is placed in a diagnostic disabled state by shutting down the interface. The error disabled interface does not allow any traffic until the interface is re-enabled. The error disabled interface can be manually enabled. Alternatively administrator can enable auto recovery feature. EFOS Auto Recovery re-enables the interface after the expiry of configured time interval.

5.39.0.1 errdisable recovery cause

Use this command to enable auto recovery for a specified cause or all causes. When auto recovery is enabled, ports in the diag-disable state are recovered (link up) when the recovery interval expires. If the interface continues to experience errors, the interface may be placed back in the diag-disable state and disabled (link down). Interfaces in the diag-disable state can be manually recovered by entering the `no shutdown` command for the interface.

Default None

Format `errdisable recovery cause {all | arp-inspection | bpduguard | dhcp-rate-limit | sfp-mismatch | udld | ucast-storm | bcast-storm | mcast-storm | bpdustorm | keep-alive | mac-locking | denial-of-service | link-flap}`

Mode Global Config

5.39.0.1.1 no errdisable recovery cause

Use this command to disable auto recovery for a specific cause. When disabled, auto recovery will not occur for interfaces in a diag-disable state due to that cause.

Format `no errdisable recovery cause {all | arp-inspection | bpduguard | dhcp-rate-limit | sfp-mismatch | udld | ucast-storm | bcast-storm | mcast-storm | bpdustorm | keep-alive mac-locking | denial-of-service}`

Mode Global Config

5.39.0.2 errdisable recovery interval

Use this command to configure the auto recovery time interval. The auto recovery time interval is common for all causes. The time can be any value from 30 to 86400 seconds.When the recovery interval expires, the system attempts to bring interfaces in the diag-disable state back into service (link up).

Default 300

Format `errdisable recovery interval` *`30-86400`*

Mode Global Config

5.39.0.2.1 no errdisable recovery interval

Use this command to reset the auto recovery interval to the factory default value of 300.

Format `no errdisable recovery interval`

Mode Global Config

5.39.0.3 show errdisable recovery

Use this command to display the error-disabled auto-recovery configuration status of all configurable causes.

Format `show errdisable recovery`
Mode Privileged EXEC

The following information is displayed.

Parameter	Description
arp-inspection	Enable/Disable status of arp-inspection auto recovery.
bpdguard	Enable/Disable status of bpduguard auto recovery.
dhcp-rate-limit	Enable/Disable status of dhcp-rate-limit auto recovery.
sfp-mismatch	Enable/Disable status of sfp-mismatch auto recovery.
udld	Enable/Disable status of UDLD auto recovery.
bpdustorm	Enable/Disable status of bpdustorm auto recovery.
keepalive	Enable/Disable status of keepalive auto recovery.
mac-locking	Enable/Disable status of MAC locking auto recovery.
denial-of-service	Enable/Disable status of DoS auto recovery.
link-flap	Enable/Disable status of link-flap auto recovery.
time interval	Time interval for auto recovery in seconds.

Example:

```
(Routing) #show errdisable recovery

Errdisable Reason      Auto-recovery Status
------------------     --------------------
dhcp-rate-limit           Disabled
arp-inspection            Disabled
udld                      Disabled
bpduguard                 Disabled
bpdustorm                 Disabled
sfp-mismatch              Disabled
keepalive                 Disabled
mac-locking               Disable
denial-of-service         Disabled
link-flap                 Disabled

Timeout for Auto-recovery from D-Disable state  300
```

5.39.0.4 show interfaces status err-disabled

Use this command to display the interfaces that are error disabled.

Format `show interfaces status err-disabled`
Mode Privileged EXEC

The following information is displayed.

Parameter	Description
interface	An interface that is error disabled.
Errdisable Reason	The cause of the interface being error disabled.
Auto-Recovery Time Left	The amount of time left before auto recovery begins.

Example:

```
(Routing) #show interfaces status err-disabled

Interface      Errdisable Reason    Auto-Recovery Time Left(sec)
----------        -----------------           ------------------
0/1             udld                             279
0/2             bpduguard                285
0/3             bpdustorm                291
```

Chapter 6: Data Center Commands

This chapter describes the commands to configure the data center features available in the EFOS CLI.

6.1 Data Center Bridging Exchange Protocol Commands

The Data Center Bridging Exchange Protocol (DCBX) is used by DCB devices to exchange configuration information with directly-connected peers. The protocol is also used to detect misconfiguration of the peer DCB devices and, optionally, for configuration of peer DCB devices.

6.1.0.1 lldp dcbx version

Use the **lldp dcbx version** command in Global Configuration mode to configure the administrative version for the Data Center Bridging Capability Exchange (DCBX) protocol. This command enables the switch to support a specific version of the DCBX protocol or to detect the peer version and match it. DCBX can be configured to operate in IEEE mode or CEE mode or CIN. In auto mode, version detection is based on the peer device DCBX version. The switch operates in either IEEE or one of the legacy modes on each interface.

In **auto** mode, the switch will attempt to jump start the exchange by sending an IEEE frame, followed by a CEE frame followed by a CIN frame. The switch will parse the received response and immediately switch to the peer version.

NOTE: CIN is Cisco Intel Nuova DCBX (version 1.0). CEE is converged enhanced ethernet DCBX (version 1.06).

Default auto
Format `lldp dcbx version { auto | cin | cee | ieee }`
Mode Global Config

Parameter	Description
auto	Automatically select the version based on the peer response.
cin	Force the mode to Cisco-Intel-Nuova. (DCBX 1.0)
cee	Force the mode to CEE (DCBX 1.06)
ieee	Force the mode to IEEE 802.1Qaz

Example: The following example configures the switch to use CEE DCBX.

```
(Routing)(config)#lldp dcbx version cee
```

6.1.0.1.1 no lldp dcbx version

Use the **no** form of the command to reset the DCBX version to the default value of **auto**.

Format `no lldp dcbx version`
Mode Global Config

6.1.0.2 lldp tlv-select dcbxp

Use the **lldp tlv-select dcbxp** command in Interface Configuration or Global Configuration mode to send specific DCBX TLVs if LLDP is enabled to transmit on the given interface. If no parameter is given, all DCBX TLVs are enabled for transmission. The default is all DCBX TLVs are enabled for transmission. If executed in Interface mode, the interface configuration overrides the global configuration on the designated interface. Entering the command with no parameters enables transmission of all TLVs.

Default Transmission of all TLVs is enabled by default.

Format *lldp tlv-select dcbxp [ets-config | ets-recommend | pfc | application-priority]*

Mode
- Interface Config
- Global Config

Parameter	Description
ets-config	Transmit the ETS configuration TLV.
ets-recommend	Transmit the ETS recommendation TLV.
pfc	Transmit the PFC configuration TLV.
application-priority	Transmit the application priority TLV.

6.1.0.2.1 no lldp tlv-select dcbxp

Use the **no lldp tlv-select dcbxp** command to disable LLDP from sending all or individual DCBX TLVs, even if LLDP is enabled for transmission on the given interface.

Format *no lldp tlv-select dcbxp [ets-config | ets-recommend | pfc | application-priority]*

Mode
- Interface Config
- Global Config

Example: The following example configures the port to transmit all TLVs.

```
(Routing) (Config)#no lldp tlv-select dcbxp
```

6.1.0.3 lldp dcbx port-role

Use the **lldp dcbx port-role** command in Interface Configuration mode to configure the port role to manual, auto-upstream, auto-downstream and configuration source. In order to reduce configuration flapping, ports that obtain configuration information from a configuration source port will maintain that configuration for 2x the LLDP timeout, even if the configuration source port becomes operationally disabled.

Default The default port role is manual.

Format *lldp dcbx port-role {auto-up |auto-down|manual |configuration-source}*

Mode Interface Config

Parameter	Description
Manual	Ports operating in the **Manual** role do not have their configuration affected by peer devices or by internal propagation of configuration. These ports will advertise their configuration to their peer if DCBX is enabled on that port. The willing bit is set to disabled on manual role ports.

Parameter	Description
Auto-up	Advertises a configuration, but is also willing to accept a configuration from the link-partner and propagate it internally to the auto-downstream ports as well as receive configuration propagated internally by other auto-upstream ports. These ports have the willing bit enabled. These ports should be connected to FCFs.
Auto-down	Advertises a configuration but is not willing to accept one from the link partner. However, the port will accept a configuration propagated internally by the configuration source. These ports have the willing bit set to disabled. Selection of a port based upon compatibility of the received configuration is suppressed. These ports should be connected to a trusted FCF.
Configuration Source	In this role, the port has been manually selected to be the configuration source. Configuration received over this port is propagated to the other auto-configuration ports. Selection of a port based upon compatibility of the received configuration is suppressed. These ports should be connected to a trusted FCF. These ports have the willing bit enabled.

Example: The following example configures an FCF facing port.

```
(Routing) (Interface 0/1)#lldp dcbx port-role auto-up
```

Example: The following example configures an FCoE host facing port:

```
(Routing) (Interface 0/1)#lldp dcbx port-role auto-down
```

6.1.0.3.1 no lldp dcbx port-role

Use the **no lldp dcbx port-role** command in Interface Configuration mode to configure the port role to manual.

6.1.0.4 show lldp tlv-select

Use the **show lldp tlv-select** command in Privileged EXEC mode to display the per interface TLV configuration.

Format `show lldp tlv-select {interface all | slot/port }`

Mode Privileged EXEC

Parameter	Description
all	All interfaces.
slot/port	A valid physical interface specifier.

Example: The following command shows the TLVs selected for transmission on multiple interfaces.

```
(Routing) # show lldp tlv-select interface all
Interface    ETS Config  ETS Recommend  PFC  App Priority QCN
-------------- ----------  -------------  ---  ------------ ---
0/1              Yes         No       Yes  No           Yes
0/2              No          No          Yes  No           Yes     4.1.3.2
```

6.1.0.5 show lldp dcbx interface

Use the **show lldp dcbx interface** command in Privileged EXEC mode to display the local DCBX control status of an interface.

Format `show lldp dcbx interface all | slot/port <detail | status>`

Mode Privileged EXEC

Parameter	Description
slot/port	A valid physical interface specifier.
all	All interfaces.
Detail	Display detailed DCBX information.
Status	Displays a status summary.

Example: The following shows DCBX status.

```
(Routing) #show lldp dcbx interface all

Is configuration source selected..... False

                                              DCBX   DCBX  DCBX    unknown
Interface  Status     Role          Version   Tx     Rx    Errors  TLV
---------- ---------- ------------- --------- ------- ----- ------- -------
0/1        Disabled   Manual        Auto      0       0     0       0
0/2        Disabled   Manual        Auto      0       0     0       0
0/3        Disabled   Manual        Auto      0       0     0       0
0/4        Disabled   Manual        Auto      0       0     0       0
0/5        Disabled   Manual        Auto      0       0     0       0
0/6        Disabled   Manual        Auto      0       0     0       0
0/7        Disabled   Manual        Auto      0       0     0       0
0/8        Disabled   Manual        Auto      0       0     0       0
```

Example: In the following example, DCBX is not enabled.

```
(Routing) #show lldp dcbx interface 0/1

DCBX operational status:..................... Disabled (Reason: LLDP Tx/Rx is
disabled.)
Configured DCBX version:..................... Auto
Peer DCBX version:...........................
Peer MAC:....................................
Peer Description:............................
Auto-configuration Port Role:................ Manual
Peer Is configuration Source:................ False

Error counters:
ETS incompatible configuration............... 0
PFC incompatible configuration............... 0
Disappearing neighbor........................ 0
Multiple neighbors detected.................. 0
```

Example: The following example displays details.

```
(Routing) #show lldp dcbx interface 0/1 detail

DCBX operational status:..................... Disabled (Reason: LLDP Tx/Rx is
disabled.)
Configured DCBX version:..................... Auto
Peer DCBX version:...........................
Peer MAC:....................................
Peer Description:............................
Auto-configuration Port Role:................ Manual
Peer Is configuration Source:................ False

Error counters:
```

```
ETS incompatible configuration.................. 0
PFC incompatible configuration.................. 0
Disappearing neighbor........................... 0
Multiple neighbors detected..................... 0

Local configuration:


PFC configuration (Tx enabled)
Willing: False  MBC:  False   Max PFC classes supported:  8
PFC enable vector:    0:0   1:0   2:0   3:0   4:0   5:0   6:0   7:0

ETS configuration (Tx enabled)
```

6.2 Quantized Congestion Notification Commands

The Quantized Congestion Notification (QCN) feature is part of the Data Center Package.

6.2.0.1 qcn enable

Use the `qcn enable` command in Global Configuration mode to enable QCN on all the ports of the system. This command is master enable control. When QCN is enabled, the system recognizes the CN-TAG in received frames, the Congestion algorithm runs on the configured Congestion Points (CP) and Congestion Notification Messages (CNMs) are transmitted if congestion is detected on a CP.

Default disabled
Format `qcn enable`
Mode Global Config

6.2.0.1.1 no qcn enable

Use the `no qcn enable` command in Global Configuration mode to disable QCN on all the ports of the system. This command is the master disable command. When QCN is disabled, received frames with CN-TAGs are treated as normal data frames and CNMs are never generated.

Format `no qcn enable`
Mode Global Config

6.2.0.2 qcn cnm-transmit-priority

Use the `qcn cnm-transmit-priority` command in Global Configuration mode to globally configure the dot1p priority of congestion notification messages (CNM) that are transmitted by the system. This command configures the dot1p priority value with which the CNM are transmitted. By default, CNMs are transmitted with dot1p priority as zero.

Default The value is set to 0.
Format `qcn cnm-transmit-priority dot1p priority`
Mode Global Config

Parameter	Description
dot1p priority	The range is 0–7.

6.2.0.2.1 no qcn cnm-transmit-priority

Use the `no qcn cnm-transmit-priority` command in Global Configuration mode to set to the default value the dot1p priority on CNMs that are transmitted by the system.

Format `no qcn cnm-transmit-priority`
Mode Global Config

6.2.0.3 qcn cnpv-priority (datacenter bridging config)

Use the `qcn cnpv-priority` command in Data Center Bridging Configuration mode to globally configure a CP (port-queue) that is mapped to the specified dot1p priority as congestion enabled (**interior**) or congestion disabled (**disable**) or edge congestion point (**edge**) for all ports which have the defense mode configured as **component**.

Default All priorities are disabled for QCN.

Format `qcn cnpv-priority priority {interior | edge | disable}`

Mode Data Center Bridging Config

Parameter	Description
cnpv-priority	The range is 1–7.
The possible selections for a Congestion Point (CP) are:	
Interior congestion point (ICP)	Used when a flow with the specified dot1p priority needs to be congestion aware. This setting enables detection of congestion of the selected priority.
Edge congestion point (ECP)	Used when the congestion point (CP) is on the edge of the congestion notification domain (CND).
Disabled for QCN	Used when it is desired that the priority be congestion unaware. This setting disables detection of congestion on the priority.

6.2.0.4 qcn cnpv-priority alternate-priority

Use the `qcn cnpv-priority alternate-priority` command in Global Configuration mode to globally configure the alternate priority for the selected cnpv-priority. When a frame is received with a dot1p priority equal to congestion notification priority value, the priority value in the frame is remarked with the alternate priority. The alternate priority is applied to incoming frames if and only if the incoming frame's dot1p priority is equal to CNPV priority of the CP and CP is configured as Edge.

Use the alternate priority setting to steer away traffic that comes from CN-unaware sources. Traffic from non-congestion aware sources is remarked when entering the CND domain so that the resources assigned to the congestion-enabled queues are not exhausted with traffic from QCN unaware sources. Since the frames are coming from non-QCN sources, they do not have a CN-TAG. If the frames are mapped to the congestion-enabled queue, then they may contribute to the congestion and, in turn, trigger generation of CNMs. This is not useful to sources that are QCN-unaware.

This configuration is applied to all ports whose defense-mode-choice is configured as *component*.

Format `qcn cnpv-priority cnpv priority alternate-priority non-cnpv priority`

Mode Global Config

Parameter	Description
cnpv priority	The range is 1–7.
non-cnpv priority	The range of alternate priority is 0–7.

6.2.0.4.1 no qcn cnpv-priority alternate-priority

Use the `no qcn cnpv-priority alternate-priority` command in Global Configuration mode to reset the alternate priority to the default value.

Format `no qcn cnpv-priority cnpv priority alternate-priority`
Mode Global Config

6.2.0.5 qcn cnpv-priority cp-creation

Use the `qcn cnpv-priority cp-creation` command in Global Configuration mode to globally configure the default scope for the per port-priority defense mode choice when a CP is newly created. The default scope for per-port defense mode choice can be **admin** or **component**.

Default qcn cp-creation is set to enable
Format `qcn cnpv-priority cnpv-priority cp-creation {enable | disable}`
Mode Global Config

Parameter	Description
cnpv-priority	The range is 1–7.
admin scope	Is per-priority.
component scope	Is per priority level configuration.
enable	If cp-creation is enabled, the per-port defense mode choice is set to **component**.
disable	If cp-creation is disabled, the per-port defense mode choice is set to **admin**.

6.2.0.6 qcn cnpv-priority defense-mode-choice

Use the `qcn cnpv-priority defense-mode-choice` command in Interface Configuration mode to select the defense-mode as **admin** or **component** on an interface, namely whether **interior**/**edge**/**disable** and alternate priorities should use the per-priority configuration or the per-port-priority configuration.

Default enable
Format `qcn cnpv-priority cnpv priority defense-mode-choice {admin | component}`
Mode Interface Config

Parameter	Description
cnpv priority	The range is 1–7.
admin scope	Is per-priority.
component scope	Is per priority level configuration.

6.2.0.7 qcn cnpv-priority

Use the `qcn cnpv-priority` command in Interface Config mode to configure a CP (port-queue) that is mapped to the specified dot1p priority as congestion enabled (interior) or congestion disabled (disabled) or edge congestion point (edge) for an interface which has the defense mode configured as **component** and a defense mode of **Admin**.

This configuration is applied if the defense mode choice is configured as **Admin**.

Default By default, QCN is not enabled for any priority.

Format `qcn cnpv-priority priority {interior | edge | disable}`

Mode Interface Config

Parameter	Description
cnpv-priority	The range is 1–7.
The possible selections for a Congestion Point (CP) are:	
Interior congestion point (ICP)	Used when a flow with the specified dot1p priority needs to be congestion aware. This setting enables detection of congestion of the selected priority.
Edge congestion point (ECP)	Used when the congestion point (CP) is on the edge of the congestion notification domain (CND).
Disabled for QCN	Used when it is desired that the priority be congestion unaware. This setting disables detection of congestion on the priority.

6.2.0.8 qcn cnpv-priority alternate-priority

Use the `qcn cnpv-priority alternate-priority` command in Interface Configuration mode to configure the alternate priority on an interface for the specified incoming ICP priority. This alternate-priority overrides the alternate-priority set in the global mode for this incoming ICP priority on this port. This configuration is applied if the defense mode choice is configured as **Admin**.

Default `By default, the alternate-priority configured in global is used.`

Format `qcn alternate-priority incoming priority alternate-priority`

Mode Interface Config

Parameter	Description
cnpv-priority	The range is 1–7.
alternate-priority	The range is 0–7.

6.2.0.8.1 no qcn cnpv-priority alternate-priority

Use the `no qcn cnpv-priority alternate-priority` command in Interface Configuration mode to reset the alternate priority of the given port-priority to the default value. If a global alternate priority value is configured, it is used.

Default `By default, the alternate-priority configured in global is applied.`

Format `no qcn alternate-priority incoming-priority alternate-priority`

Mode Interface Config

6.2.0.9 qcn transmit-tlv enable

Use the `qcn transmit-tlv enable` command in Interface Configuration mode to enable transmission of QCN TLVs via LLDP.

Default By default, transmission of QCN TLVs is disabled.

Format `qcn transmit-tlv enable`

Mode Interface Config

6.2.0.9.1 no qcn transmit-tlv enable

Use the `no qcn transmit-tlv enable` command in Interface Configuration mode to configure the mode of the QCN TLV transmission to disable. QCN TLVs transmission is propagated using LLDP.

Default By default, the alternate-priority configured in global gets applied.

Format `no qcn transmit-tlv enable`

Mode Interface Config

6.2.0.10 clear qcn statistics

Use the `clear qcn statistics` command in Privileged EXEC mode to clear the CNM transmitted counters on the CP. If interface and the CP are not mentioned, then this command clears all the CNM counters for all CPs in the system. If only the interface number is specified, then all the CNM transmit counters on that interface are cleared.

Format `clear qcn statistics [interface slot/port] [cp cp-index]`

Mode Privileged EXEC

Parameter	Description
slot/port	If only the interface number is specified, then all the CNM transmit counters on that interface are cleared.
cp-index	If only the cp index is specified, then CNM transmit counters for that cp index on all interfaces are cleared.

6.2.0.11 show qcn priority

Use the `show qcn priority` command in Privileged EXEC mode to display the QCN configuration.

Format `show qcn  priority [priority ] [interface slot/port| all]`

Mode Privileged EXEC

Parameter	Description
priority	If only priority is specified, then per-priority configuration is displayed.
all	If all is specified, then per priority information for all dot1p priorities is displayed.
slot/port	If the interface number is also specified, then the command displays the configuration per-port-priority for the given priority.

The following data is displayed as part of this command.

Example: The following shows example CLI display output for the command.

```
(Routing) #show qcn priority 1
```

Global Configuration:

```
QCN status(Master enable) :  Enabled
CNM transmit priority         : 0
```

Per-priority configuration:

```
Defense mode : interior
Alternate priority: 2
cp-creation : disabled
Errored port list: 0/1,0/8
LLDP mismatch port list : 0/5-8
Configured as CNPV on ports: 0/1,0/7-12
```

Example: The following shows example CLI display output for the command.

```
(Routing) #show qcn priority
```

Global Configuration:

```
QCN status(Master enable) :  Enabled
CNM transmit priority         : 0
```

Per-priority configuration:

```
dot1p-       Defense-mode Alternate-   cp-creation  Errored Port  LLDP         Configured
priority                  priority                  List          mismatch     as cnpv on
                                                                  list         ports
0            disabled     -            -            -             -            -
1            interior     0            enable       0/1,0/8       0/5-7        0/1-10
2            edge         0            disable      0/1           0/5-7        0/1-10
3            disabled     -            -            -             -            -
4            disabled     -            -            -             -            -
5            disabled     -            -            -             -            -
6            disabled     -            -            -             -            -
7            disabled     -            -            -             -            -
```

Example: The following shows example CLI display output for the command.

```
(Routing) #show qcn priority 1 interface 0/1
```

Global Configuration:

```
QCN status(Master enable) :  Enabled
CNM transmit priority         : 0
```

Per-port-priority configuration:

```
Defence mode choice : admin
Defense mode : interior
Alternate priority: 2
```

Example: The following shows example CLI display output for the command.

```
(Routing) #show qcn priority 1 interface all
```

Global Configuration:

```
QCN status(Master enable) :  Enabled
CNM transmit priority         : 0
```

Per-port-priority configuration

Interface Number	Defense-mode Choice	Defense Mode	Alternate Priority
0/1	admin	disabled	–
0/2	admin	interior	2
0/3	admin	edge	–
0/4	component	interior	3

6.2.0.12 show qcn active priority

Use the `show qcn active priority` command in Privileged EXEC mode to display the operational QCN configuration for the specified dot1p priority.

Format `show qcn active priority 0-7`
Mode Privileged EXEC

Interface Number	Defense mode	Alternate priority
0/1	interior	2
0/2	edge	–
0/3	interior	0
0/4	disabled	–
0/5	interior	–

Example: The following shows example CLI display output for the command.

```
(Routing) #show qcn active priority 1
Port     Defense        Alternate
         mode           priority
------  ------------ ---------------

0/1     disable        0

0/2     disable        0

0/3     disable        0

0/4     disable        0

0/5     disable        0

0/6     disable        0

0/7     disable        0

0/8     disable        0

0/9     disable        0

--More-- or (q)uit
```

6.2.0.13 show qcn interface

Use the `show qcn interface` command in Privileged EXEC mode to display Congestion Point information for the specified port.

Format `show qcn interface slot/port [cp cpindex]`
Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) #show qcn interface 0/1 cp-index 1

Interface        0/1

cp-index        1

MAC-Address         00:10:18:00:00:FF

CP-Identifier       : 00012610071005

CNM-transmit-Priority        0

Congestion queue weight

Sample-base

Cp-Sizesetpoint

Min-HeaderOctets

Note: CPID can be deciphered  as mentioned below.
000126 : Last 3 bytes of system MAC Address
1  - unit number on which congestion is detected
0  - slot number on which congestion is detected
07 – port number on which congestion is detected
1 – unit number from which CNM is transmitted
0 – slot number from which CNM is transmitted
05- port number on which CNM is transmitted.
```

6.2.0.14 show qcn statistics

Use the `show qcn statistics` command in Privileged EXEC mode to display the statistics of the CNM and data frames for all the ports or for the specified CP for the given port.

Format `show qcn statistics {all | interface slot/port cp cp index}`

Mode Privileged EXEC

Example: The following data is displayed in tabular format as output for this command.

```
(Routing) #show qcn statistics interface 0/1 cp-index 1
Interface     Cp Index       CNMs transmitted
0/1           1            1230
```

6.3 Enhanced Transmission Selection Commands

Enhanced Transmission Selection (ETS) allows Class of Service (CoS) configuration settings to be advertised to other devices in a data center network through DCBX ETS TLVs. CoS information is exchanged with peer DCB devices using ETS TLVs.

ETS is configured in conjunction with CoS Queuing, which allows you to directly configure certain aspects of the device hardware queuing to provide the desired Quality of Service (QoS) behavior for different types of network traffic. The priority of a packet arriving at an interface can be used to steer the packet to the appropriate outbound CoS queue through a mapping table. CoS queue characteristics such as minimum guaranteed bandwidth, transmission rate shaping, etc. are user configurable at the queue (or port) level. For more information about the CoS commands, see Section 12.1, Class of Service Commands.

6.3.0.1 classofservice traffic-class-group

Use the `classofservice traffic-class-group` command in Global Config or Interface Config mode to map the internal Traffic Class Group (TCG).

Default All traffic classes are mapped to TCG 0.

Format `classofservice traffic-class-group` *`trafficclass traffic class group`*

Mode
- Global Config
- Interface Config

Parameter	Description
trafficclass	The Traffic Class can range from 0–7, although the actual number of available traffic classes depends on the platform.
traffic class group	The Traffic Class Group can range from 0–7, although the actual number of available traffic classes depends on the platform.

6.3.0.1.1 no classofservice traffic-class-group

Use the `no classofservice traffic-class-group` command in Global Config or Interface Config mode to restore the default mapping for each of the Traffic Classes.

Format `no classofservice traffic-class-group`

Mode
- Global Config
- Interface Config

6.3.0.2 traffic-class-group max-bandwidth

Use the `traffic-class-group max-bandwidth` command in Global Config or Interface Config mode to specify the maximum transmission bandwidth limit for each Traffic Class Group (TCG). Also known as rate shaping, this has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded. The total number of TCG supported per interface is platform specific.

Default Max-bandwidth is zero for all TCG.

Format `traffic-class-group max-bandwidth` *`bw-0 bw-1 … bw-n`*

Mode
- Global Config
- Interface Config

This command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces. The Interface Config mode command is only available on platforms that support independent per-port class of service queue configuration.

Each bw-x value is a percentage that ranges from 0 to 100 in increments of 1. All n bandwidth values must be specified with this command, and each is independent of the others. The number n is platform-dependent and corresponds to the number of supported traffic classes groups. The default maximum bandwidth value for each TCG is 0, meaning no upper limit is enforced, which allows the TCG queue to consume any available non-guaranteed bandwidth of the interface.

If a non-zero value is specified for any bw-x maximum bandwidth parameter, it must not be less than the current minimum bandwidth value for the corresponding queue. A bw-x maximum bandwidth parameter value of 0 may be specified at any time without restriction.

The maximum bandwidth limits may be used with either a weighted or strict priority scheduling scheme.

NOTE: A value of 0 (the default) implies an unrestricted upper transmission limit, which is similar to 100%, although there may be subtle operational differences depending on how the device handles a *no limit* case versus *limit to 100%*.

6.3.0.2.1 no traffic-class-group max-bandwidth

Use the `no traffic-class-group max-bandwidth` command in Global Config or Interface Config mode to restore the default for each queue's maximum bandwidth value.

Format `no traffic-class-group max-bandwidth`

Mode
- Global Config
- Interface Config

6.3.0.3 traffic-class-group min-bandwidth

Use the `traffic-class-group min-bandwidth` command in Global Config or Interface Config mode to specify the minimum transmission bandwidth guarantee for each interface TCG. The total number of TCG supported per interface is platform specific.

Default Min-bandwidth is zero for all TCG.

Format `traffic-class-group min-bandwidth` *`bw-0 bw-1 … bw-n`*

Mode
- Global Config
- Interface Config

The command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces. The Interface Config mode command is only available on platforms that support independent per-port class-of-service queue configuration.

Each bw-x value is a percentage that ranges from 0 to 100 in increments of 1. All n bandwidth values must be specified with this command, and their combined sum must not exceed 100%. The number n is platform dependent and corresponds to the number of supported Traffic Class Groups. The default minimum bandwidth value for each TCG is 0, meaning no bandwidth is guaranteed (best effort).

If the value of any bw-x minimum bandwidth parameter is specified as greater than the current maximum bandwidth value for the corresponding TCG, then its corresponding maximum bandwidth automatically increases the maximum to the same value.

6.3.0.3.1 no traffic-class-group min-bandwidth

Use the `no traffic-class-group min-bandwidth` command in Global Config or Interface Config mode to restore the default for each queue's minimum bandwidth value.

Format `no traffic-class-group min-bandwidth`

Mode
- Global Config
- Interface Config

6.3.0.4 traffic-class-group strict

Use the `traffic-class-group strict` command in Global Config or Interface Config mode to activate the strict priority scheduler mode for each specified TCG.

Default Weighted scheduler mode is used for all TCG

Format `traffic-class-group strict` *`tcg-id-0`* `[`*`tcg-id-1 … tcg-id-n`*`]`

Mode
- Global Config
- Interface Config

The command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces. The Interface Config mode command is only available on platforms that support independent per-port class-of-service queue configuration.

At least one, but no more than *n*, tcg-id values are specified with this command. Duplicate tcg-id values are ignored. Each tcg-id value ranges from 0 to (n-1), where n is the total number of TCG supported per interface. The number n is platform dependent and corresponds to the number of supported Traffic Class Groups.

When strict priority scheduling is used for a TCG, the minimum bandwidth setting for the TCG is ignored and packets are scheduled for transmission as soon as they arrive. A maximum bandwidth setting for the queue, if configured, serves to limit the outbound transmission rate of a strict priority TCG queue so that it does not consume the entire capacity of the interface. If multiple TCG on the same interface are configured for strict priority mode, the method of handling their packet transmission is platform specific. One typical scheme is to schedule all strict priority TCG ahead of the weighted queues, giving preference among the strict priority TCG to the one with the highest tcg-id.

6.3.0.4.1 no traffic-class-group strict

Use the `no traffic-class-group strict` command in Global Config or Interface Config mode to restore the default weighted scheduler mode for each specified TCG.

Format `no traffic-class-group strict` *`tcg-id-0`* `[`*`tcg-id-1 … tcg-id-n`*`]`

Mode
- Global Config
- Interface Config

6.3.0.5 traffic-class-group weight

Use the `traffic-class-group weight` command in Global Config or Interface Config mode to specify the weight for each interface TCG. The total number of TCGs supported per interface is platform specific.

Default For TCG0:TCG1:TCG2, weights are in the ratio 100%:0%:0%

Format `traffic-class-group weight` *`wp-0 wp-1 … wp-n`*

Mode
- Global Config
- Interface Config

The command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces. The Interface Config mode command is only available on platforms that support independent per-port class-of-service queue configuration.

Each wp-x (weight percentage) value is a percentage that ranges from 0 to 100 in increments of 1. All *n* bandwidth values must be specified with this command, and their combined sum must not exceed 100%. The number *n* is platform dependent and corresponds to the number of supported Traffic Class Groups. The default weight percentage value is in the ratio of 1:2:3 for TCG0:TCG1:TCG2, which is calculated as 100%:0%:0%.

The weight percentage is not considered for TCG that are configured for strict scheduling.

6.3.0.5.1 no traffic-class-group weight

Use the `no traffic-class-group weight` command in Global Config or Interface Config mode to restore the default for each queue's weight percentage value.

Format `traffic-class-group weight` *`wp-0 wp-1 … wp-n`*

Mode
- Global Config
- Interface Config

6.3.0.6 show classofservice traffic-class-group

Use the `show classofservice traffic-class-group` command in Privileged EXEC mode to display the Traffic Class to Traffic Class Group mapping.

Format `show classofservice traffic-class-group [`*`slot/port`*`]`

Mode Privileged EXEC

Parameter	Description
slot/port	Optional and is only valid on platforms that support independent per-port class of service mappings. ■ If *slot/port* is specified, the TCG mapping table of the interface is displayed. ■ If *slot/port* is omitted, the global configuration settings are displayed (these may have been subsequently overridden by per-port configuration).
Traffic Class	The traffic class queue identifier.
Traffic Class Group	The traffic class Group identifier.

Example: The following shows example CLI display output for the command.

```
(Routing) #show classofservice traffic-class-group
```

```
 Traffic Class    Traffic Class Group
 -------------    -------------------
   0                0
   1                1
   2                1
   3                1
   4                2
   5                1
   6                1
   7                1
```

6.3.0.7 show interfaces traffic-class-group

Use the `show interfaces traffic-class-group` command in Privileged EXEC mode to display the Traffic Class Group configuration.

Format `show interfaces traffic-class-group [slot/port]`

Mode Privileged EXEC

Parameter	Description
slot/port	Optional and is only valid on platforms that support independent per-port class of service mappings. ■ If *slot/port* is specified, the TCG mapping table of the interface is displayed. ■ If *slot/port* is omitted, the global configuration settings are displayed (these may have been subsequently overridden by per-port configuration).
Interface	This displays the slot/port of the interface. If displaying the global configuration, this output line is replaced with a Global Configuration indication.
Traffic Class Group	The traffic class Group identifier.
Min-Bandwidth	The minimum transmission bandwidth, expressed as a percentage. A value of zero means bandwidth is not guaranteed and the TCG operates using best-effort. This is a configured value.
Max-Bandwidth	The maximum transmission bandwidth, expressed as a percentage. A value of zero means no upper limit is enforced, so the queue may use any or all of the available bandwidth of the interface. This is a configured value.
Scheduler Type	Indicates whether this queue is scheduled for transmission using a strict priority or a weighted scheme. Strict priority scheduler is to provide lower latency to the higher CoS classes of traffic. Weighted scheduling is a round robin mechanism with weights associated to each CoS class of traffic. This is a configured value.
Weight Percentage	The weight of the TCG used during non-strict scheduling.

Example: The following shows example CLI display output for the command.

```
(Routing) #show interfaces traffic-class-group

Global Configuration

TCG Id    Min.         Max         Scheduler  Weight
          Bandwidth    Bandwidth   Type       Percentage
-------   ----------   ---------   ---------  ----------
   0       0           0        Strict        0
   1       0           0        WDRR         50
   2       0           0        WDRR         50
```

6.4 FIP Snooping Commands

The Fibre Channel over Ethernet (FCoE) Initialization Protocol (FIP) is used to perform the functions of FC_BB_E device discovery, initialization and maintenance. FIP uses a separate EtherType from FCoE to enable the distinction of discovery, initialization, and maintenance traffic from other FCoE traffic. FIP frames (with one exception) are the standard Ethernet size (1518 Byte 802.1q frame) whereas FCoE frames are a maximum of 2240 bytes.

This document describes FIP snooping, which is a frame inspection method used by FIP Snooping Bridges to monitor FIP frames and apply policies based upon the L2 header information in those frames, following recommendations in Annex C of FC_BB_5 Rev 2.00. This allows for:

1. Auto-configuration of Ethernet ACLs based on information in the Ethernet headers of FIP frames.
2. Emulation of FC point-to-point links within the DCB Ethernet network.
3. Enhanced FCoE security/robustness by preventing FCoE MAC spoofing.

The FIP Snooping Bridge solution in EFOS supports configuration-only of perimeter port role and FCF-facing port roles and is only intended for use at the edge of the switched network.

The role of FIP Snooping-enabled ports on the switch falls under one of the following types:

1. Perimeter or Edge port (connected directly to ENode).
2. FCF facing port (that receives traffic from FCFs targeted to the ENodes).

The default port role in an FCoE enabled VLAN is as a perimeter port. FCF facing ports must be configured by the user.

6.4.0.1 feature fip-snooping

Use the **feature fip-snooping** command in Global Configuration mode to globally enable Fibre Channel over Ethernet Initialization Protocol (FIP) snooping on the switch. When FIP snooping is disabled, received FIP frames are forwarded or flooded using the normal multicast rules.

When FIP snooping is enabled, FC-BB-5 Annex D ACLs are installed on the switch and FIP frames are snooped. FIP snooping will not allow FIP or Fiber Channel over Ethernet (FCoE) frames to be forwarded over a port until the port is operationally enabled for PFC. VLAN tagging must be enabled on the interface in order to carry the dot1p values through the network.

Default	disabled
Format	`feature fip-snooping`
Mode	Global Config

Example: The following example enables the FIP snooping feature.

```
s1(config)#feature fip-snooping
```

6.4.0.1.1 no feature fip-snooping

Use the **no** form of the command to return the settings to the default values and globally disable FIP snooping. When FIP snooping is globally disabled, received FIP frames are forwarded or flooded using the normal multicast rules. In addition, other FIP snooping commands are not available until the FIP snooping feature is enabled.

Format	`no feature fip-snooping`

Mode Global Config

Example: The following example disables the FIP snooping feature.

```
s1(config)#no feature fip-snooping
```

6.4.0.2 fip-snooping enable

Use the **fip-snooping** command in VLAN Configuration mode to enable snooping of FIP packets on the configured VLANs. FIP snooping is disabled on VLANs by default.

Priority Flow Control (PFC) must be operationally enabled before FIP snooping can operate on an interface. VLAN tagging must be enabled on the interface in order to carry the dot1p value through the network.

This command can only be entered after FIP snooping is enabled using the Section 6.5.0.1, priority-flow-control mode command. Otherwise, it does not appear in the CLI syntax tree.

Default disabled

Format `feature fip-snooping`

Mode VLAN Config

Example: The following example enables FIP snooping on VLANs 2, 3,...8.

```
s1(config)#vlan 2-8
s1(config-vlan)#fip-snooping enable
```

6.4.0.2.1 no fip-snooping enable

Use the **no** form of the command to return the mode to the default (off).

Format `no feature fip-snooping`

Mode VLAN Config

Example: The following example disables FIP snooping on VLANs range 2 to 8.

```
s1(config)#vlan 2-8
s1(config)(vlan 2-8)#no fip-snooping enable
s1(config)(vlan 2-8)# exit
```

6.4.0.3 fip-snooping fc-map

Use the **fip-snooping fc-map** command in VLAN Configuration mode to configure the FP-MAP value on a VLAN. The FC map value is used to help in securing the switch against misconfiguration.

When configured using fabric-provided MAC addresses, FCoE devices transmit frames containing the FC map value in the upper 24 bits. Only frames that match the configured FC map value are passed across the VLAN. Frames with MAC addresses that do not match the FC map value are discarded.

This command can only be entered after FIP snooping is enabled using the Section 6.5.0.1, priority-flow-control mode command. Otherwise, it does not appear in the CLI syntax tree.

Default The default FC map value is 0x0efc00.

Format `fip-snooping fc-map 0x0 - 0xffffff`
Mode VLAN Config

Parameter	Description
map value	Valid FC map values are in the range of 0x0 to 0xffffff.

Example: The following example configures an FC map value of 0x100 on VLAN 208.

```
(config)# vlan 208
(config-vlan)# fip-snooping enable
(config-vlan)# fip-snooping fc-map 0x100
```

Example: The following example configures an FC value of 0xFFCB for VLAN range 2 to 8.

```
(config)# vlan 2-8
(config)(vlan 2-8)# fip-snooping fc-map 0xecffcb
(config)(vlan 2-8)# exit
```

6.4.0.3.1 no fip-snooping fc-map

The no version of the command sets the FC-MAP value for the VLAN to the default value.

Format `no fip-snooping fc-map`
Mode VLAN Config

6.4.0.4 fip-snooping port-mode

To relay the FIP packets received from the hosts toward the Fibre Channel Fabric (FCF), the switch needs to know the interfaces to which the FCFs are connected. Use the **fip-snooping port-mode** command in Interface Configuration mode to configure the interface that is connected towards FCF. By default, an interface is configured to be a host-facing interface if it is not configured to be an FCF-facing interface.

It is recommended that FCF-facing ports be placed into auto-upstream mode in order to receive DCBX information and propagate it to the CNAs on the downstream (host-facing) ports.

Interfaces enabled for PFC should be configured in trunk or general mode and must be PFC-operationally enabled before FCoE traffic can pass over the port.

This command can only be entered after FIP snooping is enabled using the Section 6.5.0.1, priority-flow-control mode command. Otherwise, it does not appear in the CLI syntax tree.

Default Configuration as a host-facing interface.
Format `fip-snooping port-mode fcf`
Mode Interface Config

Parameter	Description
fcf	Fibre Channel Fabric

Example: The following example configures an interface to be connected to an FCF switch.

```
(Config)# interface 1/0/1
(Interface 1/0/1)# fip-snooping port-mode fcf
(Interface 1/0/1)# exit
```

6.4.0.4.1 no fip-snooping port-mode

Use the no form of the command to set the interface to be connected towards the host.

Format `no fip-snooping port-mode`

Mode Interface Config

Example: The following example sets the interface to be connected towards the host.

```
(Config)# interface 1/0/1
(Interface 1/0/1)# no fip-snooping port-mode fcf
(Interface 1/0/1)# exit
```

6.4.0.5 show fip-snooping

Use the **show fip-snooping sessions** command in User EXEC or Privileged EXEC mode to display information about the global FIP snooping configuration and status.

Format `show fip-snooping`

Mode
- User EXEC
- Privileged EXEC

The following information is displayed.

Parameter	Description
Global Mode	FIP snooping configuration status on the switch. It displays **Enable** when FIP snooping is enabled on the switch and **Disable** when FIP snooping is disabled on the switch.
FCoE VLAN List	List of VLAN IDs on which FIP snooping is enabled.
FCFs	Number of FCFs discovered on the switch.
ENodes	Number of Enodes discovered on the switch.
Sessions	Total virtual sessions on the switch.
Max VLANs	Maximum number of VLANs that can be enabled for FIP snooping on the switch.
Max FCFs in VLAN	Maximum number of FCFs supported in a VLAN.
Max ENodes	Maximum number of ENodes supported in the switch.
Max Sessions	Maximum number of Sessions supported in the switch.

Example: The following shows example CLI display output for the command.

```
(switch)# show fip-snooping

Global Mode:   Enable
FCoE VLAN List :   2,4,5-8
FCFs   :   2
ENodes :   2
Sessions:   10
Max VLANs:   8
Max FCFs in VLAN:   4
Max ENodes:   312
```

```
Max Sessions:   1024
```

6.4.0.6 show fip-snooping enode

Use the **show fip-snooping enode** command in User EXEC or Privileged EXEC mode to display information about the interfaces connected to ENodes.

NOTE: This command can only be entered after FIP snooping is enabled using the **feature fip-snooping** command. Otherwise, it does not appear in the CLI syntax tree.

Format `show fip-snooping enode [enode-mac]`

Mode
- User EXEC
- Privileged EXEC

Parameter	Description
enode-mac	MAC address of the enode to display.

The command displays the following information.

Parameter	Description
Interface	Interface to which the ENode is connected.
VLAN	ID number of the VLAN to which the ENode belongs.
NameID	Name of the ENode.
FIP-MAC	MAC address of the ENode.
FCID	Fiber channel ID number of the virtual port that was created by FCF when the ENode logged into the network.
Sessions Established	Number of successful virtual connections established.

The command displays the following additional information when the optional argument is supplied.

Parameter	Description
Sessions Waiting	Number of virtual connections waiting for FCF acceptance.
Sessions Failed	Number of virtual sessions failed.
Max-FCoE-PDU	Maximum FCoE PDU size the ENode MAC intends to use for FCoE traffic. This is equivalent to the maximum Ethernet frame payload the ENode intends to send.
Time elapsed	Time elapsed since first successful login session snooped from the ENode.

Example: The following example displays sample output of the command with no optional argument supplied.

```
(switch)# show fip-snooping enode
Interface  VLAN  Name-ID          ENode-MAC      FCFs   Sessions
--------------------------------------------------------1/0/2     1    00000000    00:0c:29:65:82:bc
1     3
1/0/5      100   00000000     00:0d:31:23:53:11   2     5
```

Example: The sample output of the command below displays with the optional argument supplied.

```
(switch)# show fip-snooping enode 00:0c:29:65:82:bc

Interface    1/0/2
```

```
VLAN          1
Name-ID       000000
ENode-MAC     00:0c:29:65:82:bc
FCFs Connected1
Sessions Established3
Sessions Waiting 1
Session Failed 0
Max-FCoE-PDU  2158
Time elapsed  0 days, 1 hours, 20 minutes
```

6.4.0.7 show fip-snooping fcf

Use the **show fip-snooping fcf** command in User EXEC or Privileged EXEC mode to display information about the interfaces connected to FCFs.

NOTE: This command can only be entered after FIP snooping is enabled using the **feature fip-snooping** command. Otherwise, it does not appear in the CLI syntax tree.

Format `show fip-snooping fcf [fcf-mac]`

Mode
- User EXEC
- Privileged EXEC

The following information is displayed when no FCF mac argument is supplied.

Parameter	Description
Interface	Interface to which the FCF is connected.
VLAN	ID number of the VLAN to which the FCF belongs.
No. of ENodes	Total number of ENodes that are connected to the FCF.
FPMA/SPMA	Type of the MAC address for ENode as negotiated by the FCF.
FCMAP	FCMAP value used by the FCF.
FCF-MAC	MAC address of the FCF.
Fabric Name	Name of the FCF.

Below is additional information regarding the FCF that is displayed when the optional FCF MAC address argument is provided.

Parameter	Description
Sessions	Total number of virtual sessions accepted by FCF in the associated VLAN.
D-bit	This reflects the value of the D-bit provided by the most recently received Discovery Advertisement from the FCF. When D-bit value is zero then FIP snooping bridge verifies the periodic VN_Port FIP Keep Alive frames associated with FCF and Discovery Advertisements sent by FCF. When D-bit is set to 1, switch discards snooped VN_Port FIP Keep Alive frames associated with FCF and does not timeout the FCoE sessions established with the FCF based on FKA_VN_PERIOD*5 interval.
Available for Login	This reflects the value of the A bit provided by the most recently received Discovery Advertisement from the FCF. This provides the information that the transmitting FCF is available for FIP FLOGI/FDISC from ENodes. This is informational and shall have no effect on existing logins.
Priority	The Priority returned from the FCF in the Solicited Discovery Advertisement. This indicates the Priority that has been manually assigned to the FCF.
FKA-ADV	FIP keepalive interval (FKA_ADV_PERIOD) in seconds configured on the FCF multiplied by five. For example, if the FKA_ADV period configured on the FCF is 80 seconds, the value of this field is 400.
FCF Expiry Time	This is timer value to monitor the status of the FCF. FCF entry and all its associated virtual sessions will be removed when the value reaches 0. This value is reset to **Configured FKA-ADV** every time a Discovery Advertisement is received from the FCF-MAC.
Time Elapsed	Time since FCF is Discovered.

Example: The following displays sample output of the command when no optional argument is provided.

```
(config)# show fip-snooping fcf
--------------------------------------------------------------------------------
Interface VLAN ENodes FPMA/ FC-MAP       FCF-MAC       Name-ID     Fabric-Name
                      SPMA
--------------------------------------------------------------------------------1/0/11     1   2
FPMA 0e:fc:00 00:0d:ec:b2:2c:80 20:65:00:0d: 20:65:00:0d:
                                                    ec:b1:9e:81  ec:97:52:c1
3/0/10     1   1      FPMA 0e:fc:00 00:0d:ec:b2:2c:81 00000000     00000000
3/0/15    100  1      FPMA 0e:fc:10 00:0c:ab:2c:eb:12 00000000     00000000
```

Example: The following displays sample output of the command when the optional argument is provided.

```
(switch)# show  fip-snooping   fcf   00:0d:ec:b2:2c:81
Interface     3/0/10
VLAN             1
ENodes        1
FPMA/SPMA     FPMA
FCF-MAC       00:0d:ec:b2:2c:81
FC-MAP           0e:fc:00
Name-ID       20:65:00:0d:ec:b1:9e:81
Fabric-Name   20:65:00:0d:ec:97:52:c1
Sessions      3
D-bit            0
Available for Login1
Priority      2
FKA-ADV(FKA_ADV_PERIOD*5)       250
FCF Expiry Time219
Time Elapsed 0 days, 2 hours, 8 minutes
```

6.4.0.8 show fip-snooping sessions

Use the `show fip-snooping sessions` command in User EXEC or Privileged EXEC mode to display information about the active FIP snooping sessions.

NOTE: This command can only be entered after FIP snooping is enabled using the `feature fip-snooping` command. Otherwise, it does not appear in the CLI syntax tree.

Format `show fip-snooping sessions [[[vlan vlan-id] | [interface interface-id] | [fcf fcf-mac [enode enode-mac]]] [detail]]`

Mode
- User EXEC
- Privileged EXEC

Parameter	Description
Interface-id	ID of an interface on which FIP snooping has been enabled.
FCF-MAC	MAC address of the FCF that is part of the session.
ENode-MAC	MAC address of the ENode that is part of the session.
VLAN	ID number of the VLAN that contains the session.
FCoE MAC	Source MAC address of the FCoE packets that are originated by the ENode as part of the session.
FC-ID	Fiber Channel ID of the virtual port that was created by the FCF when the ENode VN_Port did a FLOGI/NPIV/ FDISC request.

The command output format is different when the **detail** option is used. The information below is displayed.

Parameter	Description
VLAN	VLAN to which the session belongs.
FC-MAP	FCMAP value used by the FCF.
FCFs	Number of FCFs discovered.
ENodes	Number of ENodes discovered.
Sessions	Total virtual sessions in FCoE VLAN.
FCF Information	
Interface	Interface on which the FCF is discovered.
MAC	MAC address of the FCF.
ENodes	Total number of ENodes that are connected to the FCF.
Sessions	Total number of virtual sessions accepted by FCF in the associated VLAN.
ENode Information	
Interface	Interface to which the ENode is connected.
MAC	MAC address of the ENode.
Sessions	Total number of virtual sessions originated from ENodes to FCF in the VLAN.
Waiting	Total number of virtual connections waiting for FCF acceptance in the VLAN.
Session Information	
FCoE-MAC	Source MAC address of the FCoE packets that are originated by the ENode as part of the session.
Request (FP, SP)	FIP session request type sent by ENode. This can be FLOGI or FDESC (NPIV FDISC). Whereas FP and SP values are the FP bit and the SP bit values in the FLOGI or NPIV FDISC request respectively.

Parameter	Description
Expiry Time	This is virtual connection/session expiry interval. This is used to monitor the status of the session. Session entry is removed when the value reaches 0. This value is reset to 450 secs (5*90 secs) every time an associated VN_Port FKA is received from the ENode. This is ignored (marked as **NA**) if the D-bit is set to one in the FCF Discovery Advertisements.
Mode	This is the addressing mode in use by the VN_Port at ENode. In other words, this is the type of MAC address granted (selected and returned) by FCF. This can be one of the addressing modes, i.e. FPMA or SPMA.
State	This is the state of the virtual session. The state is displayed as **Tentative** during the process of ENode login to FCF (using FLOGI or FDESC). It displays **Active** after ENode and FCF establish a successful virtual connection.
Session-Time	Time elapsed after this successful virtual session is established by ENode with FCF. The value is displayed in **xd**, **yh**, **zm** format where **x** represents number of days, **y** represents hours and **z** represents minutes elapsed following this successful virtual session. This field has no useful information for waiting sessions.

Example: The following sample command output displays when no arguments are provided.

```
(switch)# show fip-snooping sessions
--------------------------------------------------------------------------------
     FCF-MAC            ENode-MAC     VLAN      FCoE-MAC        FC-ID
--------------------------------------------------------------------------------
00:0d:ec:b2:2c:80  00:0c:29:65:82:bc  100   0e:fc:00:ad:00:00  38:0f:db
00:0d:ec:b2:2c:80  00:0c:29:65:82:bc  100   0e:fc:00:ad:00:01  38:0f:dc
00:0d:ec:b2:2c:80  00:0c:29:65:82:bc  100   0e:fc:00:ad:00:02  38:0f:dd
00:0d:ec:b2:2c:80  00:0c:29:65:82:bc  100   0e:fc:00:ad:00:05  38:0f:e1
00:0d:ec:b2:2c:80  00:0c:29:65:82:bc  100   0e:fc:00:ad:00:07  38:0f:e3
00:0d:ec:b2:2c:80  00:0c:29:65:82:bc  100   0e:fc:00:ad:00:10  38:0f:e6
00:0d:ec:b2:2c:80  00:0c:29:65:82:bc  100   0e:fc:00:ad:00:19  38:0f:ee
00:0e:ad:12:23:53  00:0d:29:12:22:a6  200   0e:fc:11:aa:bb:00  44:23:a4
00:0e:ad:12:23:53  00:0d:29:12:22:a6  200   0e:fc:11:aa:bb:01  44:02:ab
00:0e:ad:12:23:53  00:0d:29:23:14:22  200   0e:fc:11:aa:bb:02  44:35:1b
00:0e:ad:12:23:53  00:0d:29:23:14:22  200   0e:fc:11:aa:bb:03  44:35:2a
00:0e:ad:12:23:53  00:0d:29:23:14:22  200   0e:fc:11:aa:bb:04  44:36:3b
```

Example: The sample command output below displays when the detail option is specified.

```
(switch)# show fip-snooping sessions detail

VLAN: 100   FC-MAP: 0e:fc:00        FCFs:  1   ENodes: 1   Sessions: 7
   <FCF Information>
   Interface: 3/0/15   MAC: 00:0d:ec:b2:2c:80 ENodes: 1   Sessions: 7
      <ENode Information>
      Interface: 2/0/1    MAC: 00:0c:29:65:82:bc Sessions:  7   Waiting: 0
         <Session Information>
         FCoE-MAC           Request    Expiry  Mode State      Session-Time
                            (FP,SP)    Time
         0e:fc:00:ad:00:00  FLOGI(1,1) 200     FPMA ACTIVE     0d, 04h, 20m
         0e:fc:00:ad:00:01  FDESC(1,1) 259     FPMA ACTIVE     0d, 04h, 19m
         0e:fc:00:ad:00:02  FDESC(1,1) 215     FPMA ACTIVE     0d, 04h, 18m
         0e:fc:00:ad:00:05  FDESC(1,1) 231     FPMA ACTIVE     0d, 04h, 10m
         0e:fc:00:ad:00:07  FDESC(1,1) 189     FPMA ACTIVE     0d, 04h, 01m
         0e:fc:00:ad:00:10  FDESC(1,1) 210     FPMA ACTIVE     0d, 02h, 07m
         0e:fc:00:ad:00:19  FDESC(1,1) 222     FPMA ACTIVE     0d, 01h, 20m
--------------------------------------------------------------------------------
VLAN: 200   FC-MAP: 0e:fc:11        FCFs:  1   ENodes: 2   Sessions: 5

   <FCF Information>
   Interface: 3/0/11   MAC: 00:0e:ad:12:23:53 ENodes: 2   Sessions: 5

      <ENode Information>
```

```
      Interface: 1/0/10   MAC: 00:0d:29:12:22:a6 Sessions: 2    Waiting: 0
         <Session Information>
         FCoE-MAC          Request    Expiry  Mode State      Session-Time
                           (FP,SP)    Time
         0e:fc:11:ad:00:00 FLOGI(1,1) 242     FPMA ACTIVE     0d, 02h, 30m
         0e:fc:11:ad:00:01 FDESC(1,1) 245     FPMA ACTIVE     0d, 02h, 28m
      <ENode Information>
      Interface: 1/0/11   MAC: 00:0d:29:23:14:22 Sessions: 3    Waiting: 1
         <Session Information>
         FCoE-MAC          Request    Expiry  Mode State      Session-Time
                           (FP,SP)    Time
         0e:fc:11:ad:00:02 FLOGI(1,1) 202     FPMA ACTIVE     0d, 02h, 20m
         0e:fc:11:ad:00:03 FDESC(1,1) 228     FPMA ACTIVE     0d, 01h, 18m
         0e:fc:11:ad:00:03 FDESC(1,1) 232     FPMA ACTIVE     0d, 01h, 02m
         ----------------- FDESC(1,1) ---     FPMA TENTATIVE  ------------
```

Example: The sample command output below displays sessions between specified FCF and ENode.

```
(switch)# show fip-snooping sessions fcf 00:0e:ad:12:23:53 enode 00:0d:29:12:22:a6

--------------------------------------------------------------------------------
     FCF-MAC            ENode-MAC     VLAN      FCoE-MAC       FC-ID
--------------------------------------------------------------------------------
00:0e:ad:12:23:53  00:0d:29:12:22:a6  200   0e:fc:11:aa:bb:00  44:23:a4
00:0e:ad:12:23:53  00:0d:29:12:22:a6  200   0e:fc:11:aa:bb:01  44:02:ab
```

Example: The sample command output below displays sessions between specified FCF and ENode with the **detail** option.

```
(switch)# show fip-snooping sessions fcf 00:0e:ad:12:23:53 enode 00:0d:29:12:22:a6 detail

VLAN: 200   FC-MAP: 0e:fc:11        FCFs:  1   ENodes: 2   Sessions: 5

   <FCF Information>
   Interface: 3/0/11   MAC: 00:0e:ad:12:23:53 ENodes: 2   Sessions: 5

      <ENode Information>
      Interface: 1/0/10   MAC: 00:0d:29:12:22:a6 Sessions: 2    Waiting: 0
         <Session Information>
         FCoE-MAC          Request    Expiry  Mode State      Session-Time
                           (FP,SP)    Time
         0e:fc:11:ad:00:00 FLOGI(1,1) 242     FPMA ACTIVE     0d, 02h, 30m
         0e:fc:11:ad:00:01 FDESC(1,1) 245     FPMA ACTIVE     0d, 02h, 28m
```

6.4.0.9 show fip-snooping statistics

Use the **show fip-snooping statistics** command in User EXEC or Privileged EXEC mode to display the statistics of the FIP packets snooped in the VLAN or on an interface. If the optional (VLAN or interface) argument is not given, this command displays the statistics for all of the FIP snooping enabled VLANs.

NOTE: This command can only be entered after FIP snooping is enabled using the **feature fip-snooping** command. Otherwise, it does not appear in the CLI syntax tree.

Format **show fip-snooping statistics [vlan *vlan-id*] | [interface *interface-id*]**

Mode
- User EXEC
- Privileged EXEC

Parameter	Description
vlan-id	A VLAN on which FIP snooping is enabled.
interface-id	An interface belonging to a VLAN on which FIP snooping is enabled.

The following table describes the packet counters per FIP Operation.

Packet Counter	Description
VR	Number of VLAN Request messages received on the VLAN.
VN	Number of VLAN Notification messages received on the VLAN.
MDS	Number of Multicast Discovery Solicitation messages snooped on the VLAN.
UDS	Number of Unicast Discovery Solicitation messages snooped on the VLAN.
FLOGI	Number of Fabric Logins snooped on the VLAN.
FDISC	Number of fabric discovery logins snooped on the VLAN.
LOGO	Number of Fabric Logouts on the VLAN.
VNPort-keep-alive	Number of VN_Port keepalive messages snooped on the VLAN.
MDA	Number of Multicast Discovery Advertisement messages snooped on the VLAN.
UDA	Number of Unicast Discovery Advertisement messages snooped on the VLAN.
FLOGI_ACC	Number of Fabric Logins accepted on the VLAN.
FLOGI_RJT	Number of Fabric Logins rejected on the VLAN.
FDISC_ACC	Number of Fabric Discoveries accepted on the VLAN.
FDISC_RJT	Number of Fabric Discoveries rejected on the VLAN.
LOGO_ACC	Number of Fabric Logouts accepted on the VLAN.
LOGO_RJT	Number of Fabric Logouts rejected on the VLAN.
CVL	Number of Clear Virtual Links actions on the VLAN.

The following table describes the other interface or session-related counters.

Other Counters	Description
Number of Virtual Session Timeouts	Number of Virtual sessions removed due to session timer expiry.
Number of FCF Session Timeouts	Number of ACTIVE sessions timed out due to Discovery Advertisements expiry from FCFs in the VLAN.
Number of Session configuration failures	Number of sessions in the VLAN that failed to be configured in the hardware.
Number of Sessions denied with FCF limit	Number of sessions that are denied to be created for the new FCF as the number of FCFs reached the maximum allowed in the VLAN.
Number of Sessions denied with ENode limit	Number of session create requests that are denied for the new ENode as the number of ENodes reached the maximum allowed in the system.
Number of Sessions denied with System limit	Number of sessions that are denied to be created as the number of sessions reached the maximum allowed in the system.

When an interface is provided as an argument, interface applicable statistics are only displayed. See **Example #3** below for applicable statistics on interface.

Example #1

Example: Below is the sample command usage with no optional arguments supplied.

```
(switch)# show fip-snooping statistics
VLAN: 4
```

```
---------------------------------
FIP-Operation    Number of Pkts
VR               2
VN               2
MDS               2
UDS               2
FLOGI             2
FDISC             2
LOGO              0
VNPort-keep-alive 200
MDA               25
UDA               2
FLOGI_ACC         2
FLOGI_RJT         0
FDISC_ACC         2
FDISC_RJT         0
LOGO_ACC          0
LOGO_RJT          0
CVL               0
---------------------------------
Number of Virtual Session Timeouts:23
Number of FCF Session Timeouts:    6
Number of Session configuration failures: 10
Number of Sessions denied with FCF limit:  10
Number of Sessions denied with ENode limit:  10
Number of Sessions denied with System limit:   12

VLAN: 200
-------------------------------
FIP-Operation    Number of Pkts
VR               2
VN               2
MDS               5
UDS               4
FLOGI             5
FDISC             5
LOGO              1
VNPort-keep-alive 310
MDA               35
UDA               3
FLOGI_ACC         4
FLOGI_RJT         0
FDISC_ACC         15
FDISC_RJT         0
LOGO_ACC          1
LOGO_RJT          0
CVL               0
-------------------------------

Number of Virtual Session Timeouts:2
Number of FCF Session Timeouts:    0
Number of Session configuration failures: 10
Number of Sessions denied with FCF limit:  0
Number of Sessions denied with ENode limit:  0
Number of Sessions denied with System limit:   21
```

Example #2

Example: Below is the sample command output with optional VLAN argument supplied.

```
(switch)# show fip-snooping statistics vlan 200

VLAN: 200

--------------------------------
FIP-Operation    Number of Pkts
--------------------------------
VR               2
VN               2
MDS               5
UDS               4
FLOGI             5
FDISC             5
LOGO              1
VNPort-keep-alive 310
MDA               35
UDA               3
FLOGI_ACC         4
FLOGI_RJT         0
FDISC_ACC         15
FDISC_RJT         0
LOGO_ACC          1
LOGO_RJT          0
CVL               0
--------------------------------

Number of Virtual Session Timeouts:2
Number of FCF Session Timeouts:    0
Number of Session configuration failures: 10
Number of Sessions denied with FCF limit:  0
Number of Sessions denied with ENode limit:  0
Number of Sessions denied with System limit:   21
```

Example #3

Example: Below is the sample command output with optional interface argument supplied.

```
(switch)# show fip-snooping statistics interface 1/0/5

--------------------------------
FIP-Operation    Number of Pkts
--------------------------------
VR               2
VN               2
MDS               5
UDS               1
FLOGI             2
FDISC             5
LOGO              1
VNPort-keep-alive 310
MDA               35
UDA               3
FLOGI_ACC         4
FLOGI_RJT         0
FDISC_ACC         15
FDISC_RJT         0
LOGO_ACC          1
LOGO_RJT          0
```

```
CVL               0
--------------------------------

Number of Virtual Session Timeouts:2
Number of FCF Session Timeouts:    0
Number of Session configuration failures: 10
Number of Sessions denied with FCF limit:  0
Number of Sessions denied with ENode limit:  0
Number of Sessions denied with System limit:   21
```

6.4.0.10 show fip-snooping vlan

Use the **show fip-snooping vlan** command in User EXEC or Privileged EXEC mode to display the FCoE VLANs information and, additionally, the FIP snooping port status when optional argument is specified.

NOTE: This command can only be entered after FIP snooping is enabled using the **feature fip-snooping** command. Otherwise, it does not appear in the CLI syntax tree.

Format `show fip-snooping vlan [vlan-id]`

Mode
- User EXEC
- Privileged EXEC

Parameter	Description
vlan-id	A VLAN enabled for FIP snooping.
VLAN	VLAN in which FIP snooping is enabled/operational.
FC-MAP	FCoE mapped address prefix of the FCoE forwarder for the FCoE VLAN.
FCFs	Number of FCFs discovered.
ENodes	Number of ENodes discovered.
Sessions	Total virtual sessions in FCoE VLAN.

Example: The following shows example CLI display output for the command.

```
(switch)# show fip-snooping

Global Mode:   Enable
FCoE VLAN List :   2,4,5-8
FCFs   :   2
ENodes :   2
Sessions:   10
Max VLANs:   8
Max FCFs in VLAN:   4
Max ENodes:   312
Max Sessions:   1024
```

6.4.0.11 clear fip-snooping statistics

Use the **clear fip-snooping statistics** command in User EXEC or Privileged EXEC mode to clear the FIP Snooping statistics in the supplied VLAN or on a supplied interface. If the optional (VLAN or interface) argument is not given, this command clears the statistics on all FIP snooping-enabled VLANs.

NOTE: This command can only be entered after FIP snooping is enabled using the **feature fip-snooping** command. Otherwise, it does not appear in the CLI syntax tree.

Format `clear fip-snooping statistics [vlan vlan-id] | [interface interface-id]`

Mode
- User EXEC
- Privileged EXEC

Parameter	Description
vlan-id	A VLAN on which FIP snooping is enabled.
interface-id	An interface belonging to a VLAN on which FIP snooping is enabled.

6.5 Priority-Based Flow Control Commands

NOTE: Support for this feature is platform-dependent.

Ordinarily, when flow control is enabled on a physical link, it applies to all traffic on the link. When congestion occurs, the hardware sends pause frames that temporarily suspend traffic flow. Pausing traffic helps prevent buffer overflow and dropped frames.

Priority-based flow control (PFC) provides a way to distinguish which traffic on physical link is paused when congestion occurs, based on the priority of the traffic. An interface can be configured to pause only high priority (i.e., loss-sensitive) traffic when necessary prevent dropped frames, while allowing traffic that has greater loss tolerance to continue to flow on the interface.

Priorities are differentiated by the priority field of the IEEE 802.1Q VLAN header, which identifies an IEEE 802.1p priority value. In EFOS, these priority values must be mapped to internal class-of-service (CoS) values.

To enable priority-based flow control for a particular CoS value on an interface:

1. Ensure that VLAN tagging is enabled on the interface so that the 802.1p priority values are carried through the network (see Section 5.8, Provisioning (IEEE 802.1p) Commands).
2. Ensure that 802.1p priority values are mapped to EFOS CoS values (see Section 12.1.0.1, classofservice dot1p-mapping).

When priority-flow-control is disabled, the interface defaults to the IEEE 802.3x flow control setting for the interface. When priority-based flow control is enabled, the interface will not pause any CoS unless there is at least one no-drop priority.

6.5.0.1 priority-flow-control mode

Use the **priority-flow-control mode on** command in Datacenter-Bridging Config mode to enable Priority-Flow-Control (PFC) on the given interface.

Use the **no** form of the command to return the mode to the default (off). VLAN tagging (trunk or general mode) must be enabled on the interface in order to carry the dot1p value through the network. Additionally, the dot1mapping to class-of-service must be set to one-to-one.

When PFC is enabled on an interface, the normal PAUSE control mechanism is operationally disabled.

Default Priority-flow-control mode is off (disabled) by default.

Format `priority-flow-control mode { on | off }`

Mode Datacenter-Bridging Config mode

Parameter	Description
on	Enable PFC on the interface.
off	Disable PFC on the interface.

Example: The following example enables PFC on an interface.

```
(Routing) (Config)#interface 0/1
(Routing) (Interface 0/1)#datacenter-bridging
(Routing) (config-if-dcb)#priority-flow-control mode on
```

6.5.0.1.1 no priority-flow-control mode

Use the **no priority-flow-control mode** command to return the PFC mode to the default (**off**).

Format `no priority-flow-control mode`
Mode Datacenter-Bridging Config mode

6.5.0.2 priority-flow-control priority

Use the **priority-flow-control priority** command in Datacenter-Bridging Config mode to enable the priority group for lossless (no-drop) or lossy (drop) behavior on the selected interface. Up to two lossless priorities can be enabled on an interface. The administrator must configure the same no-drop priorities across the network in order to ensure end-to-end lossless behavior.

The command has no effect on interfaces not enabled for PFC. VLAN tagging needs to be turned on in order to carry the dot1p value through the network. Additionally, the dot1pmapping to class of service must be set to one to one.

Default The default behavior for all priorities is drop.
Format **`priority-flow-control priority`** ***`priority-list`*** **`{drop | no-drop}`**
Mode Datacenter-Bridging Config mode

Parameter	Description
drop	Disable lossless behavior on the selected priorities.
no-drop	Enable lossless behavior on the selected priorities.

Example: The following example sets priority 3 to no drop behavior.

```
(Routing) (Config)#interface 0/1
(Routing) (Interface 0/1)#datacenter-bridging
(Routing) (config-if-dcb)#priority-flow-control mode on
(Routing) (config-if-dcb)#priority-flow-control priority 1 no-drop
```

6.5.0.2.1 no priority-flow-control priority

Use the **no priority-flow-control priority** command in Datacenter-Bridging Config mode to enable lossy behavior on all priorities on the interface. This has no effect on interfaces not enabled for PFC or with no lossless priorities configured.

Format **`no priority-flow-control priority`**
Mode Datacenter-Bridging Config mode

6.5.0.3 clear priority-flow-control statistics

Use the **clear priority-flow-control statistics command to clear all global and interface** PFC statistics.

Format **`clear priority-flow-control statistics`**
Mode Privileged EXEC

Example: The following shows examples of the commands.

```
(Routing) #clear priority-flow-control statistics
```

6.5.0.4 show interface priority-flow-control

Use the **show interface priority-flow-control** command in Privileged EXEC mode to display the PFC information of a given interface or all interfaces.

Format `show interface [slot/port] priority-flow-control`

Mode Privileged EXEC

Parameter	Description
slot/port	A valid Ethernet port.

When an interface number is not provided, the following information displays for all interfaces.

Parameter	Description
Interface Detail	The port for which data is displayed.
PFC Operational Status	The operational status of the interface.
PFC Configured State	The administrative mode of PFC on the interface.
Configured Drop Priorities	The 802.1p priority values that are configured with a drop priority on the interface. Drop priorities do not participate in pause.
Configured No-Drop Priorities	The 802.1p priority values that are configured with a no-drop priority on the interface. If an 802.1p priority that is designated as no-drop is congested, the priority is paused.
Operational Drop Priorities	The 802.1p priority values that the switch is using with a drop priority. The operational drop priorities might not be the same as the configured priorities if the interface has accepted different priorities from a peer device
Configured No-Drop Priorities	The 802.1p priority values that the switch is using with a no-drop priority. The operational drop priorities might not be the same as the configured priorities if the interface has accepted different priorities from a peer device
Delay Allowance	The operational status of the interface.
Peer Configuration Compatible	Indicates whether the local switch has accepted a compatible configuration from a peer switch.
Compatible Configuration Count	The number of received configurations accepted and processed as valid. This number does not include duplicate configurations.
Incompatible Configuration Count	The number of received configurations that were not accepted from a peer device because they were incompatible.
Priority	The 802.1p priority value.
Received PFC Frames	The number of PFC frames received by the interface with the associated 802.1p priority.
Transmitted PFC Frames	The number of PFC frames transmitted by the interface with the associated 802.1p priority.

Example: The following examples show the priority flow control status and statistics.

Example #1:

```
(Routing) #show interface 0/1 priority-flow-control

Interface Detail:                0/1
PFC Configured State:            Disabled
PFC Operational State:            Enabled
Configured Drop Priorities:        2-7
Operational Drop Priorities:       2-7
Configured No-Drop Priorities:     0-1
```

```
Operational No-Drop Priorities:  0-1
Delay Allowance:                 32456 bit times
Peer Configuration Compatible:     True
Compatible Configuration Count:    3
Incompatible Configuration Count:  1

Priority  Received PFC Frames     Transmitted PFC Frames
--------  ---------------------    ----------------------
0         0                       0
1         0                       0
2         0                       0
3         0                       0
4         0                       0
5         0                       0
6         0                       0
7         0                       0
```

Example #2:

```
(Routing) #show interface priority-flow-control

Port   Drop      No-Drop      Oper
       PrioritiesPriorities   State
------ ---------- ----------  -----
0/1    1-4,7     5,6          Enabled
0/2    1-4,6-7   5            Enabled
….
0/48   1-4,7     5,6          Enabled
```

6.6 OpenFlow Commands

The OpenFlow feature enables the switch to be managed by a centralized OpenFlow Controller using the OpenFlow protocol.

6.6.0.1 openflow enable

This command enables the OpenFlow feature. If the OpenFlow feature is not in disabled state, then issuing this command has no effect on the OpenFlow feature.

Default	Disabled
Format	`openflow enable`
Mode	Global Config

6.6.0.1.1 no openflow enable

This command disables the OpenFlow feature. If the OpenFlow feature is not in enabled state, then issuing this command has no effect on the OpenFlow feature. The OpenFlow feature can be administratively disabled at any time.

Format	`no openflow enable`
Mode	Global Config

6.6.0.2 openflow static-ip

This command sets the IP address to be used for the OpenFlow feature. The static IP is applied only when the static IP mode is enabled. The switch must have an operational IP interface with the specified address in order for the static IP address to be used for the OpenFlow feature. If the system does not have an interface with a matching IP address then the OpenFlow feature is operationally disabled.

If the OpenFlow feature is enabled when this command is issued and the specified static IP address is not the same as the IP address already in use by the OpenFlow feature then the feature is automatically disabled and re-enabled.

Default	0.0.0.0
Format	`openflow static-ip` *`IPv4 Address`*
Mode	Global Config

6.6.0.2.1 no openflow static-ip

This command sets the OpenFlow static IP address to 0.0.0.0. Issuing this command when OpenFlow is enabled and using a static IP causes the OpenFlw feature to become operationally disabled.

Format	`no openflow static-ip`
Mode	Global Config

6.6.0.3 openflow controller

Specify up to twenty IP addresses to which the switch should establish an OpenFlow Controllers connection. Each command invocation specifies one IP address and connection mode (TCP or SSL). If the IP Port is omitted then the default IP port number 6633 is used. The default connection mode is SSL. The controller table configured by this command is used by the switch in OpenFlow 1.0/1.3 modes.

Format `openflow controller` *`ip-address`* `[`*`ip-port`*`] [`*`connection mode`*`]`
Mode Global Config

Parameter	Description
ip-address	Specify up to five IP addresses to which the switch should establish an OpenFlow Management connection.
ip-port	IP port to use for an OpenFlow Management connection. If the IP Port is omitted, then the default IP port number 6632 is used.
connection mode	TCP or SSL. The default is SSL.

6.6.0.3.1 no openflow controller

Delete the specified OpenFlow Controller IP address or delete all Controller addresses. If the IP Port number is omitted then all entries for the specified IP address are deleted.

Format `no openflow controller {`*`ip-address`* `[`*`ip-port`*`] | all}`
Mode Global Config

6.6.0.4 openflow default-table

Configure the Hardware Table used as the target for flows installed by an OpenFlow 1.0 controller which is not enhanced to handle multiple hardware tables. The parameter is applicable only when the OpenFlow variant is set to **OpenFlow 1.0**.

Default full-match
Format `openflow default-table` *`parameter`*
Mode Global Config

Parameter	Description
parameter	Possible values are **full-match** or **layer-2-match**.

6.6.0.5 openflow ip-mode

This command directs the OpenFlow feature to use the configured IP address. Issuing this command when OpenFlow is already enabled causes the feature to be disabled and re-enabled with the new IP address.

Default Disabled
Format `openflow ip-mode {auto|static|serviceport}`
Mode Global Config

6.6.0.5.1 no openflow ip-mode

This command directs the OpenFlow feature to automatically assign the IP address to itself.

Format	`no openflow ip-mode`
Mode	Global Config

6.6.0.6 openflow passive-mode

This command enables OpenFlow passive-mode.

Default	Disabled
Format	`openflow passive-mode`
Mode	Global Config

6.6.0.6.1 no openflow passive-mode

This command disables OpenFlow passive-mode.

Format	`no openflow ip-mode`
Mode	Global Config

6.6.0.7 openflow variant

This command configures the OpenFlow feature to the specified variant. You can configure the OpenFlow feature to use one of two variants, **OpenFlow 1.0** or **OpenFlow 1.3**. The OpenFlow feature is configured to **OpenFlow 1.3** by default.

Default	OpenFlow 1.3
Format	`openflow variant` *`openflow10`*|*`openflow13`*
Mode	Global Config

6.6.0.8 clear openflow ca-cert

This command erases the Certificate Authority certificates used for validating the OpenFlow Controllers from the switch. Issuing this command automatically disables and re-enables the OpenFlow feature. The new SSL certificates are reloaded from the OpenFlow Controller on the first connection to the controller or can be manually loaded with a copy command.

Format	`clear openflow ca-cert`
Mode	Privileged EXEC

6.6.0.9 show openflow

This command displays the OpenFlow feature status and configuration information.

Format	`show openflow`
Mode	Privileged EXEC

Parameter	Description
Administrative Mode	The OpenFlow feature administrative mode set by the Section 6.6.0.1, openflow enable command.
Administrative Status	The operational status of the OpenFlow feature. Although the feature may be administratively enabled, it could be operationally disabled due to various reasons.
Disable Reason	If the OpenFlow feature is operationally disabled, then this status shows the reason for the feature to be disabled.
IP Address	IPv4 Address assigned to the feature. If the IP address is not assigned, then the status is **None**.
IP Mode	IP mode assigned by the Section 6.6.0.5, openflow ip-mode command. The IP mode can be **Auto**, **Static**, or **ServicePort IP**.
Static IP Address	Static IP address assigned by the Section 6.6.0.2, openflow static-ip command.
OpenFlow Variant	OpenFlow Protocol Variant. The OpenFlow protocol can be **OpenFlow 1.0** or **OpenFlow 1.3**.
Default Table	The Hardware Table used as the target for flows installed by an OpenFlow 1.0 controller which is not enhanced to handle multiple hardware tables.
Passive Mode	The OpenFlow passive mode set by the Section 6.6.0.6, openflow passive-mode command.

Example: The following shows example CLI display output for the command.

```
(Routing) #show openflow

Administrative Mode.......................... Enable
Administrative Status........................ Disabled
Disable Reason............................... No-Suitable-IP-Interface
IP Address................................... None
IP Mode...................................... Auto
Static IP Address............................ 10.1.1.1
OpenFlow Variant............................. Tenant Networking
Default Table................................ layer-2-match
Passive Mode................................. Enable
```

Example: The following shows example CLI display output for the command.

```
(Routing) #show openflow

Administrative Mode.......................... Enable
Administrative Status........................ Enabled
Disable Reason............................... None
IP Address................................... 10.27.65.64
IP Mode...................................... Auto
Static IP Address............................ 10.1.1.1
OpenFlow Variant............................. OpenFlow 1.0
Passive Mode................................. Enable
```

6.6.0.10 show openflow configured controller

This command displays a list of configured OpenFlow Controllers. The switch communicates with these controllers only when the OpenFlow variant is 1.0 or 1.3.

Format `show openflow configured controller`

Mode Privileged EXEC

Parameter	Description
IP Address	IPv4 address of the controller.

Parameter	Description
IP Port	IPv4 port number for the controller connection.
Connection Mode	SSL or TCP Controller Connection mode.
Role	The role of the controller: Master, Equal, Slave

Example: The following shows example CLI display output for the command.

```
(Routing) # show openflow configured controller

IP Address    IP Port  Connection Mode    Role
------------  -------  ---------------    ------
172.21.4.217  6633     SSL                Master
```

6.6.0.11 show openflow installed flows

This command displays the list of configured flows on the switch.

Format `show openflow installed flows [dest_ip` *`ip-address`* `| dest_ip_port` *`1-65535`* `| dest_mac` *`macaddr`* `| dscp` *`0-63`* `| ether_type` *`0-0xFFFF`* `| ingress_port` *`slot/port`* `| ip_proto` *`0-255`* `| priority` *`1-65535`* `| source_ip` *`ip-address`* `| source_ip_port` *`1-65535`* `| source_mac` *`macaddr`* `| table` *`4,24,25`* `| vlan` *`1-4093`* `| vlan_prio` *`0-7`*`]`

Mode Privileged EXEC

Parameter	Description
dest_ip	The IP address of the destination.
dest_ip_port	The port number of the destination.
dest_mac	The MAC address of the destination.
dscp	The DSCP value.
ether_type	The ethertype value.
ingress_port	The slot and port for the ingress.
ip_proto	The IP protocol.
priority	The priority of the flow.
source_ip	The IP address of the source.
source_ip_port	The port number of the source.
source_mac	The MAC address of the source.
table	The table number.
vlan	The VLAN.
vlan_prio	The VLAN priority.

Parameter	Description
Flow Type	The type of flow. (For example, 1.0 or Layer 2 Match).
Flow Table	The hardware table in which the flow is installed.
Flow Priority	The priority of the flow versus other flows.
Match Criteria	The match criteria specified by the flow.
Ingress Port	The port on which the flow is active.
Action	The action specified by the flow.

Parameter	Description
Idle	The time since the flow was hit.
Installed in hardware	If the flow could be added to the hardware. ■ 0 is displayed if the flow cannot be added. ■ 1 is displayed if the flow was added.
Hard Timeout	The number of seconds after which the flow is expired regardless of whether or not packets are hitting the entry.
Idle Timeout	The number of seconds after which the flow is expired with no received traffic.
Queue	The queue that should be used to queue when packets are output.

Example: The following shows example CLI display output for the command for the flow type 1DOT0.

```
(Routing) #show openflow installed flows

Flow type "1DOT0"

Match criteria:
Flow table              24 : Priority                1
Ingress port           0/0
Actions:
Action:               Drop
Status:
Duration                 2 : Idle                    0 : installed in hardware    1

Flow type "1DOT0"

Match criteria:
Flow table              24 : Priority              102
Ingress port           0/0 : Ether type           88CC
Actions:
Status:
Duration                55 : Idle                   45 : installed in hardware    1
```

Example: The following shows example CLI display output for the command for the flow type 1DOT3.

```
(Routing) # show openflow installed flows

Flow type "1DOT3"

Match criteria:
Flow table         60 : Priority           10
Ingress port      0/1 : Src MAC  00:00:02:37:38:01 : Dst MAC  00:00:18:37:22:01
VLAN                1 : VLAN prio           1 : Ether type          0x0800
IP proto           17 : Src IP     100.0.0.225 : Dst IP        192.0.0.225
Src IP port         1 : Dst IP port         1 : TOS                32(DSCP: 8)

Actions:
New Src IP         3.3.3.3 : New SrcIP Mask 255.255.255.255 : New Dst IP         4.4.4.4
New DstIP Mask 255.255.255.255 : Egress port       0/1
Status:
Duration            5 : Idle                2 : installed in hardware  1

Flow type "1DOT3"

Match criteria:
Flow table         60 : Priority        32768
Dst MAC  00:00:00:00:00:55 : Dst MAC Mask FF:FF:FF:FF:FF:FF : VLAN              100
```

```
VLAN Mask        4095
Actions:
New VLAN          102 : Queue           3
Egress port       0/2

Hard Timeout        0 : Idle Timeout        0

Status:
Duration            5 : Packet Count                      0 : Byte Count                          0
Idle                0 : installed in hardware  0
```

6.6.0.12 show openflow installed groups

Use this command to display the list of configured groups on the switch.

Format `show openflow installed groups`

Mode Privileged EXEC

Parameter	Description
Group Type	Type of the Group – Indirect, All, Select etc.
Group Id	Unique Id of the Group
Reference Count	Group Reference Count - is used only for Indirect groups. This count indicates how many Select groups are referring to the current Indirect group
Duration	The time since the group was created
Bucket Count	Number of Buckets in the group
Reference Group Id	References the Indirect group ID and used for Select group only

Example:

```
(Routing) # show openflow installed groups

Max Indirect Group Entries.....................................  1234
Current Indirect Group Entries in database.....................  123

Max All Group Entries..........................................  1234
Current All Group Entries in database..........................  123

Max Select Group Entries.......................................  1234
Current Select Group Entries in database.......................  123

Group Id 12345678 type "Indirect"
=================================

Ref Count              1 : Duration            8 : Bucket Count     1

Bucket Entry List:
------------------

Bucket Index         25 : Output Port            1
Src MAC  00:00:00:00:00:AB : Dst MAC  00:00:00:00:00:CD
VLAN              101 : Reference Group Id      NA
```

```
Group Id 23456789 type "All"
============================
Ref Count              NA : Duration            10 : Bucket Count     2

Bucket Entry List:
------------------
Bucket Index          26 : Output Port           2
Src MAC               NA : Dst MAC              NA
VLAN                 102 : Reference Group Id    NA

Bucket Index          27 : Output Port           3
Src MAC               NA : Dst MAC              NA
VLAN                 103 : Reference Group Id    NA

Group Id 34567890 type "Select"
===============================
Ref Count              NA : Duration            10 : Bucket Count     3

Bucket Entry List:
------------------

Bucket Index          28 : Output Port          NA
Src MAC               NA : Dst MAC              NA
VLAN                  NA : Reference Group Id    12345678

Bucket Index          29 : Output Port          NA
Src MAC               NA : Dst MAC              NA
VLAN                  NA : Reference Group Id    12345678

Bucket Index          30 : Output Port          NA
Src MAC               NA : Dst MAC              NA
VLAN                  NA : Reference Group Id    12345678
```

6.6.0.13 show openflow table-status

This command displays the supported OpenFlow tables and report usage information for the tables.

Format `show openflow table-status {openflow10|opnflow13)`

Mode Privileged EXEC

Parameter	Description
Flow Table	OpenFlow table identifier. The range is 0 to 255.
Flow Table Name	The name of this table.
Flow Table Description	A detailed description for this table.
Maximum Size	Platform-defined maximum size for this flow table.
Number of Entries	Total number of entries in this table. The count includes delete-pending entries.
Hardware Entries	Number of entries currently inserted into the hardware.
Software-Only Entries	Number of entries that are not installed in the hardware for any reason. This includes entries pending for insertion, entries that cannot be inserted due to missing interfaces and entries that cannot be inserted due to table-full condition.
Waiting for Space Entries	Number of entries that are not currently in the hardware because the attempt to insert the entry failed.

Parameter	Description
Flow Insertion Count	Total number of flows that were added to this table since the switch powered up.
Flow Deletion Count	Total number of flows that were deleted from this table since the switch powered up.
Insertion Failure Count	Total number of hardware insertion attempts that were rejected due to lack of space since the switch powered up.

Example: The following shows example CLI display output for the command.

```
(Routing) # show openflow table-status openflow10

Flow Table.............................1
Flow Table Name..... Forwarding Database
Maximum Size...........................64
Number of Entries.....................8
Hardware Entries......................7
Software-Only Entries.................1
Waiting for Space Entries.............0
Flow Insertion Count..................1
Flow Deletion Count...................0
Insertion Failure Count...............0
Flow Table Description:
The forwarding database maps non-multicast MAC addresses and the ports on which these addresses are
located.
```

Example: The following shows example CLI display output for the command.

```
(Routing) #show openflow table-status openflow13
Flow Table.................................. 60
Flow Table Name............................. Openflow 1.3
Maximum Size................................ 1920
Number of  Entries.......................... 0
Hardware Entries............................ 0
Software-Only Entries....................... 0
Waiting for Space Entries................... 0
Flow Insertion Count........................ 0
Flow Deletion Count......................... 0
Insertion Failure Count..................... 0
Flow Table Description..................... The Openflow 1.3 table matches on the packet layer-2
header, including DA-MAC, SA-MAC, VLAN, Vlan priority ether type; layer-3 header, including SRC-IP,
DST-IP, IP protocol, IP-TOS; layer-4 header, including UDP/TCP source and dest port, ICMP type, and
code; SRC-IPv6, DST_IPv6, IPv6 Flow Label,ECN, ICMPv6 type and code, source L4 Port for TCP / UDP /
SCTP and input port including physical port and LAG port.
```

6.7 MPLS Commands

This section describes the MPLS commands for the data center.

6.7.0.1 mplsd bgp-advertise

Use this command to enable or disable the BGP protocol from sending MPLS labels. The per-switch label and the per-interface label distribution is affected by this command. When bgp-advertise mode is disabled, the BGP protocol does not advertise the label distribution capability to the BGP neighbors. The default is enabled.

Format `mplsd bgp-advertise`
Mode Global Config

6.7.0.1.1 no mplsd bgp-advertise

Use this command to disable MPLS label advertisement mode.

Format `no mplsd bgp-advertise`
Mode Global Config

6.7.0.2 mplsd lfdb ipv4

Use this command to create a new label in the label forwarding database. The label is associated with an IPv4 network.

The swap command transmits the packet with the same label as it was received. The same label is used because the switches associate one label to one subnet in the entire routing domain.

The pop command strips the top label from the label stack.

The last-pop command strips the top label from the label stack and sends the packet without the MPLS header.

Format `mplsd lfdb ipv4 label <swap | pop | last-pop> ipv4address/prefix-length>`
Mode Global Config

6.7.0.3 mplsd lfdb ipv6

Use this command to create a new label in the label forwarding database. The label is associated with an IPv6 network.

The swap command transmits the packet with the same label as it was received. The same label is used because the switches associate one label to one subnet in the whole routing domain.

The pop command strips the top label from the label stack. The last-pop command strips the top label from the label stack and sends the packet without the MPLS header.

Format `mplsd lfdb ipv4 label <swap | pop | last-pop> ipv4address/prefix-length>`
Mode Global Config

6.7.0.4 mplsd lfdb layer-2

Use this command to create a new label in the label forwarding database. The label is associated with the specified egress interface and MAC address. The egress interface may be a physical port, a port-based routing interface, or a LAG.

Note that the swap-label parameter is applicable only if the swap option is selected. The other parameters are present for all options. The pop option strips the top label from the label stack. The last-pop option strips the top label from the label stack and sends the packet without the MPLS header.

Format `mplsd lfdb layer-2 label {swap | pop | last-pop} {swap-label} slot/port vlan mac-addr`
Mode Global Config

6.7.0.4.1 no mplsd lfdb

Use this command to delete either one label or multiple labels in the label range from the label forwarding database.

Format `no mplsd lfdb layer-2 label [-last-label]`
Mode Global Config

6.7.0.5 mplsd bgp-mpls-label

Use this command to enable BGP to distribute the specified label for the specified routing interface. The label is associated with the primary IPv4 address assigned to the interface.

The command may be invoked for port-based and VLAN routing interfaces to assign per-interface labels. The command may be invoked for the loopback interfaces to assign the per-switch labels. This command is not supported for the tunnel interfaces.

Format `mplsd bgp-mpls-label label`
Mode Interface Config

6.7.0.5.1 no mplsd bgp-mpls-label

Use this command to disable MPLS label distribution associated with the IPv4 address for the specified routing interface.

Format `no mplsd bgp-mpls-label`
Mode Interface Config

6.7.0.6 ipv6 mplsd bgp-mpls-label

Use this command to enable BGP to distribute the specified label for the specified routing interface. The label is associated with the primary IPv6 address assigned to the interface.

This command may be invoked for port-based and VLAN routing interfaces. This command is not supported for tunnel interfaces.

Format `ipv6 mplsd bgp-mpls-label label`
Mode Interface Config

6.7.0.6.1 no ipv6 mplsd bgp-mpls-label

Use this command to disable MPLS label distribution associated with the IPv6 address for the specified routing interface.

Format `no ipv6 mplsd bgp-mpls-label`
Mode Interface Config

6.7.0.7 clear counters mplsd

Use this command to reset the MPLS counters to zero. This includes global counters and per-label counters.

Format `clear counters mplsd`
Mode Global Config

6.7.0.8 debug mplsd packet-capture

Use this command to enable hardware to capture packets that match the specified criteria. Label filtering for label-1 is done in hardware. Label filtering for label-2 and label-3 is done in software. Packets that match the capture criteria are logged in the syslog.

The label parameters are accepted only if the packet type is mpls.

If a packet capture session is already active when the command is issued, the previous session is terminated and a new session is started.

Format `debug mplsd packet-capture [USP | any-port] [mpls | any-packet-type] [label-1] [label-2] [label-3]`
Mode Interface Config

6.7.0.8.1 no debug mplsd packet-capture

Use this command to disable packet capture.

Format `no debug mplsd packet-capture`
Mode Interface Config

6.7.0.9 show mplsd

Use this command to display the global status of the MPLS feature.

Format `show mplsd`
Mode Global Config

Parameter	Description
MPLS MAC	The MAC address that MPLS packets to this switch must use for the switch to handle the packets.
BGP Label Distribution Mode	Flag indicating whether BGP is configured to distribute per-switch and per-interface MPLS labels.
LFDB Size	Maximum number of entries in the Label Forwarding Database.

Parameter	Description
Maximum number of MPLS tunnel initiators	Maximum number of tunnel initiators supported in hardware
Current number of MPLS tunnel initiators	Current number of tunnel initiators in the hardware
LFDB Label Range	The MPLS label IDs supported by the switch.
Number of MPLS tunnels with 1-label	The current number of MPLS tunnels with one-label encapsulation
Number of MPLS tunnels with 2-labels	The current number of MPLS tunnels with two-label encapsulation
Number of MPLS tunnels with 3-labels	The current number of MPLS tunnels with three-label encapsulation
LFDB Entries	The number of MPLS labels currently in the database.
LFDB Entries In Hardware	The number of MPLS labels currently inserted in the hardware.
LFDB Entries Not In Hardware	The number of MPLS labels in the LFDB, that are currently not inserted into the hardware.
LFDB Static Entries	The number of LFDB entries added by the static protocol, which means these labels are saved in the configuration file.
LFDB Dynamic Entries	Number of LFDB entries added by the Dynamic protocol. These entries can be added via Open API or SNMP.
LFDB BGP Entries	Number of LFDB entries added by the BGP protocol.
LFDB Layer-2 Entries	Number of layer 2 entries currently in the LFDB.
LFDB IPv4 Entries	Number of IPv4 entries currently in the LFDB.
LFDB IPv6 Entries	Number of IPv6 entries currently in the LFDB.
LFDB Dynamic Insert Failure Count	Number of failed LFDB insertion attempts from the BGP protocol or from the dynamic protocol.
LFDB High Watermark	The maximum number of LFDB entries that was ever added to the database since the last time the counters were cleared.
ECMP In-Use/High/Max	The current number, the high watermark, and the maximum size of the ECMP database. The In-Use and High counts include the entries used by the routing feature as well as the MPLS feature.
LFDB Lookup Failure Packets	The number of MPLS packets received by the switch that did not match any MPLS entry in the hardware label forwarding database.

Example:

```
#show mplsd

MPLS MAC..................................... 70:72:CF:A3:C5:62
BGP Label Distribution Mode.................. Enabled
LFDB Size.................................... 14336
Maximum number of MPLS tunnel initiators.....20448
Current number of MPLS tunnel initiators.....2
LFDB Label Range............................. 16 - 1048575
Number of MPLS tunnels with 1-label..........20
Number of MPLS tunnels with 2-label..........0
Number of MPLS tunnels with 3-label..........0
LFDB Entries................................. 1012
LFDB Entries In Hardware..................... 1012
LFDB Entries Not In hardware................. 0
LFDB Static Entries.......................... 1012
LFDB Dynamic Entries......................... 0
LFDB BGP Entries............................. 0
LFDB Layer-2 Entries......................... 0
```

```
LFDB IPv4 Entries.............................. 1012
LFDB IPv6 Entries.............................. 0
LFDB Dynamic Insert Failure Count.............. 0
LFDB High Water Mark........................... 1012
ECMP In-Use/High/Max........................... 1013/1016/1024
LFDB Lookup failure packets.................... 63135103
```

6.7.0.10 show mplsd lfdb

Use this command to display the configuration and status of MPLS labels in the label forwarding database. This command can filter on particular label types or on a specific label or range of labels.

Format `show mpls lfdb {all | bgp | dynamic | ipv4 | ipv6 | layer-2 | static} | {label[-label]}`

Mode Global

Parameter	Description
Label	The MPLS Label.
Protocol	Which protocol added the label, such as BGP, Static, and Dynamic. The Dynamic entries can only be created via SNMP and Open API.
Type	The type of label, such as ipv4, ipv6, or layer-2.
Subnet	The subnet associated with this label. For layer-2 labels, this field is set to N/A.
Egress Label Action	Label action, such as swap, pop, and last-pop.
Egress Label	For entries with swap actions this is the label used to replace the top label in the MPLS stack.
Egress Port	For layer-2 entries, this is the egress port on which the packet is transmitted. The field is N/A for IPv4 and IPv6 entries.
Vlan	For layer-2 entries, this is the VLAN with which the packets are transmitted. The field is N/A for IPv4 and IPv6 entries.
MAC	For layer-2 entries, this is the MAC address appended to the transmitted MPLS packets. The field is N/A for IPv4 and IPv6 entries.
Hardware Status	This flag indicates whether the label is inserted into the hardware.
Not Inserted Reason	If the label is not inserted into the hardware, this field displays the reason for not inserting the label.
Byte Count	A 64 bit counter that counts the number of bytes received by the switch that match this MPLS label.
Packet Count	A 64 bit counter that counts the number of packets received by the switch that match the MPLS label.
Duplicate Insertion Attempts	The number of times an attempt was made to insert this label when the label was already in the database.

Example:

```
#show mplsd lfdb label 3000

Label:3000  Protocol:Static  Type:ipv4  Subnet:30.0.1.0/24
     Egress Label Action:swap  Egress Label:N/A
     Egress Port:N/A  Vlan:N/A  MAC:N/A
     Hardware Status:Inserted  Not Inserted Reason:N/A
     Byte Count:91797199811712  Packet Count:717165623021
     Duplicate Insertion Attempts:0
```

6.7.0.11 show mplsd interface

Use this command to display the configured MPLS labels distributed by the BGP protocol for IPv4 and IPv6 interfaces. When the all option is specified, the command displays all interfaces that have a configured MPLS label for either the IPv4 or IPv6 interface.

Format `show mplsd interface {all | USP | vlan | loopback}`
Mode Global

Parameter	Description
Interface	USP of the interface.
IPv4 MPLS Label	MPLS Label associated with the primary IPv4 address. The field reports None if no label is assigned for IPv4.
IPv6 MPLS Label	MPLS label associated with the primary IPv6 address.

Example:

```
#show mplsd interface vlan 100

Interface: 4/1 (VLAN- 100)
IPv4 MPLS Label: 100
IPv6 MPLS Label: 110

#show mplsd interface vlan 101

Interface: 4/2 (VLAN- 101)
IPv4 MPLS Label: 200
IPv6 MPLS Label: None
```

6.7.0.12 show mplsd tunnels

This command displays the MPLS tunnel initiator table. The command can filter on particular label types or on a specific label or range of labels.

When the `all` option is specified, the command displays all tunnel initiators which are configured for either IPv4 or IPv6.

Format `show mplsd tunnels {all | ipv4 | ipv6 | label [`*`label`*`]}`
Mode Global

Parameter	Definition
Label	The MPLS Label.
Type	The type of label, such as ipv4, ipv6 or all
IP address	The IPv4 or IPv6 address of the next hop with which this tunnel is associated.
MPLS Label-1	The top MPLS label of the tunnel.
MPLS Label-2	The second MPLS label of the tunnel.
MPLS Label-3	The third MPLS label of the tunnel.
Egress Interface	The interface index to which this tunnel entry is pointing. The value is displayed as U/S/P or LAG-n format.
Egress VLAN	VLAN on which the packets egress the switch. Port based routing interfaces report the internal MPLS tunneling VLAN.

Parameter	Definition
Egress MAC	MAC address used as the destination MAC for packets transmitted on this MPLS tunnel.
Reference Count	Number of routes and ECMP groups pointing to this MPLS tunnel initiator.
Age since last update	Number of seconds since last update.

Example:

```
(Routing) #show mplsd tunnels all

Nexthop IP: 172.16.6.1
     MPLS Label(s): 10001
     Egress Physical Port:0/49  Vlan:4093  MAC:70:72:CF:A3:C5:63
     Seconds since last update:2208  Reference Count:1
Nexthop IP: 172.16.6.3
     MPLS Label(s): 10001
     Egress Physical Port:0/47  Vlan:4093  MAC:C4:54:44:43:8F:4D
     Seconds since last update:2208  Reference Count:1
```

6.8 NVGRE/VXLAN Commands

This section lists the commands that enable the network virtualization technologies (VXLAN/NVGRE) to communicate with another network.

6.8.0.1 nvgre enable

Use this command to enable the NVGRE mode on the switch. NVGRE mode must be enabled prior to performing any NVGRE configuration on the switch. The default is disabled.

NOTE: VXLAN mode and NVGRE mode are mutually exclusive modes. NVGRE mode cannot be enabled if VXLAN mode is enabled on the switch. VXLAN mode must be disabled prior to enabling NVGRE mode.

Format `nvgre enable`
Mode Global Config

6.8.0.1.1 no nvgre enable

Use this command to disable the NVGRE mode on the switch. This command also clears all the existing NVGRE configurations on the switch, which includes all NVGRE tunnels, tenants, tenant VLAN associations, and configured forwarding entries.

Format `no nvgre enable`
Mode Global Config

6.8.0.2 nvgre nve

Use this command to specify the IP address of another network virtualization endpoint (NVE) in the virtual network with the given virtual subnet ID (VSID). If the virtual network identified by the VSID has not already been created, it is created when this command is issued. The user can create a maximum of 1024 DCVPNs on the switch.

Multiple remote NVEs can be configured one by one for the same VSID, as required.

NOTE: The switch does support configuration of Multicast IP address to discover remote NVEs automatically to define a flood group for DCVPN. This command should be used to manually configure all remote NVEs behind which Tenant (VSID) hosts are present for each DCVPN.

The user can optionally specify one or more tenant systems reachable through the NVE. The tenant systems for a particular VN can be added or deleted incrementally one by one. Normally, the system automatically learns tenant systems from received messages. If a tenant system is configured, the configuration overrides learning for the given MAC address.

The tenant system MAC addresses are maintained in a separate table. These are not listed as part of FDB mac-address table. They internally consume shared system hardware layer 2 address table resources. So the maximum number of tenant systems depends on the number of resources left in the hardware layer 2 table, which is dynamic in nature.

The user is allowed to configure a maximum of 600 remote tenant system entries per VN and overall 4096 entries on the switch.

The configurable range for the VSID 1 to 16777214. 16777215 is reserved for internal purposes.

Default By default, no NVEs are associated with the VSID.

Format `nvgre vsid nve ip-address [tenant-system mac-addr]`
Mode Global Config

6.8.0.2.1 no nvgre nve

Use this command to remove a remote NVE from the specified virtual network identified by the specified virtual subnet ID (VSID). This also clears all tenant system MAC address associations with specified NVE and DCVPN from the system. If the `tenant-system mac-addr` option is specified, this command deletes the manual association of a tenant system to a remote NVE. This command cannot be used to delete a dynamically-learned tenant system.

Format `no nvgre vsid nve ip-address [tenant-system mac-addr]`
Mode Global Config

6.8.0.3 nvgre source-ip

Use this command to specify the outer source IP address for encapsulated packets sent on a NVGRE with a given virtual subnet ID (VSID). The source-ip is the intended local NVE for the specified tenant specified with vsid. If no VN with the given vsid exists, the system creates it.

The configurable range for the VSID 1 to 16777214. 16777215 is reserved for internal purposes.

NOTE: It is recommended to configure a loopback interface with the intended local NVGRE Gateway IP address and use it as the source-ip for all tenants. It is also possible to configure tenants with a different source-ip when multiple loopback interfaces are configured and used as local NVGRE Gateways, if required. Loopback interfaces that are intended to be used as local NVGRE Gateways, should be dedicated interfaces and must not be used for any other purposes.

Default No source is set.
Format `nvgre vsid source-ip ip-address`
Mode Global Config

6.8.0.3.1 no nvgre source

Use this command to remove the local NVE configuration for the specified vsid.

Format `no nvgre vsid source-ip`
Mode Global Config

6.8.0.4 nvgre tenant-system

Use this command to configure the forwarding entry for the tenant system MAC address mac-addr in the given VN that is reachable through the access interface. The user can configure tenant systems incrementally one by one. Normally, the system automatically learns tenant systems MAC address from the received traffic on the access interface. The user can configure the tenant systems MAC address mac-addr when accessing the interface to avoid initial flooding. If the user configures a tenant system on interface, the configuration overrides learning for the given MAC address in that VN.

NOTE: This command is valid only on physical and port-channel interfaces. The configured interface should also be a member of VLAN that is associated with the specified vsid.

These tenant system MAC addresses are maintained in a separate table. These are not listed as part of the FDB mac-address table. They internally consume shared system hardware L2 address table resources. The maximum number of tenant systems configured or learned depends on the number of resources left in the hardware L2 table which is dynamic in nature.

The configurable range for the VSID 1 to 16777214. 16777215 is reserved for internal purposes.

The user is allowed to configure maximum 24 tenant systems per physical or port-channel interface.

Default	No tenant MAC addresses are associated with the VN.
Format	`nvgre` ***`vsid`*** `tenant-system` ***`mac-addr`***
Mode	Interface Config

6.8.0.4.1 no nvgre tenant-system

Use this command to delete the configured tenant system forwarding entry on an interface when the tenant system mac-address and vsid are specified. This command cannot be used to delete a dynamically-learned tenant system association on the interface.

NOTE: When an access port configuration of the VN specified by `vsid` is removed, by removing the port participation of associated VLAN, all forwarding entries, if any, configured by user and learned by the switch on that access port are also removed.

Format	`no nvgre` ***`vsid`*** `tenant-system` ***`mac-addr`***
Mode	Interface Config

6.8.0.5 nvgre vlan

Use this command to associate an access VLAN to the NVGRE VN specified by vsid. If the vsid VN has not yet been created, it is created when this command is issued. The user can create a maximum of 1024 DCVPNs on the switch.

The packets that arrive with the specified VLAN vlan-id tag are associated to the NVGRE VN. This command only associates the traffic from the specified VLAN to a given VN identified by vsid. For this command to work, the VLAN vlan-id must already by created. The user must configure access ports for the VN specified by the vsid configuring the VLAN vlan-id membership on eligible interfaces before or after this command is issued.

NOTE: It is recommended to configure ingress filtering on all member ports of the VLAN ‘vlan-id’.

The configurable range for the VSID 1 to 16777214. 16777215 is reserved for internal purposes.

Default	No VLAN is associated with the vsid.
Format	`nvgre` ***`vsid`*** `vlan` ***`vlan-id`***
Mode	Global Config

6.8.0.5.1 no nvgre vlan

Use this command to remove an associated VLAN from a specified VN. All configured access ports of the specified are removed.

Format	`no nvgre` ***`vsid`*** `vlan`

Mode Global Config

6.8.0.6 vxlan enable

Use this command to enable the VXLAN mode on the switch. VXLAN mode must be enabled prior to performing any VXLAN configuration on the switch. By default, this is disabled.

NOTE: VXLAN mode and NVGRE mode are mutually exclusive modes. VXLAN mode cannot be enabled if NVGRE mode is enabled on the switch. NVGRE mode must be disabled prior to enabling VXLAN mode.

Format `vxlan enable`
Mode Global Config

6.8.0.6.1 no vxlan enable

Use this command to disable the VXLAN mode on the switch. This command also clears the existing VXLAN configuration on the switch, which includes all VXLAN tunnels, tenants, tenant VLAN associations, and configured forwarding entries.

Format `no vxlan enable`
Mode Global Config

6.8.0.7 vxlan source-ip

Use this command to specify the outer source IP address for encapsulated packets sent on a VXLAN with a given virtual network ID (VNID). The source-ip is the intended local VTEP for the tenant specified with vnid. If there is no VXLAN with the given VNID, the system creates it.

The configurable range for the VNID 1 to 16777214. 16777215 is reserved for internal purposes.

NOTE: It is recommended to configure a loopback interface with the intended local VXLAN Gateway IP address and use it as the source-ip for all tenants. It is also possible to configure tenants with a different source-ip when multiple loopback interfaces are configured and used as local VXLAN Gateways, if required. Loopback interfaces intended to be used as local VXLAN Gateways should be dedicated interfaces and must not be used for any other purpose.

Default There is no source IP address.
Format `vxlan` *`vnid`* `source-ip` *`ip-address`*
Mode Global Config

6.8.0.7.1 no vxlan source

Use this command to remove the configuration of local VTEP identified by ip-address from the VXLAN specified by vnid.

Format `no vxlan` *`vnid`* `source-ip`
Mode Global Config

6.8.0.8 vxlan tenant-system

Use this command to configure a forwarding entry for the tenant systems MAC address mac-addr' in the given VN that is reachable through the access interface. The user can configure tenant systems incrementally one by one. Normally, the system automatically learns tenant systems MAC address from received traffic on the access interface. The user can configure the tenant systems MAC address mac-addr on the access interface to avoid initial flooding. If the user configures a tenant system on interface, the configuration overrides learning for the given MAC address in that VN.

NOTE: This command is valid only on physical and port-channel interfaces. The configured interface should also be a member of VLAN that is associated with the specified vnid.

These tenant system MAC addresses are maintained in a separate table. These are not listed as part of FDB mac-address table. They internally consume shared system hardware L2 address table resources. So, the maximum number of tenant systems configured or learned depend on the number of resources left in the hardware L2 table, which is dynamic in nature.

The configurable range for the VNID 1 to 16777214. 16777215 is reserved for internal purposes.

User is allowed to configure maximum 24 tenant systems per physical or port-channel interface.

Default `No tenant MAC addresses are associated with the VN.`

Format `vxlan` *`vnid`* `tenant-system` *`mac-addr`*

Mode Interface Config

6.8.0.8.1 no vxlan tenant-system

Use this command to delete the configured tenant system forwarding entry on an interface when the tenant system mac-address and vnid are specified. This command cannot be used to delete a dynamically-learned tenant system association on the interface in a specified vnid VN.

NOTE: When an access port configuration of the VN specified by vnid is removed, by removing the port participation of associated VLAN, all forwarding entries, if any, configured by the user and learned by the switch on that access port are also removed.

Format `no vxlan` *`vnid`* `tenant-system` *`mac-addr`*

Mode Interface Config

6.8.0.9 vxlan udp-dst-port

Use this command to configure a specified UDP port as the VXLAN UDP destination port on the switch. All VXLANs on the switch use this UDP port as the UDP destination port in the UDP header when encapsulating. The switch also terminates incoming VXLAN packets matching specified UDP destination port.

This command also updates all existing VXLAN tunnels in the hardware with newly configured UDP destination port. There is no or very minimal traffic disruption during this operation.

The configurable range for the VNID 1 to 16777214. 16777215 is reserved for internal purposes.

The configurable range for the UDP port 1024 to 65535.

Default The default value is 4789. (IANA-assigned UDP port to VXLAN)

Format `vxlan udp-dst-port` *`port-number`*

Mode Global Config

6.8.0.9.1 no vxlan udp-dst-port

Use this command to reset the VXLAN UDP destination port configuration on the switch to the default value. This command updates all existing VXLAN tunnels in the hardware with the default VXLAN UDP destination port. There is no, or very minimal, traffic disruption during this operation.

Format `no vxlan udp-dst-port`
Mode Global Config

6.8.0.10 vxlan vlan

Use this command to associate an access VLAN to the specified VXLAN tenant. If the specified VXLAN has not yet been created, this command creates it. The user can create a maximum of 1024 DCVPNs on the switch.

The packets that arrive with the specified VLAN vlan-id tag are associated to the VXLAN vnid. This command only associates the traffic from the specified VLAN to a given VN identified by vsid. The VLAN vlan-id must be created already for this command to work. The user must configure the access ports for the VN specified by vnid by configuring the VLAN vlan-id membership on the eligible interfaces before or after this command is issued.

NOTE: It is recommended to configure ingress filtering on all member ports of the VLAN vlan-id.

The configurable range for the VNID 1 to 16777214. 16777215 is reserved for internal purposes.

Default `No VLAN is associated with the VXLAN.`
Format `vxlan` *`vnid`* `vlan` *`vlan-id`*
Mode Global Config

6.8.0.10.1 no vxlan vlan

Use this command to remove the association of the specified VLAN from a given VXLAN. All configured access ports of VN specified by vnid are removed.

Format `no vxlan` *`vnid`* `vlan`
Mode Global Config

6.8.0.11 vxlan vtep

Use this command to configure a specified IP address as the remote virtual tunnel endpoint (VTEP) in the VXLAN. If the specified VXLAN has not yet been created, it is created when this command is issued. The user can create a maximum of 1024 DCVPNs on the switch. Multiple remote VTEPs can be configured one by one for the same vnid as required.

NOTE: The switch does support configuration of Multicast IP address to automatically discover remote VTEPs to define a flood group for DCVPN. This command should be used to manually configure, for each DCVPN, all remote VTEPs behind which Tenant (VNID) hosts are present.

The user can optionally specify one or more tenant systems reachable through the VTEP. The tenant systems for a particular VXLAN can be added or deleted incrementally one by one. Normally, the system automatically learns tenant systems from received messages. If a tenant system is configured, the configuration overrides learning for the given MAC address.

The tenant system MAC addresses are maintained in a separate table. These are not listed as part of FDB mac-address table. They internally consume shared system hardware L2 address table resources. The maximum number of tenant systems configured depend on the number of resources left in the hardware L2 table, which is dynamic in nature.

The user is allowed to configure maximum of 600 remote tenant system entries per VN and overall 4096 entries on the switch.

The configurable range for the VNID 1 to 16777214. 16777215 is reserved for internal purposes.

Default `No VTEPs are associated with the VXLAN.`
Format `vxlan` *`vnid`* `vtep` *`ip-address`* `[ tenant-system` *`mac-addr`* `]`
Mode Global Config

6.8.0.11.1 no vxlan vtep

Use this command to remove a remote VTEP from a VXLAN. This also clears all tenant system MAC address associations with the specified VTEP and DCVPN from the system. If the optional`[ tenant-system` *`mac-addr`* `]` is used, this command deletes the configured association of a tenant system to a remote VTEP. This command cannot be used to delete a dynamically-learned tenant system association.

Format `no vxlan` *`vnid`* `vtep` *`ip-address`* `tenant-system` *`mac-addr`*
Mode Global Config

6.8.0.12 clear counters nvgre

Use this command to clear packet and byte counters of all configured NVGRE virtual networks.

Format `clear counters nvgre`
Mode Privileged EXEC

The following counter information is cleared for all configured NVGRE NVEs:

Parameter	Description
Packets TX	Number of unicast packets sent to the NVE.
Packets RX	Number of unicast packets received from the NVE.
Bytes TX	Number of unicast bytes sent to the NVE.
Bytes RX	Number of unicast bytes received from the NVE.

6.8.0.13 clear counters vxlan

Use this command to clear packet and byte counters in all configured VXLAN virtual networks.

Format `clear counters vxlan`
Mode Privileged EXEC

The following counter information is cleared for all configured VXLAN VTEPs:

Parameter	Description
Packets TX	Number of unicast packets sent to the VTEP
Packets RX	Number of unicast packets received from the VTEP
Bytes TX	Number of unicast bytes sent to the VTEP
Bytes RX	Number of unicast bytes received from the VTEP

6.8.0.14 show nvgre

Use this command to display configuration and status for one or more NVGRE VNs. It also provides information on allowed limits and statistics.

Format `show nvgge [vsid]`

Mode Privileged EXEC

Parameter	Description
NVGRE Admin Mode	Admin mode of NVGRE Enable/Disable
NVGRE ID	Virtual Subnet ID (VSID)
Source Address	Source IP address of the local TEP
VLAN	Associated VLAN ID to classify access ports
Access Ports	List of access ports associated with this VN
Remote TEP(s)	List of remote NVEs participating in this VN

Example:

```
(Routing) (Config)#show nvgre

NVGRE Admin Mode.............................. Enable

Maximum Allowed Limits or Table Sizes
-----------------------------------------------------

Tenant Table Size............................. 1024
Access Ports Table Size....................... 2048
Tunnel/Network Reference Ports Table Size...... 8192

Current Entries Count or Table Usage
-----------------------------------------------------

Tenant Table Entries.......................... 1
Access Port Entries........................... 1
Tunnel/Network Reference Port entries.......... 2

NVGRE ID  Source Address   VLAN  Access Port(s)        Remote TEP(s)
--------- --------------- ----- --------------------- --------------
1         192.168.10.1    10    0/2                   10.10.10.1
                                                      100.100.100.1
(Routing) #show nvgre 1

Source Address................................ 192.168.10.1
Tenant VLAN................................... 10
Access Port(s)................................ 0/2
```

```
Remote TEP(s)..................................... 10.10.10.1
                                                   100.100.100.1
```

6.8.0.15 show nvgre nve

Use this command to display the status of the specified remote NVE in a specified NVGRE virtual network.

Format `show nvgre` *`vsid`* `nve [`*`ip-address`*`]`

Mode Privileged EXEC

Parameter	Description
NVGRE ID	Virtual subnet ID (VSID)
Remote NVE	Remote NVE IP address
Up Time	How long the NVE has been reachable
Reachable	Whether the NVE is currently reachable
Reachable Transitions	Number of times the NVE has transitioned to reachable state
Packets TX	Number of unicast packets sent to the NVE
Packets RX	Number of unicast packets received from the NVE
Bytes TX	Number of unicast bytes sent to the NVE
Bytes RX	Number of unicast bytes received from the NVE

Example:

```
(Routing) (Config)#show nvgre 1 nve

                 Uptime                  Reachable
Remote NVE       (sec)      Reachable    Transitions
-----------------------------------------------------
10.10.10.1       0          NO           0
100.100.100.1    0          NO           0

(Routing) (Config)#show nvgre 1 nve 10.10.10.1

NVGRE ID..................................... 1
Remote NVE................................... 10.10.10.1
Reachable.................................... NO
Uptime (sec)................................. 0
Reachable Transitions........................ 0

Unicast Counters
-----------------------------------------------
Packets Tx................................... 0
Packets Rx................................... 0
Bytes Tx..................................... 0
Bytes Rx..................................... 0
```

6.8.0.16 show nvgre tenant-systems

Use this command to list all tenant systems currently configured or dynamically learned in a given VN. This can also be used to find a specified host or tenant system, if the optional *mac-addr* for a VN is specified.

Format `show nvgre` *`vsid`* `tenant-systems [`*`mac-addr`*`]`

Mode Privileged EXEC

Parameter	Description
Tenant MAC	MAC address of a host or tenant system
NVE	IP address of NVE if the tenant system is behind the remote NVE. This is valid for remote tenant system, otherwise it is blank.
Interface	Access interface on which MAC entry is learned or configured. This is valid for tenant system on local access interface, otherwise, it is blank.
Entry Type	Configured or learned
Age	How long since the entry was learned. Not applicable for configured entries.

Example:

```
(Routing) (Config)#show nvgre 1 tenant-systems

Tenant MAC             NVE          Interface   Type       Age (sec)
------------------ --------------- ---------- ----------- ----------
00:00:00:00:00:02                  0/2        Learned     278
00:00:DC:2C:00:32  10.10.10.1                 Learned     13423
```

6.8.0.17 show nvgre tenant-systems all

Use this command to list all tenant systems currently configured or dynamically learned in all configured VNs. It also provides information on allowed limits on tenant systems configuration and forwarding table statistics.

The user may also optionally filter entries based on tenant system location, local or remote. Local entries are reachable through configured local access ports. Remote entries are behind the remote NVEs and reachable through the configured NVGREs to remote NVEs.

Format `show nvgre tenant-systems [local|remote]`

Mode Privileged EXEC

Parameter	Description
Tenant ID	Virtual Subnet ID (VSID)
Tenant MAC	MAC address of a host or tenant system
NVE	IP address of NVE if the tenant system is behind the remote NVE. This is valid for the remote tenant system, otherwise it is blank.
Interface	Access interface on which the MAC entry is learned or configured. This valid for the tenant system on the local access interface, otherwise it is blank.
AppIfIndex	Internal access or tunnel port handle.
Entry Type	Configured or learned.

Example:

```
(Routing) #show nvgre tenant-systems
```

```
Maximum Allowed Limits or Table Sizes
-----------------------------------------------------

Static Local Host Entries per Interface........ 24
Static Remote Host Entries per Tenant.......... 600
Static Remote Host Entries per Switch.......... 4096
Forwarding Table Size.......................... 32768

Current Entries Count or Table Usage
-----------------------------------------------------

Static Host Entries............................ 4
Learned Host Entries........................... 2
Forwarding Table Entries....................... 6

Tenant ID Tenant MAC           NVE           Interface  AppIfIndex  Entry Type
--------- ----------------- ---------------- ---------- ----------  ----------
1         00:00:00:11:22:33                   0/13       8537        Static
1         00:00:00:11:22:44                   0/13       8537        Static
1         00:72:44:3A:D2:43                   0/13       8537        Learned
1         00:00:AA:BB:CC:DD  1.1.1.1                     345         Static
1         00:00:AA:BB:CC:EE  1.1.1.1                     345         Static
1         00:EA:08:CA:16:45  1.1.1.1                     345         Learned
```

```
(Routing) #show nvgre tenant-systems local

Tenant ID Tenant MAC        Interface  AppIfIndex  Entry Type
--------- ----------------- ---------- ----------  ----------
1         00:00:00:11:22:33  0/13       8537        Static
1         00:00:00:11:22:44  0/13       8537        Static
1         00:72:44:3A:D2:43  0/13       8537        Learned


(Routing) #show nvgre tenant-systems remote

Tenant ID Tenant MAC         NVE              AppIfIndex  Entry Type
--------- ----------------- ---------------- ----------  -----------
1         00:00:AA:BB:CC:DD  1.1.1.1          345         Static
1         00:00:AA:BB:CC:EE  1.1.1.1          345         Static
1         00:EA:08:CA:16:45  1.1.1.1          345         Learned
```

6.8.0.18 show vxlan

Use this command to display configuration and status for one or more VXLAN VNs. It also provides information on allowed limits and statistics.

Format `show vxlan [`*`vnid`*`]`

Mode Privileged EXEC

Parameter	Description
VXLAN Admin Mode	Admin mode of VXLAN Enable/Disable
Destination UDP Port	UDP destination port used in VXLAN header
VXLAN ID	Virtual network ID (VNID)

Parameter	Description
Source Address	Source IP address of the local TEP
Access Ports	List of access ports associated with this VXLAN
VLAN	Associated VLAN ID to classify access ports
Remote TEP(s)	List of remote VTEPs participating in this VXLAN

Example:

```
(Routing) (Config)#show vxlan

VXLAN Admin Mode.............................. Enable
Destination UDP Port.......................... 4789

Maximum Allowed Limits or Table Sizes
-----------------------------------------------------

Tenant Table Size............................. 1024
Access Ports Table Size....................... 2048
Tunnel/Network Reference Ports Table Size...... 8192

Current Entries Count or Table Usage
-----------------------------------------------------

Tenant Table Entries.......................... 1
Access Port Entries........................... 1
Tunnel/Network Reference Port entries.......... 2

VXLAN ID  Source Address   VLAN  Access Port(s)        Remote TEP(s)
--------- --------------- ----- --------------------- --------------
1         192.168.10.1     10    0/2                   20.20.20.1
                                                       200.200.200.1
```

Example:

```
(Routing) #show vxlan 1

Source Address................................ 192.168.10.1
Tenant VLAN................................... 10
Access Port(s)................................ 0/2
Remote TEP(s)................................. 20.20.20.1
                                               200.200.200.1
```

6.8.0.19 show vxlan tenant-systems

Use this command to list all tenant systems currently configured or dynamically learned in a given DCVPN (identified by *vnid*). This lists tenant systems which are behind the VTEP and also reachable through local access interfaces.

Format `show vxlan` *`vnid`* `tenant-systems [`*`mac-addr`*`]`

Mode Privileged EXEC

Parameter	Description
Tenant MAC	MAC address of tenant system
VTEP	Remote VTEP IP address
Interface	Access interface on which MAC entry is learned or configured

Parameter	Description
Entry Type	Configured or learned
Age	How long since the entry was learned. Not applicable for configured entries.

Example:

```
(Routing) (Config)#show vxlan 1 tenant-systems

Tenant MAC         VTEP             Interface  Entry Type  Age (sec)
------------------ ---------------- ---------- ----------- ----------
00:00:00:00:00:02                   0/2        Learned     278323
00:00:00:1A:00:11 20.20.20.1                   Learned     12423
```

6.8.0.20 show vxlan tenant-systems all

This command lists all tenant systems currently configured or dynamically learned in all configured VNs. It also provides information on allowed limits on tenant systems configuration and forwarding table statistics.

User may also optionally filter entries based on tenant system location, local or remote. Local entries are reachable through configured local VN access ports. Remote entries are behind the remote VTEPs and reachable through the configured VXLANs to remote VTEPs.

Format `show vxlan tenant-systems [local|remote]`

Mode Privileged EXEC

The following information is displayed.

Parameter	Description
Tenant ID	Virtual Subnet ID (VSID)
Tenant MAC	MAC address of a host or tenant system
VTEP	IP address of the VTEP if the tenant system is behind the remote VTEP. This is valid for the remote tenant system, otherwise it is blank.
Interface	Access interface on which the MAC entry is learned or configured. This valid for the tenant system on the local access interface, otherwise it is blank.
AppIfIndex	Internal access or tunnel port handle.
Entry Type	Configured or learned.

Example:

```
(Routing) #show vxlan tenant-systems

Maximum Allowed Limits or Table Sizes
-----------------------------------------------------

Static Local Host Entries per Interface........ 24
Static Remote Host Entries per Tenant.......... 600
Static Remote Host Entries per Switch.......... 4096
Forwarding Table Size.......................... 32768

Current Entries Count or Table Usage
```

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

Static Host Entries.......................... 4
Learned Host Entries......................... 2
Forwarding Table Entries..................... 6

Tenant ID Tenant MAC           NVE           Interface  AppIfIndex  Entry Type
--------- ----------------- ---------------- ---------- ----------  ----------
1         00:00:00:23:27:a2                   0/11       8545        Static
1         00:00:AC:BD:12:78                   0/11       8548        Static
1         00:12:88:37:BD:C5                   0/14       8547        Learned
1         00:00:42:B2:22:A3  12.12.12.1                  346         Static
1         00:23:72:5B:62:1E  12.12.12.1                  346         Static
1         00:1A:09:A3:11:21  12.12.12.1                  346         Learned

(Routing) #show vxlan tenant-systems local

Tenant ID Tenant MAC        Interface  AppIfIndex  Entry Type
--------- ----------------- ---------- ----------  ----------
1         00:00:00:23:27:a2  0/11       8545        Static
1         00:00:AC:BD:12:78  0/11       8548        Static
1         00:12:88:37:BD:C5  0/14       8547        Learned

(Routing) #show vxlan tenant-systems remote

Tenant ID Tenant MAC         VTEP             AppIfIndex  Entry Type
--------- ----------------- ---------------- ----------  -----------
1         00:00:42:B2:22:A3  12.12.12.1       346         Static
1         00:23:72:5B:62:1E  12.12.12.1       346         Static
1         00:1A:09:A3:11:21  12.12.12.1       346         Learned
```

6.8.0.21 show vxlan vtep

Use this command to show the status of remote VTEPs in a given VXLAN virtual network.

Format `show vxlan` *`vnid`* `vtep [`*`ip-address`*`]`

Mode Privileged EXEC

The following status information is displayed for remote VTEP/s :

Parameter	Description
VXLAN ID	Virtual Network ID (VNID)
Remote VTEP	Remote VTEP IP address
Dest UDP Port	UDP destination port used in UDP header
Up Time	How long the VTEP has been reachable
Reachable	Whether the VTEP is currently reachable
Reachable Transitions	Number of times the VTEP has transitioned to reachable state.
Packets TX	Number of unicast packets sent to the VTEP
Packets RX	Number of unicast packets received from the VTEP
Bytes TX	Number of unicast bytes sent to the VTEP
Bytes RX	Number of unicast bytes received from the VTEP

Example:

```
(Routing) (Config)#show vxlan 1 vtep

                 Dest       Uptime                 Reachable
Remote VTEP      UDP Port   (sec)      Reachable   Transitions
---------------- ---------- ---------- ----------- -----------
20.20.20.1       4789       0          NO          0
200.200.200.1    4789       0          NO          0

(Routing) (Config)#show vxlan 1 vtep 20.20.20.1

VXLAN ID..................................... 1
Remote VTEP.................................. 20.20.20.1
Destination UDP Port......................... 4789
Reachable.................................... NO
Uptime (sec)................................. 0
Reachable Transitions........................ 0

Unicast Counters
-----------------------------------------------
Packets Tx................................... 0
Packets Rx................................... 0
Bytes Tx..................................... 0
Bytes Rx..................................... 0
```

Chapter 7: IPv4 Routing Commands

This section describes the routing commands available in the EFOS CLI.

NOTE: The commands in this chapter are in one of three functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Clear commands clear some or all of the settings to factory defaults.

7.1 Address Resolution Protocol Commands

This section describes the commands you use to configure Address Resolution Protocol (ARP) and to view ARP information on the switch. ARP associates IP addresses with MAC addresses and stores the information as ARP entries in the ARP cache.

7.1.0.1 arp

This command creates an ARP entry in the specified virtual router instance (vrf vrf-name). If a virtual router is not specified, the static ARP entry is created in the default router. The value for *ipaddress* is the IP address of a device on a subnet attached to an existing routing interface. The parameter *macaddr* is a unicast MAC address for that device. The interface parameter specifies the next hop interface.

The format of the MAC address is 6 two-digit hexadecimal numbers that are separated by colons, for example 00:06:29:32:81:40.

Format `arp [vrf vrf-name] ipaddress macaddr interface {slot/port | vlan id}`

Mode Global Config

7.1.0.1.1 no arp

This command deletes an ARP entry in the specified virtual router. The value for *arpentry* is the IP address of the interface. The value for *ipaddress* is the IP address of a device on a subnet attached to an existing routing interface. The parameter *macaddr* is a unicast MAC address for that device. The interface parameter specifies the next hop interface.

Format `no arp [vrf vrf-name] ipaddress interface {slot/port | vlan id}`

Mode Global Config

7.1.0.2 arp cachesize

This command configures the ARP cache size. The ARP cache size value is a platform specific integer value. The default size also varies depending on the platform.

Format `arp cachesize platform specific integer value`

Mode Global Config

7.1.0.2.1 no arp cachesize

This command configures the default ARP cache size.

Format `no arp cachesize`
Mode Global Config

7.1.0.3 arp dynamicrenew

This command enables the ARP component to automatically renew dynamic ARP entries when they age out. When an ARP entry reaches its maximum age, the system must decide whether to retain or delete the entry. If the entry has recently been used to forward data packets, the system will renew the entry by sending an ARP request to the neighbor. If the neighbor responds, the age of the ARP cache entry is reset to 0 without removing the entry from the hardware. Traffic to the host continues to be forwarded in hardware without interruption. If the entry is not being used to forward data packets, then the entry is deleted from the ARP cache, unless the dynamic renew option is enabled. If the dynamic renew option is enabled, the system sends an ARP request to renew the entry. When an entry is not renewed, it is removed from the hardware and subsequent data packets to the host trigger an ARP request. Traffic to the host may be lost until the router receives an ARP reply from the host. Gateway entries, entries for a neighbor router, are always renewed. The dynamic renew option applies only to host entries.

The disadvantage of enabling dynamic renew is that once an ARP cache entry is created, that cache entry continues to take space in the ARP cache as long as the neighbor continues to respond to ARP requests, even if no traffic is being forwarded to the neighbor. In a network where the number of potential neighbors is greater than the ARP cache capacity, enabling dynamic renew could prevent some neighbors from communicating because the ARP cache is full.

Default disabled
Format `arp dynamicrenew`
Mode Privileged EXEC

7.1.0.3.1 no arp dynamicrenew

This command prevents dynamic ARP entries from renewing when they age out.

Format `no arp dynamicrenew`
Mode Privileged EXEC

7.1.0.4 arp purge

This command causes the specified IP address to be removed from the ARP cache in the specified virtual router. If no router is specified, the ARP entry is deleted in the default router. Only entries of type dynamic or gateway are affected by this command.

Format `arp purge [vrf` *`vrf-name`*`] ` *`ipaddress`* `interface {`*`slot/port`* `| vlan` *`id`*`}`
Mode Privileged EXEC

Parameter	Description
ipaddress	The IP address to remove from the ARP cache.

Parameter	Description
vrf-name	The virtual router from which IP addresses will be removed.
interface	The interface from which IP addresses will be removed.

7.1.0.5 resptime

This command configures the ARP request response timeout.

The value for `seconds` is a valid positive integer, which represents the IP ARP entry response timeout time in seconds. The range for `seconds` is between 1-10 seconds.

Default 1
Format `arp resptime` *`1-10`*
Mode Global Config

7.1.0.5.1 no arp resptime

This command configures the default ARP request response timeout.

Format `no arp resptime`
Mode Global Config

7.1.0.6 arp retries

This command configures the ARP count of maximum request for retries.

The value for `retries` is an integer, which represents the maximum number of request for retries. The range for `retries` is an integer between 0-10 retries.

Default 4
Format `arp retries` *`0-10`*
Mode Global Config

7.1.0.6.1 no arp retries

This command configures the default ARP count of maximum request for retries.

Format `no arp retries`
Mode Global Config

7.1.0.7 arp timeout

This command configures the ARP entry ageout time.

The value for `seconds` is a valid positive integer, which represents the IP ARP entry ageout time in seconds. The range for `seconds` is between 15-21600 seconds.

Default 1200
Format `arp timeout` *`15-21600`*
Mode Global Config

7.1.0.7.1 no arp timeout

This command configures the default ARP entry ageout time.

Format `no arp timeout`

Mode Global Config

7.1.0.8 clear arp-cache

This command causes all ARP entries of type dynamic to be removed from the ARP cache for the virtual router. If no router is specified, the cache for the default router is cleared. If the *gateway* keyword is specified, the dynamic entries of type gateway are purged as well.

Format `clear arp-cache [vrf` *`vrf-name`*`] [gateway]`

Mode Privileged EXEC

7.1.0.9 clear arp-switch

Use this command to clear the contents of the switch's Address Resolution Protocol (ARP) table that contains entries learned through the Management port. To observe whether this command is successful, `ping` from the remote system to the DUT. Issue the `show arp switch` command to see the ARP entries. Then issue the `clear arp-switch` command and check the `show arp switch` entries. There will be no more arp entries.

Format `clear arp-switch`

Mode Privileged EXEC

7.1.0.10 show arp

This command displays the Address Resolution Protocol (ARP) cache for a specified virtual router instance. If a virtual router is not specified, the ARP cache for the default router is displayed. The displayed results are not the total ARP entries. To view the total ARP entries, the operator should view the `show arp` results in conjunction with the `show arp switch` results.

Format `show arp [vrf` *`vrf-name`*`]`

Mode Privileged EXEC

Parameter	Definition
Age Time (seconds)	The time it takes for an ARP entry to age out. This is configurable. Age time is measured in seconds.
Response Time (seconds)	The time it takes for an ARP request timeout. This value is configurable. Response time is measured in seconds.
Retries	The maximum number of times an ARP request is retried. This value is configurable.
Cache Size	The maximum number of entries in the ARP table. This value is configurable.
Dynamic Renew Mode	Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out.
Total Entry Count Current / Peak	The total entries in the ARP table and the peak entry count in the ARP table.
Static Entry Count Current / Max	The static entry count in the ARP table and maximum static entry count in the ARP table.

The following are displayed for each ARP entry:

Parameter	Definition
IP Address	The IP address of a device on a subnet attached to an existing routing interface.
MAC Address	The hardware MAC address of that device.
Interface	The routing *slot/port* associated with the device ARP entry.
Type	The type that is configurable. The possible values are Local, Gateway, Dynamic and Static.
Age	The current age of the ARP entry since last refresh (in hh:mm:ss format)

7.1.0.11 show arp brief

This command displays the brief Address Resolution Protocol (ARP) table information.

Format `show arp brief`

Mode Privileged EXEC

Parameter	Definition
Age Time (seconds)	The time it takes for an ARP entry to age out. This value is configurable. Age time is measured in seconds.
Response Time (seconds)	The time it takes for an ARP request timeout. This value is configurable. Response time is measured in seconds.
Retries	The maximum number of times an ARP request is retried. This value is configurable.
Cache Size	The maximum number of entries in the ARP table. This value is configurable.
Dynamic Renew Mode	Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out.
Total Entry Count Current / Peak	The total entries in the ARP table and the peak entry count in the ARP table.
Static Entry Count Current / Max	The static entry count in the ARP table and maximum static entry count in the ARP table.

7.1.0.12 show arp switch

This command displays the contents of the switch's Address Resolution Protocol (ARP) table.

Format `show arp switch`

Mode Privileged EXEC

Parameter	Definition
IP Address	The IP address of a device on a subnet attached to the switch.
MAC Address	The hardware MAC address of that device.
Interface	The routing *slot/port* associated with the device's ARP entry.

7.2 IP Routing Commands

This section describes the commands you use to enable and configure IP routing on the switch.

7.2.0.1 routing

This command enables IPv4 routing for an interface or range of interfaces. You can view the current value for this function with the `show ip brief` command. The value is labeled as “Routing Mode.”

Default disabled
Format `routing`
Mode Interface Config

7.2.0.1.1 no routing

This command disables routing for an interface.

You can view the current value for this function with the `show ip brief` command. The value is labeled as “Routing Mode.”

Format `no routing`
Mode Interface Config

7.2.0.2 ip routing

This command enables the IP Router Admin Mode for the master switch.

Format `ip routing`
Mode
- Global Config
- Virtual Router Config

7.2.0.2.1 no ip routing

This command disables the IP Router Admin Mode for the master switch.

Format `no ip routing`
Mode Global Config

7.2.0.3 ip address

This command configures an IP address on an interface or range of interfaces. You can also use this command to configure one or more secondary IP addresses on the interface. The command supports RFC 3021 and accepts using 31-bit prefixes on IPv4 point-to-point links. This command adds the label IP address in the command Section 7.2.0.24, show ip interface.

NOTE: The 31-bit subnet mask is only supported on routing interfaces. The feature is not supported on network port and service port interfaces because EFOS acts as a host, not a router, on these management interfaces.

Parameter	Description
ipaddr	The IP address of the interface.
subnetmask	A 4-digit dotted-decimal number which represents the subnet mask of the interface.

Parameter	Description
masklen	Implements RFC 3021. Using the **/** notation of the subnet mask, this is an integer that indicates the length of the subnet mask. Range is 5 to 32 bits.

Format `ip address` *`ipaddr {subnetmask | /masklen}`* `[secondary]`

Mode Interface Config

Example: The following example of the command shows the configuration of the subnet mask with an IP address in the dotted decimal format on interface vlan 100.

```
(Routing) (Interface vlan 300)#ip address 192.168.10.1 255.255.255.254

(Routing) (Interface vlan 300)#
```

Example: The next example of the command shows the configuration of the subnet mask with an IP address in the **/** notation on interface vlan 100.

```
(Routing) (Config)#interface vlan 30

(Routing) (Interface vlan 30)#ip address 192.168.10.1 /31
```

7.2.0.3.1 no ip address

This command deletes an IP address from an interface. The value for `ipaddr` is the IP address of the interface in a.b.c.d format where the range for a, b, c, and d is 1-255. The value for `subnetmask` is a 4-digit dotted-decimal number which represents the Subnet Mask of the interface. To remove all of the IP addresses (primary and secondary) configured on the interface, enter the command `no ip address`.

Format `no ip address [{`*`ipaddr subnetmask`* `[secondary]}]`

Mode Interface Config

7.2.0.4 ip address dhcp

This command enables the DHCPv4 client on an in-band interface so that it can acquire network information, such as the IP address, subnet mask, and default gateway, from a network DHCP server. When DHCP is enabled on the interface, the system automatically deletes all manually configured IPv4 addresses on the interface.

To enable the DHCPv4 client on an in-band interface and send DHCP client messages with the client identifier option (DHCP Option 61), use the **ip address dhcp client-id** configuration command in interface configuration mode.

Default disabled

Format `ip address dhcp [client-id]`

Mode Interface Config

Example: In the following example, DHCPv4 is enabled on interface 0/1.

```
(router1) #config
(router1) (Config)#interface 0/1
(router1) (Interface 0/1)#ip address dhcp
```

7.2.0.4.1 no ip address dhcp

The **no ip address dhcp** command releases a leased address and disables DHCPv4 on an interface. The **no** form of the **ip address dhcp client-id** command removes the client-id option and also disables the DHCP client on the in-band interface.

Format `no ip address dhcp [client-id]`

Mode Interface Config

7.2.0.5 ip default-gateway

This command manually configures a default gateway for the switch. Only one default gateway can be configured. If you invoke this command multiple times, each command replaces the previous value.

Format `ip default-gateway` *`ipaddr`*

Mode
- Global Config
- Virtual Router Config

7.2.0.5.1 no ip default-gateway

This command removes the default gateway address from the configuration.

Format `no ip default-gateway` *`ipaddr`*

Mode
- Interface Config
- Virtual Router Config

7.2.0.6 ip load-sharing

This command configures IP ECMP load balancing mode.

Default 6

Format `ip load-sharing` *`mode`* `{inner | outer}`

Mode Global Config

Parameter	Description
mode	Configures the load balancing or sharing mode for all EMCP groups. ■ 1: Based on a hash using the Source IP address of the packet. ■ 2: Based on a hash using the Destination IP address of the packet. ■ 3: Based on a hash using the Source and Destination IP addresses of the packet. ■ 4: Based on a hash using the Source IP address and the Source TCP/UDP Port field of the packet. ■ 5: Based on a hash using the Destination IP address and the Destination TCP/UDP Port field of the packet. ■ 6: Based on a hash using the Source and Destination IP address, and the Source and Destination TCP/UDP Port fields of the packet.
inner	Use the inner IP header for tunneled packets.
outer	Use the outer IP header for tunneled packets.

7.2.0.6.1 no ip load-sharing

Format `no ip load-sharing`
Mode Global Config

7.2.0.7 ip ipsec-load-sharing spi

This command enables hashing on the Security Parameters Index (SPI) field in IPsec packets.

IPsec packets are IPv4 and IPv6 packets with the following IP protocols:

- IP protocol 50—Encapsulating Security Payload (ESP)
- IP protocol 51—Authentication Header (AH).

The ESP and AH protocols do not employ the IP source and destination port numbers, so the hardware does not use the IP port numbers for hashing the packets. The ESP and AH packet headers contain the SPI field, which is associated with packet flows and can be used for hashing IPsec packets.

Default enabled
Format `ip ipsec-load-sharing spi`
Mode Global Config

7.2.0.7.1 no ip ipsec-load-sharing spi

This command disables the ECMP IPSEC hashing on the SPI field.

Format `no ip ipsec-load-sharing spi`
Mode Global Config

7.2.0.8 release dhcp

Use this command to force the DHCPv4 client to release the leased address from the specified interface.

Format `release dhcp {`*`slot/port`* `|` `vlan` *`id`*`}`
Mode Privileged EXEC

7.2.0.9 renew dhcp

Use this command to force the DHCPv4 client to immediately renew an IPv4 address lease on the specified interface.

NOTE: This command can be used on in-band ports as well as the service or network (out-of-band) port.

Format `renew dhcp {`*`slot/port`* `|` `vlan` *`id`*`}`
Mode Privileged EXEC

7.2.0.10 renew dhcp network-port

Use this command to renew an IP address on a network port.

Format `renew dhcp network-port`

Mode Privileged EXEC

7.2.0.11 renew dhcp service-port

Use this command to renew an IP address on a service port.

Format `renew dhcp service-port`
Mode Privileged EXEC

7.2.0.12 ip route

This command configures a static route. Use the optional `vrf` parameter to configure the static route in the specified virtual router instance. The *`ipaddr`* parameter is a valid IP address, and *`subnetmask`* is a valid subnet mask. The *`nexthopip`* parameter is a valid IP address of the next hop router. Specifying `Null0` as nexthop parameter adds a static reject route. The optional *`preference`* parameter is an integer (value from 1 to 255) that allows you to specify the preference value (sometimes called “administrative distance”) of an individual static route. Among routes to the same destination, the route with the lowest preference value is the route entered into the forwarding database. By specifying the preference of a static route, you control whether a static route is more or less preferred than routes from dynamic routing protocols. The preference also controls whether a static route is more or less preferred than other static routes to the same destination. A route with a preference of 255 cannot be used to forward traffic.

This command also enables static provisioning of MPLS tunnels based on the MPLS label(s) parameters. Up to three MPLS labels can be specified as part of this command. The unique identifier for the tunnel is the nexthop IPv4 address and the MPLS label(s). The label-1 appears first in the packet (outer label) followed by the optional labels, label-2 and label-3. The mplsd-label values are 20-bit MPLS labels. The valid range of an MPLS label is 16 to 1048575.

NOTE: The nexthop IPv4 address along with MPLS-labels define the nexthop. So, you can configure a route to the same network with the same nexthop IPv4 address but with different MPLS-labels.

The `description` parameter allows a description of the route to be entered.

Use the `track object-number` to specify that the static route is installed only if the configured track object is up. When the track object is down the static route is removed from the Route Table. Use the no form of this command to delete the tracked static route. The `object-number` parameter is the object number representing the object to be tracked. The range is from 1 to 128. Only one track object can be associated with a specific static route. If you configure a different track object, the previously configured track object is replaced by the newly configured track object. To display the IPv4 static routes that being tracked by track objects, use the `show ip route track-table` command.

For the static routes to be visible, you must perform the following steps:

- Enable IP routing globally.
- Enable IP routing for the interface.
- Confirm that the associated link is also up.

Default preference—1

Format `ip route [vrf` *`vrf-name`*`]`*`ipaddr subnetmask`* `{` *`nexthopip`* `| Null0 | interface {`*`slot/port`*`|` *`vlan-id`*`}} [mplsd-label label-1 [mplsd-label label-2] [mplsd-label label-3] [preference]` `[description` *`description`*`] [track` *`object-number`*`]`

Mode Global Config

Example:

Subnetwork 9.0.0.0/24 is a connected subnetwork in global table and subnet 56.6.6.0/24 is reachable via a gateway 9.0.0.2 in the global table.

Subnet 8.0.0.0/24 is a connected subnetwork in virtual router *Red*.

Now we leak the 2 routes from global route table into the virtual router *Red* and leak the connected subnet 8.0.0.0/24 from *Red* to global table.

When leaking connected route in the global routing table to a virtual router, the /32 host route for the leaked host is added in the virtual router instance's route table.

Also we add a non-leaked static route for 66.6.6.0/24 subnetwork scoped to the domain of virtual router Red below.

```
(Router) (Config)#ip routing
(Router) (Config)#ip vrf Red
(Router) (Config)#interface 0/27
(Router) (Interface 0/27)#routing
(Router) (Interface 0/27)#ip vrf forwarding Red
(Router) (Interface 0/27)#ip address 8.0.0.1 /24

(Router) (Interface 0/27)#interface 0/26
(Router) (Interface 0/26)#routing
(Router) (Interface 0/26)#ip address 9.0.0.1 /24
(Router) (Interface 0/26)#exit

(Router) (Config)#ip route 56.6.6.0 /24 9.0.0.2

Routes leaked from global routing table to VRF's route table are :
(Router) (Config)#ip route vrf Red 9.0.0.2 255.255.255.255 9.0.0.2 0/26
(Router) (Config)#ip route vrf Red 56.6.6.0 255.255.255.0 9.0.0.2 0/26

Route leaked from VRF's route table to global routing table is :
(Router) (Config)#ip route 8.0.0.2 255.255.255.255 0/27

Route (non-leaked) internal to VRF's route table is :
(Router) (Config)#ip route vrf Red 66.6.6.0 255.255.255.0 8.0.0.2
```

7.2.0.12.1 no ip route

This command deletes a single next hop to a destination static route. If you use the *nexthopip* parameter, the next hop is deleted.

Format	`no ip route` *ipaddr subnetmask {nexthopip | Null0 | interface {slot/port | vlan vlan-id}}*
Mode	Global Config

7.2.0.13 ip route default

This command configures the default route. Use the vrf parameter to configure the default route in a specified virtual router instance. The value for `nexthopip` is a valid IP address of the next hop router. The `preference` is an integer value from 1 to 255. A route with a preference of 255 cannot be used to forward traffic.

This command also enables static provisioning of MPLS tunnels based on the MPLS label(s) parameters. Up to three MPLS labels can be specified as part of this command. The unique identifier for the tunnel is the nexthop IPv4 address and the MPLS label(s). The label-1 appears first in the packet (outer label) followed by the optional labels, label-2 and label-3. The mplsd-label values are 20-bit MPLS labels. The valid range of an MPLS label is 16 to 1048575.

Default	preference—1
Format	`ip route default [vrf vrf-name] nexthopip [mplsd-label label-1] [mplsd-label label-2] [mplsd-label label-3] [preference]`
Mode	Global Config

7.2.0.13.1 no ip route default

This command deletes all configured default routes. If the optional `nexthopip` parameter is designated, the specific next hop is deleted from the configured default route and if the optional preference value is designated, the preference of the configured default route is reset to its default.

Format	`no ip route default [{nexthopip | preference}]`
Mode	Global Config

7.2.0.14 ip route distance

This command sets the default distance (preference) for static routes. Lower route distance values are preferred when determining the best route. The `ip route` and `ip route default` commands allow you to optionally set the distance (preference) of an individual static route. The default distance is used when no distance is specified in these commands. Changing the default distance does not update the distance of existing static routes, even if they were assigned the original default distance. The new default distance will only be applied to static routes created after invoking the `ip route distance` command.

Default	1
Format	`ip route distance 1-255`
Mode	Global Config

7.2.0.14.1 no ip route distance

This command sets the default static route preference value in the router. Lower route preference values are preferred when determining the best route.

Format	`no ip route distance`
Mode	Global Config

7.2.0.15 ip route net-prototype

This command adds net prototype IPv4 routes to the hardware.

Format `ip route net-prototype` *`prefix/prefix-length nexthopip num-routes`*
Mode Global Config

Parameter	Description
prefix/prefix-length	The destination network and mask for the route.
nexthopip	The next-hop ip address, It must belong to an active routing interface, but it does not need to be resolved.
num-routes	The number of routes need to added into hardware starting from the given prefix argument and within the given prefix-length.

7.2.0.15.1 no ip route net-prototype

This command deletes all the net prototype IPv4 routes added to the hardware.

Format `ip route net-prototype` *`prefix/prefix-length nexthopip num-routes`*
Mode Global Config

7.2.0.16 ip route static bfd interface

This command sets up a BFD session between two directly connected neighbors specified by the local interface and the neighbor's IP address. The BFD session parameters can be set on the interface by using the existing command.

`bfd interval` *`milliseconds`* `min_rx` *`milliseconds`* `multiplier` *`interval-multiplier`*

This command is supported in IPv4 networks. The maximum number of IP static BFD sessions that can be supported is limited by the maximum BFD sessions configurable per DUT.

Format `ip route static bfd interface` *`unit/slot/port`* `|` `vlan` *`id neighbor ip address`*
Mode Global Config

Parameter	Description
interface	Specify the local interface either in unit/slot/port format or as a VLAN ID.
neighbor IP address	Specify the other end of the BFD session, peer address.

Example:

```
(localhost) #configure
(localhost) (Config)#interface 0/29
(localhost) (Interface 0/29)#routing
(localhost) (Interface 0/29)#ip address 1.1.1.1 /24
(localhost) (Interface 0/29)#bfd interval 100 min_rx 100 multiplier 5
(localhost) (Interface 0/29)#exit

(localhost) (Config)#show running-config interface 0/29

!Current Configuration:
!
interface  0/29
no shutdown
routing
```

```
ip address 1.1.1.1 255.255.255.0
bfd interval 100 min_rx 100 multiplier 5
exit

(localhost) (Config)#ip route static bfd interface 0/29 1.1.1.2
```

7.2.0.17 ip netdirbcast

This command enables the forwarding of network-directed broadcasts on an interface or range of interfaces. When enabled, network directed broadcasts are forwarded. When disabled they are dropped.

Default	disabled
Format	`ip netdirbcast`
Mode	Interface Config

7.2.0.17.1 no ip netdirbcast

This command disables the forwarding of network-directed broadcasts. When disabled, network directed broadcasts are dropped.

Format	`no ip netdirbcast`
Mode	Interface Config

7.2.0.18 ip mtu

This command sets the IP Maximum Transmission Unit (MTU) on a routing interface or range of interfaces. The IP MTU is the size of the largest IP packet that can be transmitted on the interface without fragmentation. Forwarded packets are dropped if they exceed the IP MTU of the outgoing interface.

Packets originated on the router, such as OSPF packets, may be fragmented by the IP stack.

OSPF advertises the IP MTU in the Database Description packets it sends to its neighbors during database exchange. If two OSPF neighbors advertise different IP MTUs, they will not form an adjacency. (unless OSPF has been instructed to ignore differences in IP MTU with the `ip ospf mtu-ignore` command.)

NOTE: The IP MTU size refers to the maximum size of the IP packet (IP Header + IP payload). It does not include any extra bytes that may be required for Layer-2 headers. To receive and process packets, the Ethernet MTU (see Section 5.1.0.7, mtu) must take into account the size of the Ethernet header.

Default	1500 bytes
Format	`ip mtu` *`68-9198`*
Mode	Interface Config

7.2.0.18.1 no ip mtu

This command resets the ip mtu to the default value.

Format	`no ip mtu`
Mode	Interface Config

7.2.0.19 ip unnumbered gratuitous-arp accept

This command enables the configuration of static interface routes to the unnumbered peer dynamically on receiving gratuitous ARP.

Default Interface route installation for receiving gratuitous ARP is enabled by default.
Format `ip unnumbered gratuitous-arp accept`
Mode Interface Config

7.2.0.19.1 no ip unnumbered gratuitous-arp accept

This command disables interface route configuration on receiving gratuitous ARP.

Format `no ip unnumbered gratuitous-arp accept`
Mode Interface Config

7.2.0.20 ip unnumbered loopback

This command identifies unnumbered interfaces and specifies the numbered interface providing the borrowed address. The `interface` should be loopback interface number.

Default Interfaces are numbered by default.
Format `ip unnumbered loopback` *`interface`*
Mode Interface Config

Parameter	Definition
interface	The numbered interface providing the borrowed address. This interface cannot be unnumbered. The loopback interface is identified by its loopback interface number.

7.2.0.20.1 no ip unnumbered loopback

This command removes the unnumbered configuration.

Format `no ip unnumbered loopback`
Mode Interface Config

7.2.0.21 encapsulation

This command configures the link layer encapsulation type for the packet on an interface or range of interfaces. The encapsulation type can be `ethernet` or `snap`.

Default ethernet
Format `encapsulation {ethernet | snap}`
Mode Interface Config

NOTE: Routed frames are always ethernet encapsulated when a frame is routed to a VLAN.

7.2.0.22 show dhcp lease

This command displays a list of IPv4 addresses currently leased from a DHCP server on a specific in-band interface or all in-band interfaces. This command does not apply to service or network ports.

Format `show dhcp lease [interface {slot/port | vlan id}]`

Modes Privileged EXEC

Parameter	Definition
IP address, Subnet mask	The IP address and network mask leased from the DHCP server
DHCP Lease server	The IPv4 address of the DHCP server that leased the address.
State	State of the DHCPv4 Client on this interface
DHCP transaction ID	The transaction ID of the DHCPv4 Client
Lease	The time (in seconds) that the IP address was leased by the server
Renewal	The time (in seconds) when the next DHCP renew Request is sent by DHCPv4 Client to renew the leased IP address
Rebind	The time (in seconds) when the DHCP Rebind process starts
Retry count	Number of times the DHCPv4 client sends a DHCP REQUEST message before the server responds

7.2.0.23 show ip brief

This command displays the summary information of the IP global configurations for the specified virtual router, including the ICMP rate limit configuration and the global ICMP Redirect configuration. If no router is specified, information related to the default router is displayed.

Format `show ip brief [vrf vrf-name]`

Modes
- Privileged EXEC
- User EXEC

Parameter	Definition
Default Time to Live	The computed TTL (Time to Live) of forwarding a packet from the local router to the final destination.
Routing Mode	Shows whether the routing mode is enabled or disabled.
Maximum Next Hops	The maximum number of next hops the packet can travel.
Maximum Routes	The maximum number of routes the packet can travel.
Maximum Static Routes	The maximum number of static routes that can be configured.
ICMP Rate Limit Interval	Shows how often the token bucket is initialized with burst-size tokens. *Burst-interval* is from 0 to 2147483647 milliseconds. The default *burst-interval* is 1000 msec.
ICMP Rate Limit Burst Size	Shows the number of ICMPv4 error messages that can be sent during one *burst-interval*. The range is from 1 to 200 messages. The default value is 100 messages.
ICMP Echo Replies	Shows whether ICMP Echo Replies are enabled or disabled.
ICMP Redirects	Shows whether ICMP Redirects are enabled or disabled.
System uRPF Mode	Shows whether unicast Reverse Path Forwarding (uRPF) is enabled.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip brief
```

```
Default Time to Live.......................... 64
Routing Mode.................................. Disabled
Maximum Next Hops............................. 4
Maximum Routes................................ 6000
Maximum Static Routes......................... 64
ICMP Rate Limit Interval...................... 1000 msec
ICMP Rate Limit Burst Size.................... 100 messages
ICMP Echo Replies............................. Enabled
ICMP Redirects................................ Enabled
System uRPF Mode.............................. Enabled
```

7.2.0.24 show ip interface

This command displays all pertinent information about the IP interface.

Format `show ip interface {`*`slot/port | vlan vlan-id`*`}`

Modes
- Privileged EXEC
- User EXEC

Parameter	Definition
Routing Interface Status	Determine the operational status of IPv4 routing Interface. The possible values are Up or Down.
Unnumbered	For unnumbered interfaces, the IP address of the borrowed interface.
Primary IP Address	The primary IP address and subnet masks for the interface. This value appears only if you configure it.
Method	Shows whether the IP address was configured manually or acquired from a DHCP server.
Secondary IP Address	One or more secondary IP addresses and subnet masks for the interface. This value appears only if you configure it.
Helper IP Address	The helper IP addresses configured by the command Section 7.12.0.3, ip helper-address (Interface Config).
Routing Mode	The administrative mode of router interface participation. The possible values are enable or disable. This value is configurable.
Administrative Mode	The administrative mode of the specified interface. The possible values of this field are enable or disable. This value is configurable.
Forward Net Directed Broadcasts	Displays whether forwarding of network-directed broadcasts is enabled or disabled. This value is configurable.
Active State	Displays whether the interface is active or inactive. An interface is considered active if its link is up and it is in forwarding state.
Link Speed Data Rate	An integer representing the physical link data rate of the specified interface. This is measured in Megabits per second (Mbps).
MAC Address	The burned in physical address of the specified interface. The format is 6 two-digit hexadecimal numbers that are separated by colons.
Encapsulation Type	The encapsulation type for the specified interface. The types are: Ethernet or SNAP.
IP MTU	The maximum transmission unit (MTU) size of a frame, in bytes.
Bandwidth	Shows the bandwidth of the interface.
Destination Unreachables	Displays whether ICMP Destination Unreachables may be sent (enabled or disabled).
ICMP Redirects	Displays whether ICMP Redirects may be sent (enabled or disabled).
DHCP Client Identifier	The client identifier is displayed in the output of the command only if DHCP is enabled with the **client-id** option on the in-band interface. See Section 7.2.0.4, ip address dhcp.
Interface Suppress Status	Identifies whether the interface is suppressed.

Parameter	Definition
Interface Name	The user-configured name of the interface.
Unicast Reverse Path Forwarding Mode	The uRPF mode on the interface. See Section 7.3.0.2, ip verify unicast source reachable-via
Unicast Reverse Path Forwarding Allow-Default	Identifies whether the uRPF `allow-default` parameter has been set. See Section 7.3.0.2, ip verify unicast source reachable-via

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip interface 0/1

Routing interface status..................... Up
Unnumbered - numbered interface.............. loopback 1
Unnumbered - gratuitous ARP accept........... Enable
Method....................................... N/A
Routing Mode................................. Enable
Administrative Mode.......................... Enable
Forward Net Directed Broadcasts.............. Disable
Active State................................. Active
Link Speed Data Rate......................... 1000 Full
MAC address.................................. 00:10:18:82:18:26
Encapsulation Type........................... Ethernet
IP MTU....................................... 1500
Bandwidth.................................... 1000000 kbps
Destination Unreachables..................... Enabled
ICMP Redirects............................... Enabled
Interface Suppress Status.................... Unsuppressed
Interface Name............................... rt1_0_1
Unicast Reverse Path Forwarding Mode.......... Disabled
Unicast Reverse Path Forwarding Allow-Default.. False
```

Example: In the following example the DHCP client is enabled on a VLAN routing interface.

```
(Routing) #show ip interface vlan 10

Routing Interface Status..................... Up
Method....................................... DHCP
Routing Mode................................. Enable
Administrative Mode.......................... Enable
Forward Net Directed Broadcasts.............. Disable
Active State................................. Inactive
Link Speed Data Rate......................... 10 Half
MAC address.................................. 00:10:18:82:16:0E
Encapsulation Type........................... Ethernet
IP MTU....................................... 1500
Bandwidth.................................... 10000 kbps
Destination Unreachables..................... Enabled
ICMP Redirects............................... Enabled
Interface Suppress Status.................... Unsuppressed
DHCP Client Identifier....................... 0efos-0010.1882.160E-vl10
Interface Name............................... rt_v10
```

7.2.0.25 show ip interface brief

This command displays summary information about IP configuration settings for all ports in the router, and indicates how each IP address was assigned for a specified virtual router instance. If a virtual router is not specified, the IP configuration settings cache for the default router is displayed.

Format `show ip interface [vrf vrf-name] brief`

Modes
- Privileged EXEC
- User EXEC

Parameter	Definition
Interface	Valid slot and port number separated by a forward slash.
State	Routing operational state of the interface.
IP Address	The IP address of the routing interface in 32-bit dotted decimal format. Unnumbered interfaces show unnumbered and the corresponding numbered interface instead of the IP address.
IP Mask	The IP mask of the routing interface in 32-bit dotted decimal format.
Method	Indicates how each IP address was assigned. The field contains one of the following values: ■ **DHCP** - The address is leased from a DHCP server. ■ **Manual** - The address is manually configured.

Example: The following shows example CLI display output for the command.

```
(alpha1) #show ip interface brief

Interface    State  IP Address      IP Mask         Method
----------   -----  --------------- --------------- --------
0/17       Up     192.168.75.1    255.255.255.0   DHCP
0/19       Up     unnumbered
                      -->loopback 2                 N/A
loopback 1   Down   0.0.0.0         0.0.0.0         None
loopback 2   Up     3.2.0.3         255.255.255.0   Manual
```

7.2.0.26 show ip load-sharing

This command displays the currently configured IP ECMP load balancing mode and the IPSEC SPI hashing mode.

Format `show ip load-sharing`

Mode Privileged Exec

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip load-sharing

ip load-sharing 6 inner
IPSEC Security Parameter Index (SPI) Hashing is Enabled.
```

7.2.0.27 show ip protocols

This command lists a summary of the configuration and status for each unicast routing protocol running in the specified virtual router. The command lists routing protocols which are configured and enabled. If a protocol is selected on the command line, the display will be limited to that protocol. If no virtual router is specified, the configuration and status for the default router are displayed.

Format `show ip protocols [vrf vrf-name] [bgp | ospf]`

Mode Privileged EXEC

Parameter	Description
BGP Section:	
Routing Protocol	BGP.
Router ID	The router ID configured for BGP.
Local AS Number	The AS number that the local router is in.
BGP Admin Mode	Whether BGP is globally enabled or disabled.
Maximum Paths	The maximum number of next hops in an internal or external BGP route.
Always Compare MED	Whether BGP is configured to compare the MEDs for routes received from peers in different ASs.
Maximum AS Path Length	Limit on the length of AS paths that BGP accepts from its neighbors.
Fast Internal Failover	Whether BGP immediately brings down a iBGP adjacency if the routing table manager reports that the peer address is no longer reachable.
Fast External Failover	Whether BGP immediately brings down an eBGP adjacency if the link to the neighbor goes down.
Distance	The default administrative distance (or route preference) for external, internal, and locally-originated BGP routes. The table that follows lists ranges of neighbor addresses that have been configured to override the default distance with a neighbor-specific distance. If a neighbor's address falls within one of these ranges, routes from that neighbor are assigned the configured distance. If a prefix list is configured, then the distance is only assigned to prefixes from the neighbor that are permitted by the prefix list.
Redistribution	A table showing information for each source protocol (connected, static, and ospf). For each of these sources the distribution list and route-map are shown, as well as the configured metric. Fields which are not configured are left blank. For ospf, an additional line shows the configured ospf match parameters.
Prefix List In	The global prefix list used to filter inbound routes from all neighbors.
Prefix List Out	The global prefix list used to filter outbound routes to all neighbors.
Networks Originated	The set of networks originated through a network command. Those networks that are actually advertised to neighbors are marked "active."
Neighbors	A list of configured neighbors and the inbound and outbound policies configured for each.
OSPFv2 Section:	
Routing Protocol	OSPFv2.
Router ID	The router ID configured for OSPFv2.
OSPF Admin Mode	Whether OSPF is enabled or disabled globally.
Maximum Paths	The maximum number of next hops in an OSPF route.
Routing for Networks	The address ranges configured with an OSPF network command.
Distance	The administrative distance (or "route preference") for intra-area, inter-area, and external routes.
Default Route Advertise	Whether OSPF is configured to originate a default route.
Always	Whether default advertisement depends on having a default route in the common routing table.
Metric	The metric configured to be advertised with the default route.
Metric Type	The metric type for the default route.
Redist Source	A type of routes that OSPF is redistributing.
Metric	The metric to advertise for redistributed routes of this type.

Parameter	Description
Metric Type	The metric type to adveritse for redistributed routes of this type.
Subnets	Whether OSPF redistributes subnets of classful addresses, or only classful prefixes.
Dist List	A distribute list used to filter routes of this type. Only routes that pass the distribute list are redistributed.
Number of Active Areas	The number of OSPF areas with at least one interface running on this router. Also broken down by area type.
ABR Status	Whether the router is currently an area border router. A router is an area border router if it has interfaces that are up in more than one area.
ASBR Status	Whether the router is an autonomous system boundary router. The router is an ASBR if it is redistributing any routes or originating a default route.

Example: The following shows example CLI display output for the command.

```
(Router) #show ip protocols

Routing Protocol..................... BGP
Router ID............................ 6.6.6.6
Local AS Number...................... 65001
BGP Admin Mode....................... Enable
Maximum Paths........................ Internal 32, External 32
Always compare MED ..................... FALSE
Maximum AS Path Length ................. 75
Fast Internal Failover ..................... Enable
Fast External Failover ..................... Enable

Distance............................... Ext 20 Int 200 Local 200
  Address         Wildcard        Distance    Pfx List
  -------         --------        --------    --------
  172.20.0.0      0.0.255.255           40        None
  172.21.0.0      0.0.255.255           45           1

Prefix List In....................... PfxList1
Prefix List Out...................... None

Redistributing:
Source        Metric  Dist List               Route Map
--------- ----------  ---------------------- ----------------------------
connected             connected_list
static         32120                         static_routemap
ospf                                         ospf_map
  ospf match: int ext1 nssa-ext2
Networks Originated:
     10.1.1.0 255.255.255.0 (active)
     20.1.1.0 255.255.255.0

Neighbors:
172.20.1.100
   Filter List In.................... 1
   Filter List Out................... 2
   Prefix List In.................... PfxList2
   Prefix List Out................... PfxList3
   Route Map In...................... rmapUp
   Route Map Out..................... rmapDown
172.20.5.1
   Prefix List Out................... PfxList12
```

```
Routing Protocol..................... OSPFv2
Router ID............................ 6.6.6.6
OSPF Admin Mode...................... Enable
Maximum Paths........................ 32
Routing for Networks................. 172.24.0.0 0.0.255.255 area 0
                                      10.0.0.0 0.255.255.255 area 1
                                      192.168.75.0 0.0.0.255 area 2
Distance............................. Intra 110 Inter 110 Ext 110

Default Route Advertise.............. Disabled
Always............................... FALSE
Metric............................... Not configured
Metric Type.......................... External Type 2

Redist
Source      Metric       Metric Type     Subnets    Dist List
---------  -------       -----------     -------    ---------
static     default                2         Yes         None
connected       10                2         Yes            1

Number of Active Areas............... 3 (3 normal, 0 stub, 0 nssa)
ABR Status........................... Yes
ASBR Status.......................... Yes
```

7.2.0.28 show ip route

This command displays the routing table for the specified virtual router (vrf *vrf-name*). If no router is specified, the routing table for the default router is displayed. The `ip-address` specifies the network for which the route is to be displayed and displays the best matching best-route for the address. The `mask` specifies the subnet mask for the given `ip-address`. When you use the `longer-prefixes` keyword, the `ip-address` and `mask` pair becomes the prefix, and the command displays the routes to the addresses that match that prefix. Use the `protocol` parameter to specify the protocol that installed the routes. The value for `protocol` can be *ospf, bgp,* `connected`, or *static*. Use the `all` parameter to display all routes including best and non-best routes. If you do not use the `all` parameter, the command only displays the best route.

NOTE: If you use the `connected` keyword for `protocol`, the `all` option is not available because there are no best or non-best connected routes.

Format `show ip route [vrf` *`vrf-name`*`] [{`*`ip-address [protocol`*`] | {`*`ip-address mask`*` [longer-prefixes] [`*`protocol`*`] |` *`protocol`*`} [all] | all}]`

Modes
- Privileged EXEC
- User EXEC

Parameter	Definition
Route Codes	The key for the routing protocol codes that might appear in the routing table output.

The `show ip route` command displays the routing tables in the following format:

```
Code   IP-Address/Mask [Preference/Metric] via Next-Hop, Route-Timestamp, Interface, Truncated
```

The columns for the routing table display the following information:

Parameter	Definition
Code	The codes for the routing protocols that created the routes.
Default Gateway	The IP address of the default gateway. When the system does not have a more specific route to a packet's destination, it sends the packet to the default gateway.
IP-Address/Mask	The IP-Address and mask of the destination network corresponding to this route.
Preference	The administrative distance associated with this route. Routes with low values are preferred over routes with higher values.
Metric	The cost associated with this route.
via Next-Hop	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.
Route-Timestamp	The last updated time for dynamic routes. The format of Route-Timestamp will be ■ Days:Hours:Minutes if days > = 1 ■ Hours:Minutes:Seconds if days < 1
Interface	The outgoing router interface to use when forwarding traffic to the next destination. For reject routes, the next hop interface would be Null0 interface.
T	A flag appended to a route to indicate that it is an ECMP route, but only one of its next hops has been installed in the forwarding table. The forwarding table may limit the number of ECMP routes or the number of ECMP groups. When an ECMP route cannot be installed because such a limit is reached, the route is installed with a single next hop. Such truncated routes are identified by a **T** after the interface name.

To administratively control the traffic destined to a particular network and prevent it from being forwarded through the router, you can configure a static reject route on the router. Such traffic would be discarded and the ICMP destination unreachable message is sent back to the source. This is typically used for preventing routing loops. The reject route added in the RTO is of the type **OSPF Inter-Area**. Reject routes (routes of REJECT type installed by any protocol) are not redistributed by OSPF. Reject routes are supported in OSPFv2.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip route

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
       B - BGP Derived, IA - OSPF Inter Area
       E1 - OSPF External Type 1, E2 - OSPF External Type 2
       N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2, S U - Unnumbered Peer
       L-Leaked Route, K - Kernel, P - Net Prototype

C      3.0.0.0/24 [0/1] directly connected,   0/3
S U    6.1.0.6/32 [0/0] via 0/1
S U    6.2.0.6/32 [0/0] via 0/2, MPLS Labels: {123 456}
C      12.1.0.0/24 [0/1] directly connected,   loopback 1
C      12.2.0.0/24 [0/1] directly connected,   loopback 2
C      12.3.0.0/24 [0/1] directly connected,   loopback 3
```

Example: The following shows an example of output that displays leaked routes.

Subnetwork 9.0.0.0/24 is a connected subnetwork in global table and subnet 56.6.6.0/24 is reachable via a gateway 9.0.0.2 in the global table. These two routes leak into the virtual router *Red* and leak the connected subnet 8.0.0.0/24 from *Red* to global table.

When leaking connected route in the global routing table to a virtual router, the /32 host route for the leaked host is added in the virtual router instance’s route table. Leaking of non /32 connected routes into the virtual router table from global routing table is not supported.

This enables the nodes in subnet 8.0.0.0/24 to access shared services via the global routing table. Also we add a non-leaked static route for 66.6.6.0/24 subnetwork scoped to the domain of virtual router Red.

```
(Router) (Config)#ip route vrf Red 9.0.0.2 255.255.255.255 9.0.0.2 0/26
(Router) (Config)#ip route vrf Red 56.6.6.0 255.255.255.0 9.0.0.2 0/26
(Router) (Config)#ip route vrf Red 66.6.6.0 255.255.255.0 8.0.0.2
(Router) (Config)#ip route 8.0.0.0 255.255.255.0 0/27

(Router) #show ip route vrf Red

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
       B - BGP Derived, IA - OSPF Inter Area
       E1 - OSPF External Type 1, E2 - OSPF External Type 2
       N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
   L - Leaked Route

C      8.0.0.0/24 [0/1] directly connected,   0/27
S L    9.0.0.2/32 [1/1] directly connected,   0/26
S L    56.6.6.0/24 [1/1] via 9.0.0.2,   02d:22h:15m,  0/26
S      66.6.6.0/24 [1/1] via 8.0.0.2,   01d:22h:15m,  0/27
(Router) #show ip route

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
       B - BGP Derived, IA - OSPF Inter Area
       E1 - OSPF External Type 1, E2 - OSPF External Type 2
       N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
   L - Leaked Route

C      9.0.0.0/24 [0/1] directly connected,   0/26
S L    8.0.0.0/24 [1/1] directly connected,   0/27
```

Example: The following example shows routes obtained from the kernel.

```
(Routing)#show ip route

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
       B - BGP Derived, IA - OSPF Inter Area
       E1 - OSPF External Type 1, E2 - OSPF External Type 2
       N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
       S U - Unnumbered Peer, L - Leaked Route, K - Kernel

C      1.1.1.0/24 [0/1] directly connected,   0/9
S      12.12.12.0/24 [1/0] via 1.1.1.2,   0/9
S      13.13.13.0/24 [1/0] via 1.1.1.2,   0/9
K      25.25.25.0/24 [1/3] via 1.1.1.2,   0/9
```

The routes obtained from the kernel can be configured to be redistributed in the kernel. The CLI command below (in both IPv4 and Pv6) BGP Router mode has the kernel option kernel.

```
(7001) (Config)#router bgp 65401

(7001) (Config-router)#redistribute ?

<cr>                    Press enter to execute the command.
connected               Configure redistribution of Connected routes
kernel                  Configure redistribution of Kernel routes
ospf                    Configure redistribution of OSPF routes
rip                     Configure redistribution of RIP routes
static                  Configure redistribution of Static routes
```

```
(7001) (Config-router)#address-family ipv6

(7001) (config-router-af)#redistribute ?

<cr>                    Press enter to execute the command.
connected               Configure redistribution of Connected routes
kernel                  Configure redistribution of Kernel routes
ospf                    Configure redistribution of OSPF routes
static                  Configure redistribution of Static routes
```

Example: The following shows an example of the output that displays with a hardware failure.

```
(Router) (Config)#interface 0/1
(Router) (Interface 0/1)#routing
(Router) (Interface 0/1)#ip address 9.0.0.1 255.255.255.0
(Router) (Interface 0/1)#exit
(Router) (Config)#ip route net-prototype 56.6.6.0/24 9.0.0.2 1
(Router) #show ip route

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
       B - BGP Derived, IA - OSPF Inter Area
       E1 - OSPF External Type 1, E2 - OSPF External Type 2
       N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
       S U - Unnumbered Peer, L - Leaked Route, K – Kernel
      P – Net Prototype

C      9.0.0.0/24 [0/0] directly connected,   0/1
P      56.6.6.0/24 [1/1] via 9.0.0.2,   01d:22h:15m,  0/1  hw-failure
```

7.2.0.29 show ip route ecmp-groups

This command reports all current ECMP groups in the IPv4 routing table. An ECMP group is a set of two or more next hops used in one or more routes. The groups are numbered arbitrarily from 1 to n. The output indicates the number of next hops in the group and the number of routes that use the set of next hops. The output lists the IPv4 address and outgoing interface of each next hop in each group.

Format	`show ip route ecmp-groups`
Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(router) #show ip route ecmp-groups

ECMP Group 1 with 2 next hops (used by 1 route)
  172.20.33.100 on interface 2/33
  172.20.34.100 on interface 2/34

ECMP Group 2 with 3 next hops (used by 1 route)
  172.20.32.100 on interface 2/32
  172.20.33.100 on interface 2/33
  172.20.34.100 on interface 2/34

ECMP Group 3 with 4 next hops (used by 1 route)
  172.20.31.100 on interface 2/31
  172.20.32.100 on interface 2/32
  172.20.33.100 on interface 2/33
  172.20.34.100 on interface 2/34
```

7.2.0.30 show ip route hw-failure

Use this command to display the routes that failed to be added to the hardware due to hash errors or a table full condition.

Format `show ip route hw-failure`

Mode Privileged EXEC

Example: The following example displays the command output.

```
(Routing) (Config)#ip route net-prototype 66.6.6.0/24 9.0.0.2 4

(Routing) #show ip route connected

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
       B - BGP Derived, IA - OSPF Inter Area
       E1 - OSPF External Type 1, E2 - OSPF External Type 2
       N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
       S U - Unnumbered Peer, L - Leaked Route, K - Kernel
   P - Net Prototype

C      9.0.0.0/24 [0/0] directly connected,   0/1
C      8.0.0.0/24 [0/0] directly connected,   0/2

(Routing) #show ip route hw-failure

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
       B - BGP Derived, IA - OSPF Inter Area
       E1 - OSPF External Type 1, E2 - OSPF External Type 2
       N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
       S U - Unnumbered Peer, L - Leaked Route, K - Kernel
   P - Net Prototype

P      66.6.6.0/24 [1/1] via 9.0.0.2,   01d:22h:15m,  0/1  hw-failure
P      66.6.7.0/24 [1/1] via 9.0.0.2,   01d:22h:15m,  0/1  hw-failure
P      66.6.8.0/24 [1/1] via 9.0.0.2,   01d:22h:15m,  0/1  hw-failure
P      66.6.9.0/24 [1/1] via 9.0.0.2,   01d:22h:15m,  0/1  hw-failure
```

7.2.0.31 show ip route net-prototype

This command displays the net-prototype routes. The net-prototype routes are displayed with a P.

Format `show ip route net-prototype`

Modes Privileged EXEC

Example:

```
(Routing) #show ip route net-prototype

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
       B - BGP Derived, IA - OSPF Inter Area
       E1 - OSPF External Type 1, E2 - OSPF External Type 2
       N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
       S U - Unnumbered Peer, L - Leaked Route, K - Kernel
      P - Net Prototype

P      56.6.6.0/24 [1/1] via 9.0.0.2,   01d:22h:15m,  0/1
```

```
P       56.6.7.0/24 [1/1] via 9.0.0.2,   01d:22h:15m,  0/1
```

7.2.0.32 show ip route static bfd

This command displays information about the IPv4 static BFD configured parameters configured with the `ip route static bfd` command.

Format `show ip route static bfd`

Modes Privileged EXEC

Example:

```
(localhost)#show ip route static bfd

S   1.1.1.2    via   0/28  Up
```

7.2.0.33 show ip route summary

Use this command to display the routing table summary. When the optional `all` keyword is given, some statistics, such as the number of routes from each source, include counts for alternate routes. An alternate route is a route that is not the most preferred route to its destination and therefore is not installed in the forwarding table. To include only the number of best routes, do not use the optional keyword.

Format `show ip route summary [all]`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Connected Routes	The total number of connected routes in the routing table.
Static Routes	Total number of static routes in the routing table.
RIP Routes	Total number of routes installed by RIP protocol.
BGP Routes	Total number of routes installed by the BGP protocol.
External	The number of external BGP routes.
Internal	The number of internal BGP routes.
Local	The number of local BGP routes.
OSPF Routes	Total number of routes installed by OSPF protocol.
Intra Area Routes	Total number of Intra Area routes installed by OSPF protocol.
Inter Area Routes	Total number of Inter Area routes installed by OSPF protocol.
External Type-1 Routes	Total number of External Type-1 routes installed by OSPF protocol.
External Type-2 Routes	Total number of External Type-2 routes installed by OSPF protocol.
Reject Routes	Total number of reject routes installed by all protocols.
Net Prototype Routes	The number of net-prototype routes.
Total Routes	Total number of routes in the routing table.
Best Routes (High)	The number of best routes currently in the routing table. This number only counts the best route to each destination. The value in parentheses indicates the highest count of unique best routes since counters were last cleared.

Term	Definition
Alternate Routes	The number of alternate routes currently in the routing table. An alternate route is a route that was not selected as the best route to its destination.
Route Adds	The number of routes that have been added to the routing table.
Route Modifies	The number of routes that have been changed after they were initially added to the routing table.
Route Deletes	The number of routes that have been deleted from the routing table.
Unresolved Route Adds	The number of route adds that failed because none of the route's next hops were on a local subnet. Note that static routes can fail to be added to the routing table at startup because the routing interfaces are not yet up. This counter gets incremented in this case. The static routes are added to the routing table when the routing interfaces come up.
Invalid Route Adds	The number of routes that failed to be added to the routing table because the route was invalid. A log message is written for each of these failures.
Failed Route Adds	The number of routes that failed to be added to the routing table because of a resource limitation in the routing table.
Hardware Failed Route Adds	The number of routes failed be inserted into the hardware due to hash error or a table full condition.
Reserved Locals	The number of routing table entries reserved for a local subnet on a routing interface that is down. Space for local routes is always reserved so that local routes can be installed when a routing interface bounces.
Unique Next Hops (High)	The number of distinct next hops used among all routes currently in the routing table. These include local interfaces for local routes and neighbors for indirect routes. The value in parentheses indicates the highest count of unique next hops since counters were last cleared.
Next Hop Groups (High)	The current number of next hop groups in use by one or more routes. Each next hop group includes one or more next hops. The value in parentheses indicates the highest count of next hop groups since counters were last cleared.
ECMP Groups (High)	The number of next hop groups with multiple next hops. The value in parentheses indicates the highest count of next hop groups since counters were last cleared.
ECMP Groups	The number of next hop groups with multiple next hops.
ECMP Routes	The number of routes with multiple next hops currently in the routing table.
Truncated ECMP Routes	The number of ECMP routes that are currently installed in the forwarding table with just one next hop. The forwarding table may limit the number of ECMP routes or the number of ECMP groups. When an ECMP route cannot be installed because such a limit is reached, the route is installed with a single next hop.
ECMP Retries	The number of ECMP routes that have been installed in the forwarding table after initially being installed with a single next hop.
Routes with n Next Hops	The current number of routes with each number of next hops.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip route summary
Connected Routes............................... 7
Static Routes.................................. 1
RIP Routes..................................... 20
BGP Routes..................................... 10
  External..................................... 0
  Internal..................................... 10
  Local........................................ 0
OSPF Routes.................................... 1004
  Intra Area Routes............................ 4
  Inter Area Routes............................ 1000
  External Type-1 Routes....................... 0
  External Type-2 Routes....................... 0
Reject Routes.................................. 0
Net Prototype Routes........................... 10004
```

```
Total routes..................................... 1032

Best Routes (High)............................... 1032 (1032)
Alternate Routes................................. 0
Route Adds....................................... 1010
Route Modifies................................... 1
Route Deletes.................................... 10
Unresolved Route Adds............................ 0
Invalid Route Adds............................... 0
Failed Route Adds................................ 0
Hardware Failed Route Adds....................... 4
Reserved Locals.................................. 0

Unique Next Hops (High).......................... 13 (13)
Next Hop Groups (High)........................... 13 (14)
ECMP Groups (High)............................... 2 (3)
ECMP Routes...................................... 1001
Truncated ECMP Routes............................ 0
ECMP Retries..................................... 0
Routes with 1 Next Hop........................... 31
Routes with 2 Next Hops.......................... 1
Routes with 4 Next Hops.......................... 1000
```

7.2.0.34 clear ip route counters

The command resets to zero the IPv4 routing table counters reported in the command Section 7.2.0.33, show ip route summary for the specified virtual router. If no router is specified, the command is executed for the default router. The command only resets event counters. Counters that report the current state of the routing table, such as the number of routes of each type, are not reset.

Format `clear ip route counters`

Mode Privileged EXEC

7.2.0.35 show ip route preferences

This command displays detailed information about the route preferences for each type of route. Route preferences are used in determining the best route. Lower router preference values are preferred over higher router preference values. A route with a preference of 255 cannot be used to forward traffic.

Format `show ip route preferences`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Local	The local route preference value.
Static	The static route preference value.
BGP External	The BGP external route preference value.
OSPF Intra	The OSPF Intra route preference value.
OSPF Inter	The OSPF Inter route preference value.
OSPF External	The OSPF External route preference value.

Term	Definition
RIP	The RIP route preference value.
BGP Internal	The BGP internal route preference value.
BGP Local	The BGP local route preference value.
Configured Default Gateway	The route preference value of the statically-configured default gateway
DHCP Default Gateway	The route preference value of the default gateway learned from the DHCP server.

Example: The following shows example CLI display output for the command.

```
(alpha-stack) #show ip route preferences

Local.......................................... 0
Static......................................... 1
BGP External................................... 20
OSPF Intra..................................... 110
OSPF Inter..................................... 110
OSPF External.................................. 110
RIP............................................ 120
BGP Internal................................... 200
BGP Local...................................... 200
Configured Default Gateway..................... 253
DHCP Default Gateway........................... 254
```

7.2.0.36 show ip stats

This command displays IP statistical information. for a specified virtual router instance. If a virtual router is not specified, the IP statistical information for the default router is displayed.

Format `show ip stats [vrf` *`vrf-name`*`]`

Modes
- Privileged EXEC
- User EXEC

7.2.0.37 show routing heap summary

This command displays a summary of the memory allocation from the routing heap. The routing heap is a chunk of memory set aside when the system boots for use by the routing applications.

Format `show routing heap summary`

Mode Privileged EXEC

Parameter	Description
Heap Size	The amount of memory, in bytes, allocated at startup for the routing heap.
Memory In Use	The number of bytes currently allocated.
Memory on Free List	The number of bytes currently on the free list. When a chunk of memory from the routing heap is freed, it is placed on a free list for future reuse.
Memory Available in Heap	The number of bytes in the original heap that have never been allocated.
In Use High Water Mark	The maximum memory in use since the system last rebooted.

Example: The following shows example CLI display output for the command.

```
(Router) #show routing heap summary

Heap Size ..................................... 95053184
Memory In Use ................................. 56998
Memory on Free List ........................... 47
Memory Available in Heap ...................... 94996170
In Use High Water Mark ........................ 57045
```

7.2.1 IP Event Dampening Commands

7.2.1.1 dampening

Use this command to enable IP event dampening on a routing interface.

Format `dampening [half-life period] [reuse-threshold suppress-threshold max-suppress-time [restart restart-penalty]]`

Mode Interface Config

Parameter	Description
Half-life period	The number of seconds it takes for the penalty to reduce by half. The configurable range is 1-30 seconds. Default value is 5 seconds.
Reuse Threshold	The value of the penalty at which the dampened interface is restored. The configurable range is 1-20,000. Default value is 1000.
Suppress Threshold	The value of the penalty at which the interface is dampened. The configurable range is 1-20,000. Default value is 2000.
Max Suppress Time	The maximum amount of time (in seconds) an interface can be in suppressed state after it stops flapping. The configurable range is 1-255 seconds. The default value is four times of half-life period. If half-period value is allowed to default, the maximum suppress time defaults to 20 seconds.
Restart Penalty	Penalty applied to the interface after the device reloads. The configurable range is 1-20,000. Default value is 2000.

7.2.1.1.1 no dampening

This command disables IP event dampening on a routing interface.

Format `no dampening`

Mode Interface Config

7.2.1.2 show dampening interface

This command summarizes the number of interfaces configured with dampening and the number of interfaces being suppressed.

Format `show dampening interface`

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Router)# show dampening interface
2 interfaces are configured with dampening.
1 interface is being suppressed.
```

7.2.1.3 show interface dampening

This command displays the status and configured parameters of the interfaces configured with dampening.

Format `show interface dampening`

Mode Privileged EXEC

Parameter	Description
Flaps	The number times the link state of an interface changed from UP to DOWN.
Penalty	Accumulated Penalty.
Supp	Indicates if the interface is suppressed or not.
ReuseTm	Number of seconds until the interface is allowed to come up again.
HalfL	Configured half-life period.
ReuseV	Configured reuse-threshold.
SuppV	Configured suppress threshold.
MaxSTm	Configured maximum suppress time in seconds.
MaxP	Maximum possible penalty.
Restart	Configured restart penalty.

NOTE: Note the following:

1. The CLI command Section 4.8.0.3, clear counters resets the flap count to zero.
2. The interface CLI command Section 5.1.0.8.1, no shutdown resets the suppressed state to `False`.
3. Any change in the dampening configuration resets the current penalty, reuse time and suppressed state to their default values, meaning `0`, `0`, and `FALSE` respectively.

Example: The following shows example CLI display output for the command.

```
Router# show interface dampening

Interface 0/2
Flaps    Penalty    Supp    ReuseTm    HalfL    ReuseV    SuppV    MaxSTm    MaxP    Restart
   0          0      FALSE       0          5        1000        2000        20        16000       0
Interface 0/3
Flaps    Penalty    Supp    ReuseTm    HalfL    ReuseV    SuppV    MaxSTm    MaxP    Restart
   6       1865     TRUE       18          20       1000        2001        30         2828      1500
```

7.3 Unicast Reverse Path Forwarding Commands

Unicast Reverse Path Forwarding (uRPF) is a powerful security tool that helps limit the problems that are caused by malformed or spoofed IP source addresses by discarding IP packets that lack a verifiable IP source address. For example, DoS attacks like Smurf and Tribe Flood Network (TFN) forge or rapidly change source IP addresses to cause a flood of useless packets that choke the network. Unicast RPF deflects such attacks by forwarding only packets that have source addresses that are valid and consistent with the IP routing table. This defensive action protects the network of the ISP, its customer, and the rest of the Internet.

EFOS supports two uRPF modes:

- Strict Mode: The path to the source IP address must be through the *same* interface as that on which the packet arrived
- Loose mode: The path to the source IP address can be through any interface on the device. The packet need not need to arrive on the same routing interface to which the source IP route lookup is resolved in order to pass the uRPF check

7.3.0.1 system urpf enable

This command enables the uRPF feature. When the uRPF check is enabled, the route-table is checked for source and destination IP match in parallel. For this reason, the route table capacity is reduced once this feature is enabled. A message to this effect is displayed after issuing this command. This command enables the mode for both IPv4 and IPv6.

This command also causes the IP routing to be disabled and enabled- if it was enabled prior to issuing the command.

Format	`system urpf enable`
Mode	Global Config

Example:

```
(Routing) #configure
(Routing) #system urpf enable
Warning! Enabling the system uRPF mode toggles the global routing mode in all VRFs,disrupting the L3
forwarding plane and control plane for few seconds.Enabling this mode also reduces the Route Table
capacity.
```

7.3.0.1.1 no system urpf enable

This command disables the uRPF feature in hardware. When the uRPF check is disabled the route-table capacity is restored to the previous limits

Format	`no system urpf enable`
Mode	Global Config

Example:

```
(Routing) (Config)#no system urpf enable

Warning! Disabling the system uRPF mode toggles the global routing mode in all VRFs,
disrupting the L3 forwarding plane and control plane for few seconds.
```

7.3.0.2 ip verify unicast source reachable-via

This command sets the uRPF verification mode for the routing interface.

The same command works for both IPv4 and IPv6 interfaces.

Format `ip verify unicast source reachable-via {any | rx} [allow-default]`

Mode Interface Config

Parameter	Description
any	The uRPF verification mode is set to loose. In `any` mode, a check is performed to see if the source address is reachable in the routing table and when found the packet is forwarded.
rx	The uRPF verification mode is set to strict. In `rx` mode, a check is performed to see if the source address is reachable in the routing table via the same interface as to where the packet was received and when both these conditions are met the packet is forwarded.
allow-default	Include IP addresses not specifically contained in the routing table. When `allow-default` is set in loose mode (`any`), if the source IP address is not found but a default route is present in the table, the uRPF check will pass. When`allow-default` is set in strict mode (`rx`), it will prevent the incoming packet's source IP address to have a route out of a different interface than received. The strict mode option with the default route is used typically on the upstream interface.

7.3.0.2.1 no ip verify unicast source reachable-via

This command disables the uRPF check on the routing interface.

Format `no ip verify unicast source reachable-via`

Mode Interface Config

7.4 Black Hole Detection Commands

In networking terms, *black holes* refer to places in the Clos network where incoming or outgoing traffic is silently discarded without informing the source that the data did not reach its intended recipient. Black hole conditions arise when the traffic is directed towards an incorrect path in Clos networks where uRPF is not running.

The Black Hole Detection (BHD) feature helps in getting notification logs intermittently whenever packets are getting black-holed in the network. This feature is an alternative to uRPF in Clos networks and has the advantage of not cutting the routing table in half.

7.4.0.1 bhd enable

This command enables the BHD feature globally on the system.

Default	Disabled
Format	`bhd enable`
Mode	Global Config

7.4.0.1.1 no bhd enable

This command disables the BHD feature globally on the system.

Format	`no bhd enable`
Mode	Global Config

7.4.0.2 bhd spine-port enable

This command enables the port to be monitored for black hole detection. Only routing interfaces can be enabled as BHD spine ports.

Default	Disabled.
Format	`bhd spine-port enable`
Mode	Interface Config

7.4.0.2.1 no bhd spine-port enable

This command disables the port to be monitored for black hole detection.

Format	no bhd spine-port enable
Mode	Interface Config

7.4.0.3 show bhd status

This command displays the global configuration of black hole feature along with list of ports enabled for black hole detection.

Format	`show bhd status`
Mode	Privileged Exec

Example:

```
(Routing)# show bhd status

BHD    Admin Mode             :  Enabled


Spine Port   BHD Count
----------       -------------
0/33            4000
0/34            3000
```

7.5 Policy-Based Routing Commands

The commands in this section describe IPv4 policy-based routing (PBR) commands. For information about IPv6 PBR commands, see Section 8.7, IPv6 Policy-Based Routing Commands. For information about routing policy commands for BGP, see Section 11.2, BGP Routing Policy Commands.

7.5.0.1 ip policy

Use this command to identify a route map to use for policy-based routing on an interface specified by *route-map-name*. Policy-based routing is configured on the interface that *receives* the packets, not on the interface from which the packets are sent.

When a route-map applied on the interface is changed, that is, if new statements are added to the route-map or match/set terms are added to or removed from the route-map statement, and also if the route-map that is applied on an interface is removed, the route-map needs to be removed from the interface and added back again in order for the changed route-map configuration to take effect.

A route-map statement should contain eligible match/set conditions for policy-based routing in order to be applied to hardware.

- Valid match conditions: `match ip address acl`, `match mac-list`, `match length`
- Valid set conditions: `set ip next-hop`, `set ip default next-hop`, `set ip precedence`

A route-map statement should contain at least one match condition and one set condition as specified above for it to be eligible to be applied to hardware. If not, the route-map is not applied to hardware.

NOTE: Route-map and DiffServ cannot work on the same interface.

When a route-map is applied on a VLAN interface and a DiffServ policy is applied on a member port of the same VLAN interface, the port policy takes priority over the VLAN policy.

Format	`ip policy route-map` *`route-map-name`*
Mode	Interface Config

Example: The following is an example of this command.

```
(Routing) (Config)#interface 0/1
(Routing) (Interface 0/1)#
(Routing) (Interface 0/1)# #ip policy route-map equal-access
```

To disable policy based routing from an interface, use no form of this command
`no ip policy route-map` *`route-map-name`*

When a route-map has both IPv4 and IPv6 statements provisioned and the user applies the route-map using IP policy command, the IPv6 statements in the route-map will not take effect. A message will be displayed to the user to indicate this.

Example:

```
(Routing) (Interface vlan 40)#ip policy route-map rm4
```

IPv6 statements in this route-map will not be applied using IPv4 Policy Based Routing.

7.5.0.2 route-map

To create a route map and enter Route Map Configuration mode, use the **route-map** command in Global Configuration mode. One use of a route map is to limit the redistribution of routes to a specified range of route prefixes. The redistribution command specifies a route map which refers to a prefix list. The prefix list identifies the prefixes that may be redistributed. EFOS accepts up to 64 route maps.

Default No route maps are configured by default. If no permit or deny tag is given, *permit* is the default.

Format `route-map map-tag [permit|deny] [sequence-number]`

Mode Global Configuration

Parameter	Description
map-tag	Text name of the route map. Route maps with the same name are grouped together in order of their sequence numbers. A route map name may be up to 32 characters long.
permit	(Optional) Permit routes that match all of the match conditions in the route map.
deny	(Optional) Deny routes that match all of the match conditions in the route map.
sequence-number	(Optional) An integer used to order the set of route maps with the same name. Route maps are ordered from lowest to greatest sequence number, with lower sequence numbers being considered first. If no sequence number is specified, the system assigns a value ten greater than the last statement in the route map. The range is 0 to 65,535.

Example: In the following example, BGP is configured to redistribute the all prefixes within 172.20.0.0 and reject all others.

```
(Routing)(config)# ip prefix-list redist-pl permit 172.20.0.0/16 le 32
(Routing)(config)# route-map redist-rm permit
(Routing)(config-route-map)# match ip address prefix-list redist-pl
(Routing)(config-route-map)# exit
(Routing)(config) router bgp 1
(Routing)(Config-router) redistribute ospf route-map redist-rm
```

7.5.0.2.1 no route-map

To delete a route map or one of its statements, use the no form of this command.

Format `no route-map map-tag [permit|deny] [sequence-number]`

Mode Global Configuration

7.5.0.3 match ip address <access-list-number | access-list-name>

Use this command to configure a route map in order to match based on the match criteria configured in an IP access-list. Note that an IP ACL must be configured before it is linked to a route-map. Actions present in an IP ACL configuration are applied with other actions involved in route-map. If an IP ACL referenced by a route-map is removed or rules are added or deleted from that ACL, the configuration is rejected.

If there are a list of IP access-lists specified in this command and the packet matches at least one of these access-list match criteria, the corresponding set of actions in route-map are applied to packet.

If there are duplicate IP access-list numbers/names in this command, the duplicate configuration is ignored.

Default No match criteria are defined by default.

Format `match ip address` *`access-list-number`* `|` *`access-list-name`* `[...access-list-number | name ]`

Mode Route Map Configuration

Parameter	Description
Access-list-number	The access-list number that identifies an access-list configured through access-list CLI configuration commands. This number is 1 to 99 for standard access list number. This number is 100 to 199 for extended access list number.
Access-list-name	The access-list name that identifies named IP ACLs. Access-list name can be up to 31 characters in length. A maximum of 16 ACLs can be specified in this ‘match’ clause.

Example: The following sequence shows creating a route-map with “match” clause on ACL number and applying that route-map on an interface.

```
(Routing) (config)#access-list 1 permit ip 10.1.0.0 0.0.255.255
(Routing) (config)#access-list 2 permit ip 10.2.0.0 0.0.255.255
(Routing) (config)#route-map equal-access permit 10
(Routing) (config-route-map)#match ip address 1
(Routing) (config-route-map)#set ip default next-hop 192.168.6.6
(Routing) (config-route-map)#route-map equal-access permit 20
(Routing) (config-route-map)#match ip address 2
(Routing) (config-route-map)#set ip default next-hop 172.16.7.7
(Routing) (config)#interface 0/1
(Routing) (Interface 0/1)#ip address 10.1.1.1 255.255.255.0
(Routing) (Interface 0/1)#ip policy route-map equal-access
(Routing) (config)#interface 0/2
(Routing) (Interface 0/2)#ip address 192.168.6.5 255.255.255.0
(Routing) (config)#interface 0/3
(Routing) (Interface 0/3)#ip address 172.16.7.6 255.255.255.0
The ip policy route-map equal-access command is applied to interface 0/1. All packets coming inside
0/1 are policy-routed.
Sequence number 10 in route map equal-access is used to match all packets sourced from any host in
subnet 10.1.0.0. If there is a match, and if the router has no explicit route for the packet’s
destination, it is sent to next-hop address 192.168.6.6 .
Sequence number 20 in route map equal-access is used to match all packets sourced from any host in
subnet 10.2.0.0. If there is a match, and if the router has no explicit route for the packet’s
destination, it is sent to next-hop address 172.16.7.7.
Rest all packets are forwarded as per normal L3 destination-based routing.
```

Example: This example illustrates the scenario where IP ACL referenced by a route-map is removed or rules are added or deleted from that ACL, this is how configuration is rejected:

```
(Routing) #show ip access-lists

ACL Counters: Enabled
Current number of ACLs: 9  Maximum number of ACLs: 100

ACL ID/Name                     Rules  Direction  Interface(s)      VLAN(s)
------------------------------  -----  ---------  ----------------  ----------
1                               1
2                               1
3                               1
4                               1
5                               1
```

```
madan                           1

(Routing) #show mac access-lists

ACL Counters: Enabled
Current number of all ACLs: 9  Maximum number of all ACLs: 100

MAC ACL Name                    Rules  Direction  Interface(s)       VLAN(s)
------------------------------  -----  ---------  ----------------  ----------
madan                           1
mohan                           1
goud                            1

(Routing) #
(Routing) #configure

(Routing) (Config)#route-map madan

(Routing) (route-map)#match ip address 1 2 3 4 5 madan

(Routing) (route-map)#match mac-list madan mohan goud

(Routing) (route-map)#exit

(Routing) (Config)#exit

(Routing) #show route-map

route-map madan permit 10
     Match clauses:
       ip address (access-lists) : 1 2 3 4 5 madan
       mac-list (access-lists) : madan mohan goud
     Set clauses:

(Routing) (Config)#access-list 2 permit every

Request denied. Another application using this ACL restricts the number of rules allowed.

(Routing) (Config)#ip access-list madan

(Routing) (Config-ipv4-acl)#permit udp any any

Request denied. Another application using this ACL restricts the number of rules allowed.
```

7.5.0.3.1 no match ip address

To delete a match statement from a route map, use the **no** form of this command.

Format `no match ip address [`*`access-list-number`* | *`access-list-name`*`]`

Mode Route Map Configuration

7.5.0.4 match length

Use this command to configure a route map to match based on the Layer 3 packet length between specified minimum and maximum values. The *min* parameter specifies the packet's minimum Layer 3 length, inclusive, allowed for a match. The *max* parameter specifies the packet's maximum Layer 3 length, inclusive, allowed for a match. Each route-map statement can contain one match statement on packet length range.

NOTE: This command is available for both IPv4 and IPv6 traffic. This command can policy route IPv4/IPv6 traffic for a length match and an access-list match condition in addition to the match IPv4/IPv6 access-list condition.

Default No match criteria are defined by default.

Format `match length min max`

Mode Route Map Configuration

Example: The following shows an example of the command.

```
(Routing) (config-route-map)# match length 64 1500
```

7.5.0.4.1 no match length

Use this command to delete a match statement from a route map.

Format `no match length`

Mode Route Map Configuration

7.5.0.5 match mac-list

Use this command to configure a route map in order to match based on the match criteria configured in an MAC access-list.

A MAC ACL is configured before it is linked to a route-map. Actions present in MAC ACL configuration are applied with other actions involved in route-map. When a MAC ACL referenced by a route-map is removed, the route-map rule is also removed and the corresponding rule is not effective. When a MAC ACL referenced by a route-map is removed or rules are added or deleted from that ACL, the configuration is rejected.

Default No match criteria are defined by default.

Format `match mac-list mac-list-name [mac-list-name]`

Mode Route Map Configuration

Parameter	Description
mac-list-name	The mac-list name that identifies MAC ACLs. MAC Access-list name can be up to 31 characters in length.

Example: The following is an example of the command.

```
(Routing) (config-route-map)# match mac-list MacList1

Example 2:
This example illustrates the scenario where MAC ACL referenced by a route-map is removed or rules are
added or deleted from that ACL, this is how configuration is rejected:

(Routing) #show mac access-lists
```

```
ACL Counters: Enabled
Current number of all ACLs: 9  Maximum number of all ACLs: 100

MAC ACL Name                     Rules  Direction  Interface(s)       VLAN(s)
-------------------------------  -----  ---------  ----------------  ----------
madan                            1
mohan                            1
goud                             1

(Routing) #
(Routing) #
(Routing) #configure

(Routing) (Config)#route-map madan

(Routing) (route-map)#match mac-list madan mohan goud

(Routing) (route-map)#exit

(Routing) (Config)#exit

(Routing) #show route-map

route-map madan permit 10
     Match clauses:
       mac-list (access-lists) : madan mohan goud
     Set clauses:

(Routing) (Config)#mac access-list extended madan
(Routing) (Config-mac-access-list)#permit 00:00:00:00:00:01 ff:ff:ff:ff:ff:ff any
Request denied. Another application using this ACL restricts the number of rules allowed.
```

7.5.0.5.1 no match mac-list

To delete a match statement from a route map, use the **no** form of this command.

Format `no match mac-list […mac-list-name]`

Mode Route Map Configuration

7.5.0.6 set interface

If network administrator does not want to revert to normal forwarding but instead want to drop a packet that does not match the specified criteria, a set statement needs to be configured to route the packets to interface null 0 as the last entry in the route-map. `set interface null0` needs to be configured in a separate statement. It should not be added along with any other statement having other match/set terms.

A route-map statement that is used for PBR is configured as permit or deny. If the statement is marked as deny, traditional destination-based routing is performed on the packet meeting the match criteria. If the statement is marked as permit, and if the packet meets all the match criteria, then set commands in the route-map statement are applied. If no match is found in the route-map, the packet is not dropped, instead the packet is forwarded using the routing decision taken by performing destination-based routing.

NOTE: This command can be used with both IPv4 and IPv6 traffic.

Format `set interface null0`
Mode Route Map Configuration

7.5.0.7 set ip next-hop

Use this command to specify the adjacent next-hop router in the path toward the destination to which the packets should be forwarded. If more than one IP address is specified, the first IP address associated with a currently up-connected interface is used to route the packets.

This command affects all incoming packet types and is always used if configured. If configured next-hop is not present in the routing table, an ARP request is sent from the router.

In a route-map statement, ‘set ip next-hop’ and ‘set ip default next-hop’ terms are mutually exclusive. However, a ‘set ip default next-hop’ can be configured in a separate route-map statement.

Format `set ip next-hop ip-address [...ip-address]`
Mode Route Map Configuration

Parameter	Description
ip-address	The IP address of the next hop to which packets are output. It must be the address of an adjacent router. A maximum of 16 next-hop IP addresses can be specified in this ‘set’ clause.

7.5.0.7.1 no set ip next-hop

Use this command to remove a set command from a route map.

Format `no set ip next-hop ip-address [...ip-address]`
Mode Route Map Configuration

7.5.0.8 set ip default next-hop

Use this command to set a list of default next-hop IP addresses. If more than one IP address is specified, the first next hop specified that appears to be adjacent to the router is used. The optional specified IP addresses are tried in turn.

A packet is routed to the next hop specified by this command only if there is *no* explicit route for the packet’s destination address in the routing table. A default route in the routing table is not considered an explicit route for an unknown destination address.

In a route-map statement, `set ip next-hop` and `set ip default next-hop` terms are mutually exclusive. However, a `set ip next-hop` can be configured in a separate route-map statement

Format `set ip default next-hop ip-address [...ip-address]`
Mode Route Map Configuration

Parameter	Description
ip-address	The IP address of the next hop to which packets are output. It must be the address of an adjacent router. A maximum of 16 next-hop IP addresses can be specified in this 'set' clause.

7.5.0.8.1 no set ip default next-hop

Use this command to remove a set command from a route map.

Format `no set ip default next-hop ip-address [...ip-address]`
Mode Route Map Configuration

7.5.0.9 set ip precedence

Use this command to set the three IP precedence bits in the IP packet header. With three bits, you have eight possible values for the IP precedence; values 0 through 7 are defined. This command is used when implementing QoS and can be used by other QoS services, such as weighted fair queuing (WFQ) and weighted random early detection (WRED).

Format `set ip precedence 0-7`
Mode Route Map Configuration

Parameter	Description
0	Sets the routine precedence
1	Sets the priority precedence
2	Sets the immediate precedence
3	Sets the Flash precedence
4	Sets the Flash override precedence
5	Sets the critical precedence
6	Sets the internetwork control precedence
7	Sets the network control precedence

7.5.0.9.1 no set ip precedence

Use this command to reset the three IP precedence bits in the IP packet header to the default.

Format `no set ip precedence`
Mode Route Map Configuration

7.5.0.10 show ip policy

This command lists the route map associated with each interface.

Format `show ip policy`
Mode Privileged EXEC

Term	Definition
Interface	The interface.
Route-map	The route map

7.5.0.11 show route-map

To display a route map, use the `show route-map` command in Privileged EXEC mode.

Format `show route-map [`*`map-name`*`]`
Mode Privileged EXEC

Parameter	Description
map-name	(Optional) Name of a specific route map.

Example: The following shows example CLI display output for the command.

```
(Routing) # show route-map test
route-map test, permit, sequence 10
     Match clauses:
       ip address prefix-lists: orange
        Set clauses:
          set metric 50
```

Example: The following example shows a route map, *test1,* that is configured with extended community attributes:

```
(R1) # show route-map test
route-map test1, permit, sequence 10
     Match clauses:
       extended community list1
        Set clauses:
          extended community RT:1:100 RT:2:200
```

Example: With the inclusion of policy-based routing, more *match* and *set* clauses are added. For each sequence number, match count is shown in terms of the number of packets and number of bytes. This counter displays match count in packets and bytes when the route-map is applied. When a route-map is created/removed from interface, this count is shown to be zero. The following example shows the behavior of counters along with how they are displayed when a route-map is applied and removed from an interface:

```
(Routing) #show route-map simplest

route-map simplest permit 10
    Match clauses:
      ip address (access-lists) : 1
    Set clauses:
      ip next-hop 3.3.3.3
      ip precedence 3
Policy routing matches: 0 packets, 0 bytes
route-map simplest permit 20
    Match clauses:
      ip address (access-lists) : 1
    Set clauses:
      ip default next-hop 4.4.4.4
      ip precedence 4
Policy routing matches: 0 packets, 0 bytes
```

```
route-map simplest permit 30
    Match clauses:
    Set clauses:
      interface null0
Policy routing matches: 0 packets, 0 bytes

(Routing) #
(Routing) #configure

(Routing) (Config)#interface 0/2

(Routing) (Interface 0/2)#ip policy simplest

(Routing) (Interface 0/2)#show route-map simplest

route-map simplest permit 10
    Match clauses:
      ip address (access-lists) : 1
    Set clauses:
      ip next-hop 3.3.3.3
      ip precedence 3
Policy routing matches: 5387983 packets, 344831232 bytes
route-map simplest permit 20
    Match clauses:
      ip address (access-lists) : 1
    Set clauses:
      ip default next-hop 4.4.4.4
      ip precedence 4
Policy routing matches: 0 packets, 0 bytes
route-map simplest permit 30
    Match clauses:
    Set clauses:
      interface null0
Policy routing matches: 0 packets, 0 bytes
(Routing) (Interface 0/2)#
(Routing) (Interface 0/2)#no ip policy simplest

(Routing) (Interface 0/2)#exit

(Routing) (Config)#exit

(Routing) #show route-map simplest

route-map simplest permit 10
    Match clauses:
      ip address (access-lists) : 1
    Set clauses:
      ip next-hop 3.3.3.3
      ip precedence 3
Policy routing matches: 0 packets, 0 bytes
route-map simplest permit 20
    Match clauses:
      ip address (access-lists) : 1
    Set clauses:
      ip default next-hop 4.4.4.4
      ip precedence 4
Policy routing matches: 0 packets, 0 bytes
route-map simplest permit 30
```

```
    Match clauses:
    Set clauses:
      interface null0
Policy routing matches: 0 packets, 0 bytes
```

Example: The following output shows an example of the command when the specified route map is IPv6-based.

```
(dhcp-10-130-84-138)#show route-map

route-map rm6 permit 10
     Match clauses:
       ipv6 address (access-lists) : acl6
     Set clauses:
       ipv6 next-hop 3001::2 2001::2 5001::2 6001::2
       ipv6 next-hop interface fe80::200:6bff:fee4:35a, via 3/3
Policy routing matches: 0 packets, 0 bytes

route-map rmdef permit 10
     Match clauses:
       ipv6 address (access-lists) : acl6
     Set clauses:
       ipv6 default next-hop 1001::2
       ipv6 default next-hop interface fe80::200:6bff:fee4:35a, via 3/3
Policy routing matches: 0 packets, 0 bytes
```

7.6 Router Discovery Protocol Commands

This section describes the commands you use to view and configure Router Discovery Protocol settings on the switch. The Router Discovery Protocol enables a host to discover the IP address of routers on the subnet.

7.6.0.1 ip irdp

This command enables Router Discovery on an interface or range of interfaces.

Default disabled

Format `ip irdp`

Mode Interface Config

7.6.0.1.1 no ip irdp

This command disables Router Discovery on an interface.

Format `no ip irdp`

Mode Interface Config

7.6.0.2 ip irdp address

This command configures the address that the interface uses to send the router discovery advertisements. The valid value for `ipaddr` is 255.255.255.255, which is the limited broadcast address.

Default 224.0.0.1

Format `ip irdp address` *`ipaddr`*

Mode Interface Config

7.6.0.2.1 no ip irdp address

This command configures the default address used to advertise the router for the interface.

Format `no ip irdp address`

Mode Interface Config

7.6.0.3 ip irdp holdtime

This command configures the value, in seconds, of the holdtime field of the router advertisement sent from this interface. The holdtime range is the value of `maxadvertinterval` to 9000 seconds.

Default 3 * maxinterval

Format `ip irdp holdtime` *`maxadvertinterval-9000`*

Mode Interface Config

7.6.0.3.1 no ip irdp holdtime

This command configures the default value, in seconds, of the holdtime field of the router advertisement sent from this interface.

Format `no ip irdp holdtime`

Mode Interface Config

7.6.0.4 ip irdp maxadvertinterval

This command configures the maximum time, in seconds, allowed between sending router advertisements from the interface. The range for maxadvertinterval is 4 to 1800 seconds.

Default 600

Format `ip irdp maxadvertinterval` *`4-1800`*

Mode Interface Config

7.6.0.4.1 no ip irdp maxadvertinterval

This command configures the default maximum time, in seconds.

Format `no ip irdp maxadvertinterval`

Mode Interface Config

7.6.0.5 ip irdp minadvertinterval

This command configures the minimum time, in seconds, allowed between sending router advertisements from the interface. The range for minadvertinterval is three to the value of maxadvertinterval.

Default 0.75 * maxadvertinterval

Format `ip irdp minadvertinterval` *`3-maxadvertinterval`*

Mode Interface Config

7.6.0.5.1 no ip irdp minadvertinterval

This command sets the default minimum time to the default.

Format `no ip irdp minadvertinterval`

Mode Interface Config

7.6.0.6 ip irdp preference

This command configures the preferability of the address as a default router address, relative to other router addresses on the same subnet.

Default 0

Format `ip irdp preference` *`-2147483648 to 2147483647`*

Mode Interface Config

7.6.0.6.1 no ip irdp preference

This command configures the default preferability of the address as a default router address, relative to other router addresses on the same subnet.

Format `no ip irdp preference`

Mode Interface Config

7.6.0.7 show ip irdp

This command displays the router discovery information for all interfaces, or a specified interface.

Format `show ip irdp {`*`slot/port`* `|` `vlan` *`vlan-id`* `|` `all}`

Modes
- Privileged EXEC
- User EXEC

Parameter	Definition
Interface	The interface (*slot/port* or VLAN) that matches the rest of the information in the row.
Ad Mode	The advertise mode, which indicates whether router discovery is enabled or disabled on this interface.
Dest Address	The destination IP address for router advertisements.
Max Int	The maximum advertise interval, which is the maximum time, in seconds, allowed between sending router advertisements from the interface.
Min Int	The minimum advertise interval, which is the minimum time, in seconds, allowed between sending router advertisements from the interface.
Hold Time	The amount of time, in seconds, that a system should keep the router advertisement before discarding it.
Preference	The preference of the address as a default router address, relative to other router addresses on the same subnet.

7.7 Virtual Router Commands

7.7.0.1 ip vrf

This command creates a virtual router with a specified name and enters VRF configuration mode.

Default No VRs are defined

Format `ip vrf` *`vrf-name`*

Mode Global Config

Parameter	Description
vrf-name	The name of the virtual router. The name is a string of up to 64 characters from an ASCII set.

Example:

The following example creates two virtual router instances. The routing in the virtual router instance is enabled only when '*ip routing*' command is issued at the virtual router level.

```
(Router) (Config)#ip vrf Red
(Router) (Config-vrf-Red)#ip routing
(Router) (Config-vrf-Red)#exit
(Router) (Config)#ip vrf Blue
(Router) (Config-vrf-Blue)#ip routing
(Router) (Config-vrf-Blue)#exit
```

7.7.0.1.1 no ip vrf

Deletes the virtual router with the specified name.

Format `no ip vrf` *`vrf-name`*

Mode Global Config

7.7.0.2 maximum routes

This command reserves the number of routes allowed and sets the maximum limit on the number of routes for a virtual router instance in the total routing table space for the router, provided there is enough free space in the router's total routing table.

Default Limited by the number of free routes available.

Format `maximum routes {`*`limit`* `| warn` *`threshold`*`}`

Mode Virtual Router Config

Parameter	Description
limit	The number of routes for a virtual router instance in the total routing table space for the router. The limit ranges from 1 to 4294967295. If the limit value is greater than the total router table size, it is limited to the total size.

Parameter	Description
warn threshold	The threshold value ranges from 1 to 100 and indicates the percent of the limit value at which a warning message is to be generated. If no limit value is given the platform maximum is taken as the limit value.

7.7.0.2.1 no maximum routes

This command removes any reservation for the number of routes allowed in the virtual router instance and clears the warning threshold value.

Format `no maximum routes`
Mode Virtual Router Config

Example:

```
(Router) (Config)#ip vrf Red
(Router) (Config-vrf-Red)#ip routing
(Router) (Config-vrf-Red)#maximum routes 2048
(Router) (Config-vrf-Red)#maximum routes warn 80
(Router) (Config-vrf-Red)#exit
(Router) (Config)#ip vrf Blue
(Router) (Config-vrf-Blue)#ip routing
(Router) (Config-vrf-Blue)#maximum routes 4096
(Router) (Config-vrf-Blue)#exit
```

7.7.0.3 description

This command allows the user to configure a descriptive text for a virtual router.

Default None.
Format `description` *`text`*
Mode Virtual Router Config

Parameter	Description
text	The descriptive text for the virtual router. A set of ASCII characters up to 512 characters in length.

7.7.0.3.1 no description

This command removes the descriptive text configuration for a virtual router.

Format `no description`
Mode Virtual Router Config

7.7.0.4 ip vrf forwarding

This command associates an IP interface with a virtual router.

Default Default router

Format `ip vrf forwarding` *`vrf-name`*
Mode Interface Config

Parameter	Description
vrf-name	The name of the virtual router.

Example: This example creates two virtual router instances and assigns interfaces to those virtual routers.

```
(Router) (Config)#ip vrf Red
(Router) (Config)#ip vrf Blue
(Router) (Config)#interface 0/1
(Router) (Interface 0/1)#ip vrf forwarding Red
(Router) (Interface 0/1)#exit
(Router) (Config)#interface 0/2
(Router) (Interface 0/2)#ip vrf forwarding Blue
(Router) (Interface 0/2)#exit
```

7.7.0.4.1 no ip vrf forwarding

This command disassociates an IP interface from the configured virtual router and associates it back to the default router.

Format `no ip vrf forwarding`
Mode Interface Config

7.7.0.5 show ip vrf

This command displays information about the virtual router instances.

Default
Format `show ip vrf [{`*`vrf-name`* `| detail` *`vrf-name`* `| interfaces | memory [`*`vrf-name`*`]}]`
Mode Privileged EXEC

Parameter	Description
vrf-name	Name of the virtual router instance.
detail	Displays the configuration and status of the virtual router.
interfaces	Displays the list of interfaces and the virtual routers to which they belong.
memory	Displays the runtime memory utilization of the processes running in a virtual router.

Example:

```
Router# show ip vrf
Number of VRs.........3
Name      Identifier     Route Distinguisher
---------------------
Red            2         2:200
Blue           4         4:400
Green          3         3:300

Router# show ip vrf Red
VRF Identifier..........2
```

```
Description.............”India office bangalore”
Route Distinguisher.....2:200
Maximum Routes..........512
Threshold...............80%
Warning-only............TRUE

(Routing) #show ip vrf detail red

VRF Identifier.................................. 1
Description.....................................
Route Distinguisher............................. 300:6
Maximum Routes.................................. Not Set
Warning-only.................................... FALSE

Route table size................................ 0
Number of interfaces............................ 1

Interfaces:
-----------
0/10

Export VPN route-target communities
    RT:152:1
Import VPN route-target communities
    RT:152:1
```

7.8 Virtual LAN Routing Commands

This section describes the commands you use to view and configure VLAN routing and to view VLAN routing status information.

7.8.0.1 vlan routing

This command enables routing on a VLAN. The `vlanid` value has a range from 1 to 4093. The `[interface ID]` value has a range from 1 to 128. Typically, you will not supply the interface ID argument, and the system automatically selects the interface ID. However, if you specify an interface ID, the interface ID becomes the port number in the *`slot/port`* for the VLAN routing interface. If you select an interface ID that is already in use, the CLI displays an error message and does not create the VLAN interface. For products that use text-based configuration, including the interface ID in the vlan routing command for the text configuration ensures that the *`slot/port`* for the VLAN interface stays the same across a restart. Keeping the *`slot/port`* the same ensures that the correct interface configuration is applied to each interface when the system restarts.

Format `vlan routing` *`vlanid`* `[`*`interface ID`*`]`
Mode VLAN Database

7.8.0.1.1 no vlan routing

This command deletes routing on a VLAN.

Format `no vlan routing` *`vlanid`*
Mode VLAN Database

Example: Example 1 shows the command specifying a vlanid value. The interface ID argument is not used.

```
(Routing) (Vlan)#vlan 14
(Routing) (Vlan)#vlan routing 14 ?
<cr>                    Press enter to execute the command.
<1-128>                 Enter interface ID
```

Typically, you press **<Enter>** without supplying the Interface ID value; the system automatically selects the interface ID.

Example: In Example 2, the command specifies interface ID 51 for VLAN 14 interface. The interface ID becomes the port number in the *`slot/port`* for the VLAN routing interface. In this example, *`slot/port`* is 4/51 for VLAN 14 interface.

```
(Routing) (Vlan)#vlan 14 51
(Routing) (Vlan)#
(Routing) #show ip vlan
MAC Address used by Routing VLANs:   00:11:88:59:47:36

           Logical
VLAN ID   Interface        IP Address       Subnet Mask
-------  -------------  ---------------  ---------------
10       4/1            172.16.10.1      255.255.255.0
11       4/50           172.16.11.1      255.255.255.0
12       4/3            172.16.12.1      255.255.255.0
13       4/4            172.16.13.1      255.255.255.0
14       4/51           0.0.0.0          0.0.0.0  <--s/p is 4/51 for VLAN 14 interface
```

Example: In Example 3, you select an interface ID that is already in use. In this case, the CLI displays an error message and does not create the VLAN interface.

```
(Routing) #show ip vlan

MAC Address used by Routing VLANs:   00:11:88:59:47:36

           Logical
VLAN ID   Interface        IP Address       Subnet Mask
-------  --------------  ---------------  ---------------
10       4/1             172.16.10.1      255.255.255.0
11       4/50            172.16.11.1      255.255.255.0
12       4/3             172.16.12.1      255.255.255.0
13       4/4             172.16.13.1      255.255.255.0
14       4/51            0.0.0.0          0.0.0.0

(Routing) #config

(Routing) (Config)#exit

(Routing) #vlan database

(Routing) (Vlan)#vlan 15

(Routing) (Vlan)#vlan routing 15 1

Interface ID 1 is already assigned to another interface
```

Example: The show running configuration command always lists the interface ID for each routing VLAN, as shown in Example 4 below.

```
(Routing) #show running-config
!Current Configuration:
!
!System Description "Broadcom Trident 56846 Development System - 48xTenGig + 4 FortyGig , 1.2.0.3,
Linux 2.6.34.6"
!System Software Version "1.2.0.3"
!System Up Time          "4 days 19 hrs 5 mins 38 secs"
!Cut-through mode is configured as disabled
!Additional Packages     BGP-4,QOS,IPv6,IPv6 Management,Routing,Data Center
!Current SNTP Synchronized Time: Not Synchronized
!
set prompt "02.08"
network protocol dhcp
vlan database
vlan 10-14
vlan routing 10 1
vlan routing 12 3
vlan routing 13 4
vlan routing 11 50
vlan routing 14 51
```

7.8.0.2 interface vlan

Use this command to enter Interface configuration mode for the specified VLAN routing interface.

Format `interface vlan 1-4093`

Mode Global Config

7.8.0.3 show ip vlan

This command displays the VLAN routing information for all VLANs with routing enabled.

Format `show ip vlan`

Modes
- Privileged EXEC
- User EXEC

Parameter	Definition
MAC Address used by Routing VLANs	The MAC Address associated with the internal bridge-router interface (IBRI). The same MAC Address is used by all VLAN routing interfaces. It will be displayed above the per-VLAN information.
VLAN ID	The identifier of the VLAN.
Logical Interface	The logical *slot/port* associated with the VLAN routing interface.
IP Address	The IP address associated with this VLAN.
Subnet Mask	The subnet mask that is associated with this VLAN.

7.9 Virtual Router Redundancy Protocol Commands

This section describes the commands you use to view and configure Virtual Router Redundancy Protocol (VRRP) and to view VRRP status information. VRRP helps provide failover and load balancing when you configure two devices as a VRRP pair.

7.9.0.1 ip vrrp (Global Config)

Use this command in Global Config mode to enable the administrative mode of VRRP on the router.

Default none

Format `ip vrrp`

Mode Global Config

7.9.0.1.1 no ip vrrp

Use this command in Global Config mode to disable the default administrative mode of VRRP on the router.

Format `no ip vrrp`

Mode Global Config

7.9.0.2 ip vrrp (Interface Config)

Use this command in Interface Config mode to create a virtual router associated with the interface or range of interfaces. The parameter `vrid` is the virtual router ID, which has an integer value range from 1 to 255.

Format `ip vrrp` *`vrid`*

Mode Interface Config

7.9.0.2.1 no ip vrrp

Use this command in Interface Config mode to delete the virtual router associated with the interface. The virtual Router ID, `vrid`, is an integer value that ranges from 1 to 255.

Format `no ip vrrp` *`vrid`*

Mode Interface Config

7.9.0.3 ip vrrp mode

This command enables the virtual router configured on the specified interface. Enabling the status field starts a virtual router. The parameter `vrid` is the virtual router ID which has an integer value ranging from 1 to 255.

Default disabled

Format `ip vrrp` *`vrid`* `mode`

Mode Interface Config

7.9.0.3.1 no ip vrrp mode

This command disables the virtual router configured on the specified interface. Disabling the status field stops a virtual router.

Format `no ip vrrp vrid mode`
Mode Interface Config

7.9.0.4 ip vrrp ip

This command sets the virtual router IP address value for an interface or range of interfaces. The value for `ipaddr` is the IP address which is to be configured on that interface for VRRP. The parameter `vrid` is the virtual router ID which has an integer value range from 1 to 255. You can use the optional `[secondary]` parameter to designate the IP address as a secondary IP address.

Default none
Format `ip vrrp vrid ip ipaddr [secondary]`
Mode Interface Config

7.9.0.4.1 no ip vrrp ip

Use this command in Interface Config mode to delete a secondary IP address value from the interface. To delete the primary IP address, you must delete the virtual router on the interface.

Format `no ip vrrp vrid ipaddress secondary`
Mode Interface Config

7.9.0.5 ip vrrp accept-mode

Use this command to allow the VRRP Master to accept ping packets sent to one of the virtual router's IP addresses.

NOTE: VRRP accept-mode allows only ICMP Echo Request packets. No other type of packet is allowed to be delivered to a VRRP address.

Default disabled
Format `ip vrrp vrid accept-mode`
Mode Interface Config

7.9.0.5.1 no ip vrrp accept-mode

Use this command to prevent the VRRP Master from accepting ping packets sent to one of the virtual router's IP addresses.

Format `no ip vrrp vrid accept-mode`
Mode Interface Config

7.9.0.6 ip vrrp authentication

This command sets the authorization details value for the virtual router configured on a specified interface or range of interfaces. The parameter `{none | simple}` specifies the authorization type for virtual router configured on the specified interface. The parameter `[key]` is optional, it is only required when authorization type is simple text password. The parameter `vrid` is the virtual router ID which has an integer value ranges from 1 to 255.

Default no authorization
Format `ip vrrp vrid authentication {none | simple key}`

Mode ■ Interface Config

7.9.0.6.1 no ip vrrp authentication

This command sets the default authorization details value for the virtual router configured on a specified interface or range of interfaces.

Format `no ip vrrp` ***vrid*** `authentication`

Mode ■ Interface Config

7.9.0.7 ip vrrp preempt

This command sets the preemption mode value for the virtual router configured on a specified interface or range of interfaces. The parameter `vrid` is the virtual router ID, which is an integer from 1 to 255.

Default enabled

Format `ip vrrp` ***vrid*** `preempt`

Mode ■ Interface Config

7.9.0.7.1 no ip vrrp preempt

This command sets the default preemption mode value for the virtual router configured on a specified interface or range of interfaces.

Format `no ip vrrp` ***vrid*** `preempt`

Mode ■ Interface Config

7.9.0.8 ip vrrp priority

This command sets the priority of a router within a VRRP group. It can be used to configure an interface or a range of interfaces. Higher values equal higher priority. The range is from 1 to 254. The parameter `vrid` is the virtual router ID, whose range is from 1 to 255.

The router with the highest priority is elected master. If a router is configured with the address used as the address of the virtual router, the router is called the “address owner.” The priority of the address owner is always 255 so that the address owner is always master. If the master has a priority less than 255 (it is not the address owner) and you configure the priority of another router in the group higher than the master’s priority, the router will take over as master only if preempt mode is enabled.

Default 100 unless the router is the address owner, in which case its priority is automatically set to 255.

Format `ip vrrp` ***vrid*** `priority` ***1-254***

Mode ■ Interface Config

7.9.0.8.1 no ip vrrp priority

This command sets the default priority value for the virtual router configured on a specified interface or range of interfaces.

Format `no ip vrrp` ***vrid*** `priority`

Mode Interface Config

7.9.0.9 ip vrrp timers advertise

This command sets the frequency, in seconds, that an interface or range of interfaces on the specified virtual router sends a virtual router advertisement.

Default 1

Format `ip vrrp vrid timers advertise 1-255`

Mode Interface Config

7.9.0.9.1 no ip vrrp timers advertise

This command sets the default virtual router advertisement value for an interface or range of interfaces.

Format `no ip vrrp vrid timers advertise`

Mode Interface Config

7.9.0.10 ip vrrp track interface

Use this command to alter the priority of the VRRP router based on the availability of its interfaces. This command is useful for tracking interfaces that are not configured for VRRP. Only IP interfaces are tracked. A tracked interface is up if the IP on that interface is up. Otherwise, the tracked interface is down. You can use this command to configure a single interface or a range of interfaces.

When the tracked interface is down or the interface has been removed from the router, the priority of the VRRP router will be decremented by the value specified in the `priority` argument. When the interface is up for IP protocol, the priority will be incremented by the `priority` value.

A VRRP configured interface can track more than one interface. When a tracked interface goes down, then the priority of the router will be decreased by 10 (the default priority decrement) for each downed interface. The default priority decrement is changed using the `priority` argument. The default priority of the virtual router is 100, and the default decrement priority is 10. By default, no interfaces are tracked. If you specify just the interface to be tracked, without giving the optional priority, then the default priority will be set. The default priority decrement is 10.

Default priority: 10

Format `ip vrrp vrid track interface {slot/port | vlan vlan-id} [decrement priority]`

Mode Interface Config

7.9.0.10.1 no ip vrrp track interface

Use this command to remove the interface or range of interfaces from the tracked list or to restore the priority decrement to its default.

Format `no ip vrrp vrid track interface slot/port [decrement]`

Mode Interface Config

7.9.0.11 ip vrrp track ip route

Use this command to track the route reachability on an interface or range of interfaces. When the tracked route is deleted, the priority of the VRRP router will be decremented by the value specified in the `priority` argument. When the tracked route is added, the priority will be incremented by the same.

A VRRP configured interface can track more than one route. When a tracked route goes down, then the priority of the router will be decreased by 10 (the default priority decrement) for each downed route. By default no routes are tracked. If you specify just the route to be tracked, without giving the optional priority, then the default priority will be set. The default priority decrement is 10. The default priority decrement is changed using the `priority` argument.

Default priority: 10

Format `ip vrrp vrid track ip route ip-address/prefix-length [decrement priority]`

Mode Interface Config

7.9.0.11.1 no ip vrrp track ip route

Use this command to remove the route from the tracked list or to restore the priority decrement to its default. When removing a tracked IP route from the tracked list, the priority should be incremented by the decrement value if the route is not reachable.

Format `no ip vrrp vrid track interface slot/port [decrement]`

Mode Interface Config

7.9.0.12 show ip vrrp interface stats

This command displays the statistical information about each virtual router configured on the switch.

Format `show ip vrrp interface stats {slot/port |vlan vlan-id} vrid`

Modes
- Privileged EXEC
- User EXEC

Parameter	Definition
Uptime	The time that the virtual router has been up, in days, hours, minutes and seconds.
Protocol	The protocol configured on the interface.
State Transitioned to Master	The total number of times virtual router state has changed to MASTER.
Advertisement Received	The total number of VRRP advertisements received by this virtual router.
Advertisement Interval Errors	The total number of VRRP advertisements received for which advertisement interval is different than the configured value for this virtual router.
Authentication Failure	The total number of VRRP packets received that don't pass the authentication check.
IP TTL errors	The total number of VRRP packets received by the virtual router with IP TTL (time to live) not equal to 255.
Zero Priority Packets Received	The total number of VRRP packets received by virtual router with a priority of '0'.
Zero Priority Packets Sent	The total number of VRRP packets sent by the virtual router with a priority of '0'.
Invalid Type Packets Received	The total number of VRRP packets received by the virtual router with invalid 'type' field.
Address List Errors	The total number of VRRP packets received for which address list does not match the locally configured list for the virtual router.
Invalid Authentication Type	The total number of VRRP packets received with unknown authentication type.
Authentication Type Mismatch	The total number of VRRP advertisements received for which 'auth type' not equal to locally configured one for this virtual router.
Packet Length Errors	The total number of VRRP packets received with packet length less than length of VRRP header.

7.9.0.13 show ip vrrp

This command displays whether VRRP functionality is enabled or disabled on the switch. It also displays some global parameters which are required for monitoring. This command takes no options.

Format `show ip vrrp`

Modes
- Privileged EXEC
- User EXEC

Parameter	Definition
VRRP Admin Mode	The administrative mode for VRRP functionality on the switch.
Router Checksum Errors	The total number of VRRP packets received with an invalid VRRP checksum value.
Router Version Errors	The total number of VRRP packets received with Unknown or unsupported version number.
Router VRID Errors	The total number of VRRP packets received with invalid VRID for this virtual router.

7.9.0.14 show ip vrrp interface

This command displays all configuration information and VRRP router statistics of a virtual router configured on a specific interface. Use the output of the command to verify the track interface and track IP route configurations.

Format `show ip vrrp interface {`*`slot/port |vlan vlan-id} vrid`*

Modes
- Privileged EXEC
- User EXEC

Parameter	Definition
IP Address	The configured IP address for the Virtual router.
VMAC address	The VMAC address of the specified router.
Authentication type	The authentication type for the specific virtual router.
Priority	The priority value for the specific virtual router, taking into account any priority decrements for tracked interfaces or routes.
Configured Priority	The priority configured through the `ip vrrp vrid priority 1-254` command.
Advertisement interval	The advertisement interval in seconds for the specific virtual router.
Pre-Empt Mode	The preemption mode configured on the specified virtual router.
Administrative Mode	The status (Enable or Disable) of the specific router.
Accept Mode	When enabled, the VRRP Master can accept ping packets sent to one of the virtual router's IP addresses.
State	The state (Master/backup) of the virtual router.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip vrrp interface <slot/port> vrid

Primary IP Address.............................. 1.1.1.5
VMAC Address.................................... 00:00:5e:00:01:01
Authentication Type............................. None
Priority........................................ 80
  Configured priority........................... 100
Advertisement Interval (secs).................. 1
```

```
Pre-empt Mode................................... Enable
Administrative Mode............................. Enable
Accept Mode..................................... Enable
State........................................... Initialized
Track Interface          State          DecrementPriority
---------------         ------          -----------------

<0/1>                   down                10
TrackRoute  (pfx/len)      State         DecrementPriority
------------------------   ------          -----------------
10.10.10.1/255.255.255.0    down               10
```

7.9.0.15 show ip vrrp interface brief

This command displays information about each virtual router configured on the switch. This command takes no options. It displays information about each virtual router.

Format `show ip vrrp interface brief`

Modes
- Privileged EXEC
- User EXEC

Parameter	Definition
Interface	*slot/port*
VRID	The router ID of the virtual router.
IP Address	The virtual router IP address.
Mode	Indicates whether the virtual router is enabled or disabled.
State	The state (Master/backup) of the virtual router.

7.10 VRRPv3 Commands

VRRPv3 provides address redundancy for both IPv4 and IPv6 router addresses. VRRPv3 support in EFOS is similar to VRRP support. The following table provides a summary of the differences.

VRRPv2	VRRPv3
Supports redundancy to IPv4 addresses	Supports redundancy to IPv4 and IPv6 addresses
Supports authentication	Does not support authentication
No concept of link-local address in IPv4 address space	For IPv6 addresses, VRRP IP contains the link-local IPv6 address too.
The interval time used for sending VRRP Advertisement packets is in seconds.	The interval time is in the order of centiseconds.
VRRP MAC address format is 00-00-5E-00-01-{VRID}	VRRP MAC address format for IPv6 VR IP is 00-00-5E-00-02-{VRID}
SNMP MIB RFC according to 2787. The counters are 32-bit ones.	SNMP MIB RFC as per RFC 6527. The counters are 64-bit ones.

NOTE: Note the following:

- To enable VRRP on the device, use the `ip vrrp` command. See Section 7.9.0.1, ip vrrp (Global Config)). This command enables VRRP (v2 or v3, whichever version is the configured version) and makes it operational.
- A command is available to configure debugging for VRRP packets. For information, see Section 4.14.0.41, debug ip vrrp.

7.10.0.1 fhrp version vrrp v3

To enable Virtual Router Redundancy Protocol version 3 (VRRPv3) configuration on a device, use the `fhrp version vrrp v3` command in global configuration mode.

When VRRPv3 is in use, VRRP version 2 (VRRPv2) is unavailable. If you invoke `no fhrp version vrrp v3`, VRRPv3 is disabled and VRRPv2 is enabled. Also, operational data is reset, and the VRRPv2 configuration is applied. The same guidelines apply when VRRPv2 is in use and the `no ip vrrp` command is issued.

Defaults Disabled

Format `fhrp version vrrp v3`

Mode Global Config

7.10.0.1.1 no fhrp version vrrp v3

Use this command to disable the VRRPv3 and enable VRRPv2 on the device.

Format `no fhrp version vrrp v3`

Mode Global Config

7.10.0.2 snmp-server enable traps vrrp

Use this command to enable the two SNMP traps defined in the VRRPv2 and VRRPv3 MIB standards.

Defaults Enabled

Format `snmp-server enable traps vrrp`

Mode Global Config

7.10.0.2.1 no snmp-server enable traps vrrp

Use this command to disable the two SNMP traps defined in the VRRPv2 and VRRPv3 MIB standards.

Defaults Enabled
Format `no snmp-server enable traps vrrp`
Mode Global Config

7.10.0.3 vrrp

Use the `vrrp` command to create a VRRPv3 group and enter VRRPv3 group configuration mode.

Format `vrrp` *`group-id`* `address-family {ipv4 | ipv6}`
Mode Interface Config

Parameter	Description
group-id	Virtual router group number. The range is from 1 to 255.
address-family	Specifies the address-family for this VRRP group.
ipv4	(Optional) Specifies IPv4 address.
ipv6	(Optional) Specifies IPv6 address.

7.10.0.3.1 no vrrp

Use the `no vrrp` command to remove the specified VRRPv3 group. Before you can use this command, you must disable Virtual Router using the `shutdown` command in the appropriate VRRP Config mode.

Format `no vrrp` *`group-id`* `address-family {ipv4 | ipv6}`
Mode Interface Config

7.10.0.4 preempt

Use this command to configure the device to take over as master virtual router for a VRRP group if it has higher priority than the current master virtual route

Default Enabled with default delay value of 0
Format `preempt [delay minimum` *`centiseconds`*`]`
Mode VRRPv3 Config

Parameter	Description
delay minimum	Number of seconds that the device will delay before issuing an advertisement claiming master ownership. The default delay is 0 centiseconds. The valid range is 0–3600 centiseconds.

7.10.0.4.1 no preempt

Use this command to prevent device from taking over as master virtual router for a VRRP group if it has higher priority than the current master virtual route.

Format `no preempt [delay minimum` *`centiseconds`*`]`
Mode VRRPv3 Config

7.10.0.5 accept-mode

Use this command to control whether a virtual router in master state will accept packets addressed to the address owner's virtual IP address as its own if it is not the virtual IP address owner.

Default Disabled
Format `accept-mode`
Mode VRRPv3 Config

7.10.0.5.1 no accept-mode

Use this command to reset the accept mode to the default value.

Format `no accept-mode`
Mode VRRPv3 Config

7.10.0.6 priority

Use this command to set the priority level of the device within a VRRPv3 group. The priority level controls which device becomes the master virtual router.

Default 100
Format `priority` *`level`*
Mode VRRPv3 Config

Parameter	Description
level	Priority of the device within the VRRP group. The range is from 1 to 254. The default is 100.

7.10.0.6.1 no priority

Use this command to reset the priority level of the device to the default value.

Format `priority`
Mode VRRPv3 Config

7.10.0.7 timers advertise

Use this command to configure the interval between successive advertisements by the master virtual router in a VRRP group. To restore the default value, use the no form of this command.

The advertisements being sent by the master virtual router communicate the advertisement interval, state, and priority of the current master virtual router. The VRRP `timers advertise` command configures the time between successive advertisement packets and the time before other routers declare the master router to be down. VRRP backup routers learn timer values from the master router advertisements. The timers configured on the master router always override any other timer settings that are used for calculating the master down time interval on VRRP backup routers.

Default 100

Format `timers advertise` *`centiseconds`*

Mode VRRPv3 Config

Parameter	Description
centiseconds	Time interval between successive advertisements by the master virtual router. The unit of the interval is in centiseconds. The valid range is 1 to 4095 centiseconds.

7.10.0.7.1 no timers advertise

Use this command to reset the advertisement interval of the device to the default value.

Format `no timers advertise`

Mode VRRPv3 Config

7.10.0.8 shutdown (VRRP Group Configuration)

Use the `shutdown` command to disable the VRRP group configuration.

Format `shutdown`

Mode VRRPv3 Config

7.10.0.8.1 no shutdown

Enter the **no shutdown** command to update the virtual router state after completing configuration.

Format `no shutdown`

Mode VRRPv3 Config

7.10.0.9 address

Use this command to set the primary or secondary IP address of the device within a VRRPv3 group. To remove the secondary address, use the no form of this command.

If the primary or secondary option is not specified, the specified IP address is set as the primary. The Virtual IPv6 primary address should be a link-local address only. When a global IPv6 address is given as a primary address for the VRRP IP then the config fails with the following error message – “Error! Primary virtual IPv6 address should be a link-local address only.” Also the removing of the primary virtual IP (IPv4 or IPv6) is not allowed. The primary virtual IP of a virtual router can only be modified. The secondary virtual IP can be removed using the no form of the this command. Also, VRRPv3 for IPv6 requires that a primary virtual link-local IPv6 address is configured to allow the group to operate. After the primary link-local IPv6 address is established on the group, you can add the secondary global addresses.

Format `address ip-address [primary | secondary]`
Mode VRRPv3 Config

Parameter	Description
ip-address	IPv4 or IPv6 address, it can be specified in one of the following format: `ipv4-address`, `ipv6-link-local-address`, `ipv6-address>/<prefix-len`.
primary	(Optional) Set primary IP address of the VRRPv3 group.
secondary	(Optional) Set additional IP address of the VRRPv3 group.

7.10.0.9.1 no address

Use this command to remove the configured secondary IP or IPv6 address. The primary address can only be modified, not removed.

Format `no address ip-address secondary`
Mode VRRPv3 Config

7.10.0.10 track interface

Use this command to configure tracking of the interface for the device within a VRRPv3 group. Use the `bfdneighbor` option to track the reachability to the uplink next hop address. Once interface tracking is configured, the VRRPv3 feature receives notifications when the interface changes state. If BFD tracking is enabled with bfdneighbor config, then a BFD session is created with the BFD destination IP as that of the given BFD neighbor IP address, VRRPv3 receives notification when the BFD session state changes. The `decrement` option can be set to decrease the priority of the device within a VRRPv3 group by the specified value when the interface goes down, or the associated BFD session goes down. Similarly, the priority is increased by the same specified value when the interface comes up or the associated BFD session comes up. If the `decrement` value is not set, then the default decrement value used is 10. The overall state of a track interface object is considered as up only when both of the events (interface up event and BFD session up event) are received. The decrement or increment of priority is done based on the overall state of the track interface object.

Default Enabled
Format `track interface {slot/port | vlan vlan-id} [bfdneighbor IP-address][decrement number]`
Mode VRRPv3 Config

Parameter	Description
slot/port	The interface to track.
vlan-id	The VLAN to track.
bfdneighbor	(Optional) BFD neighbor tracking.
IP-address	(Optional) IPv4 or IPv6 address of BFD neighbor to be tracked for reachability using a BFD session.
decrement number	(Optional) Specify the VRRP priority decrement for the tracked object. The number is the amount by which priority is decremented. The range is 1–254.

7.10.0.10.1 no track interface

Use this command to disable tracking of the interface for the device within a VRRPv3 group.

Default Enabled

Format `track interface {slot/port | vlan vlan-id} [decrement number]`

Mode VRRPv3 Config

7.10.0.11 track ip route

Use this command to configure tracking of the IP route for the device within a Virtual Router Redundancy Protocol (VRRPv3) group. Once IP route tracking is configured, the VRRPv3 feature receives notifications when IP route changes state. The decrement option can be set to decrease the priority of the device within a VRRPv3 group by the specified value when the route becomes unavailable.

Default Disabled

Format `track ip route ip-address/prefix-len [decrement number]`

Mode VRRPv3 Config

Parameter	Description
ip-address/prefix-len	Prefix and prefix length of the route to be tracked.
decrement number	(Optional) Specify the VRRP priority decrement for the tracked route. The number is the amount by which priority is decremented. The range is 1–254.

7.10.0.11.1 no track ip route

Use this command to disable object tracking.

Format `no track ip route ip-address/prefix-len [decrement number]`

Mode VRRPv3 Config

7.10.0.12 clear vrrp statistics

Use this command to clear VRRP statistical information for given interface of the device within a VRRPv3 group and IP address family. If this command is issued without the optional arguments then the global statistics and all virtual routers (both IPv4 and IPv6) are reset.

If the optional arguments are specified, the statistics are reset for the virtual router corresponding to the given (IP address family, interface and VR-id) combination.

Format `clear vrrp statistics [{ipv4| ipv6} {slot/port | vlan vlan-id} vrid]`

Mode Privileged Exec

Parameter	Description
ipv4	(Optional) indicates the Virtual router group belongs to IPv4 address family.
ipv6	(Optional) indicates the Virtual router group belongs to IPv6 address family.

Parameter	Description
slot/port	(Optional) indicates the interface number to which the Virtual router belongs.
vlan-id	(Optional) indicates the VLAN number to which the Virtual router belongs.
vr-id	(Optional) Virtual router group number. The range is from 1 to 255.

7.10.0.13 show vrrp

This command displays information for all active VRRPv3 groups (no optional parameters), all active VRRPv3 groups configured in an IPv4 or IPv6 address family, or the active VRRPv3 groups configured in an IPv4 or IPv6 address family for the specified interface.

Format `show vrrp [{ipv4 | ipv6}] [{`*`slot/port`* `| vlan` *`vlan-id`*`} `*`vr-id`*`]`

Mode Privileged Exec

Parameter	Description
ipv4	(Optional) indicates the Virtual router group belongs to IPv4 address family.
ipv6	(Optional) indicates the Virtual router group belongs to IPv6 address family.
slot/port	(Optional) indicates the interface number to which the Virtual router belongs.
vlan-id	(Optional) indicates the VLAN number to which the Virtual router belongs.
vr-id	(Optional) Virtual router group number. The range is from 1 to 255.

Example: This example shows command output when no parameters are specified.

```
(Routing)#show vrrp

Admin Mode..................................... Enable


0/2 - VRID 1 - Address-Family IPv4

Virtual IP address............................. 1.1.1.9
Secondary IP Address(es)....................... 1.1.1.4
.............................................. 1.1.1.5
.............................................. 1.1.1.6
Virtual MAC Address............................ 00:00:5e:00:01:01
Priority....................................... 0
Configured Priority............................ 111
Advertisement Interval......................... 120 centisec
Pre-empt Mode.................................. Enable
Accept Mode.................................... Enable
Administrative Mode............................ Enable
State.......................................... Initialized
Master Router IP / Priority.................... 1.1.1.3 (local) / 100
Master Advertisement interval.................. 120 centisec
Master Down interval........................... 360 centisec

Track Interface State DecrementPriority  BFD-Neighbor
--------------- ----- ------------------ ------------
1/0/9           Down  222                23.10.8.6


Track Route(pfx/len)   Reachable  DecrementPriority
```

```
--------------------  ---------  ------------------
14.14.14.0/24         True       14


0/3 - VRID 2 - Address-Family IPv4

Virtual IP address.............................. 3.3.2.9
Secondary IP Address(es)........................ 3.3.2.4
................................................ 3.3.2.5
................................................ 3.3.2.6
Virtual MAC Address............................. 00:00:5e:00:01:06
Priority........................................ 0
Configured Priority............................. 130
Advertisement Interval.......................... 120 centisec
Pre-empt Mode................................... Enable
Accept Mode..................................... Enable
Administrative Mode............................. Enable
State........................................... Initialized
Master Router IP / Priority..................... 1.1.1.3 (local) / 100
Master Advertisement interval................... 120 centisec
Master Down interval............................ 360 centisec

Track Interface State DecrementPriority   BFD-Neighbor
--------------- ----- ------------------  ------------
0/7             Down  125                  55.16.27.8

Track Route(pfx/len)   Reachable  DecrementPriority
--------------------  ---------  ------------------
14.14.14.0/24         True       30


0/12 - VRID 3 - Address-Family IPv6

Virtual IP address.............................. 4001::2
Secondary IP Address(es)........................ 4001::5
................................................ 4001::6
................................................ 4001::7
Virtual MAC Address............................. 00:00:5e:00:01:06
Priority........................................ 0
Configured Priority............................. 130
Advertisement Interval.......................... 120 centisec
Pre-empt Mode................................... Enable
Accept Mode..................................... Enable
Administrative Mode............................. Enable
State........................................... Initialized
Master Router IP / Priority..................... 4001::3 (local) / 100
Master Advertisement interval................... 120 centisec
Master Down interval............................ 360 centisec

Track Interface State DecrementPriority   BFD-Neighbor
--------------- ----- ------------------  ------------
0/2             Down  250                  5001::3

Track Route(pfx/len)   Reachable  DecrementPriority
--------------------  ---------  ------------------
4004::3/32            True       20
```

Example: This example shows command output when the IPv4 parameter is specified.

```
(Routing)#show vrrp ipv4

Admin Mode..................................... Enable

0/2 - VRID 1 - Address-Family IPv4

Virtual IP address............................. 1.1.1.9
Secondary IP Address(es)....................... 1.1.1.4
.............................................. 1.1.1.5
.............................................. 1.1.1.6
Virtual MAC Address............................ 00:00:5e:00:01:01
Priority....................................... 0
Configured Priority............................ 111
Advertisement Interval......................... 120 centisec
Pre-empt Mode.................................. Enable
Accept Mode.................................... Enable
Administrative Mode............................ Enable
State.......................................... Initialized
Master Router IP / Priority.................... 1.1.1.3 (local) / 100
Master Advertisement interval.................. 120 centisec
Master Down interval........................... 360 centisec

Track Interface State DecrementPriority
--------------- ----- ------------------
0/9           Down  222

Track Route(pfx/len)   Reachable  DecrementPriority
--------------------  ---------  ------------------
14.14.14.0/24          True       14


0/3 - VRID 2 - Address-Family IPv4

Virtual IP address............................. 3.3.2.9
Secondary IP Address(es)....................... 3.3.2.4
.............................................. 3.3.2.5
.............................................. 3.3.2.6
Virtual MAC Address............................ 00:00:5e:00:01:06
Priority....................................... 0
Configured Priority............................ 130
Advertisement Interval......................... 120 centisec
Pre-empt Mode.................................. Enable
Accept Mode.................................... Enable
Administrative Mode............................ Enable
State.......................................... Initialized
Master Router IP / Priority.................... 1.1.1.3 (local) / 100
Master Advertisement interval.................. 120 centisecsec
Master Down interval........................... 360

Track Interface State DecrementPriority
--------------- ----- ------------------
0/7           Down  125

Track Route(pfx/len)   Reachable  DecrementPriority
--------------------  ---------  ------------------
14.14.14.0/24          True       30
```

Example: This example shows command output when the IPv6 parameter is specified.

```
(Routing)#show vrrp ipv6

Admin Mode..................................... Enable


0/2 - VRID 1 - Address-Family IPv6

Virtual IP address............................. 1001::8
Secondary IP Address(es)....................... 1001::5
.............................................. 1001::6
.............................................. 1001::7
Virtual MAC Address............................ 00:00:5e:00:01:01
Priority....................................... 0
Configured Priority............................ 100
Advertisement Interval......................... 100 centisec
Pre-empt Mode.................................. Enable
Accept Mode.................................... Enable
Administrative Mode............................ Enable
State.......................................... Initialized
Master Router IP / Priority.................... 1001::1 (local) / 100
Master Advertisement interval.................. 100 centisec
Master Down interval........................... 300 centisec

Track Interface State DecrementPriority
--------------- ----- ------------------
0/9           Down  222

Track Route(pfx/len)   Reachable  DecrementPriority
---------------------  ---------  ------------------
2001::2/32             True       14


0/12 - VRID 3 - Address-Family IPv6

Virtual IP address............................. 4001::2
Secondary IP Address(es)....................... 4001::5
.............................................. 4001::6
.............................................. 4001::7
Virtual MAC Address............................ 00:00:5e:00:01:06
Priority....................................... 130
Configured Priority............................ 130
Advertisement Interval......................... 120 centisec
Pre-empt Mode.................................. Enable
Accept Mode.................................... Enable
Administrative Mode............................ Enable
State.......................................... Master
Master Router IP / Priority.................... 4001::3 (local) / 130
Master Advertisement interval.................. 120 centisec
Master Down interval........................... 360 centisec

Track Interface State DecrementPriority
--------------- ----- ------------------
0/24          Down  320

Track Route(pfx/len)   Reachable  DecrementPriority
---------------------  ---------  ------------------
7003::4/32             True       50
```

Example:

```
(Routing)#show vrrp ipv4 0/3 1

Virtual IP address.............................. 1.1.1.9
Secondary IP Address(es)........................ 1.1.1.4
................................................ 1.1.1.5
................................................ 1.1.1.6
Virtual MAC Address............................. 00:00:5e:00:01:01
Priority........................................ 0
Configured Priority............................. 111
Advertisement Interval.......................... 222 centisec
Pre-empt Mode................................... Enable
Accept Mode..................................... Enable
Administrative Mode............................. Enable
State........................................... Initialized
Master Router IP / Priority..................... 1.1.1.3 (local) / 100
Master Advertisement interval................... 1000 centisec
Master Down interval............................ 3000 centisec


Track Interface State Decrement-Priority
--------------- ----- ------------------
0/9             Down  222

Track Route(pfx/len)   Reachable  Decrement-Priority
---------------------  ---------  ------------------
14.14.14.0/24          True       14
```

7.10.0.14 show vrrp brief

This command displays brief information for all active VRRPv3 groups.

Format `show vrrp brief`

Mode Privileged Exec

Field	Description
Interface	Interface on which VRRP is configured.
VR	ID of the virtual router.
A-F	IP address family type (IPv4 or Ipv6) this Virtual Router belongs to.
Pri	Priority range of the virtual router.
AdvIntvl	Advertisement interval configured for this virtual router.
Pre	Preemption state of the virtual router.
Acc	Accept Mode of the virtual router.
State	VRRP group state. The state can be one of the following: Init, Backup, Master
VR IP address	Virtual IP address for a VRRP group.

Example:

```
(Routing)#show vrrp brief

Interface   VRID A-F  Pri AdvIntvl Pre Acc State  VR IP Address
```

```
----------- ---- ---- --- -------- --- --- ------ -------------
0/1         1    IPv4 100 200s      Y   Y  Init   192.0.1.10
0/3         2    IPv4 200 200s      Y   Y  Init   124.0.3.17
0/1         7    IPv6 100 200s      Y   Y  Backup 5002::1
0/5         2    IPV6 20  200s      Y   Y  Master 2001::2
```

7.10.0.15 show vrrp statistics

This command displays statistical information for a given VRRPv3 group or displays the global statistics. If this command is issued without the optional arguments then the global statistics are displayed.

If the optional arguments are specified, the statistics are displayed for the virtual router corresponding to the given (IP address family, interface and VR-id) combination.

Format `show vrrp statistics [{ipv4| ipv6} {slot/port | vlan vlan-id} vrid]`

Mode Privileged Exec

Parameter	Description
ipv4	(Optional) indicates the Virtual router group belongs to IPv4 address family.
ipv6	(Optional) indicates the Virtual router group belongs to IPv6 address family.
slot/port	(Optional) indicates the interface number to which the Virtual router belongs.
vlan-id	(Optional) indicates the VLAN number to which the Virtual router belongs.
vr-id	(Optional) Virtual router group number. The range is from 1 to 255.

Example:

```
(Routing)#show vrrp statistics ipv6 0/1 2

Master Transitions.............................. 2
New Master Reason............................... Priority
Advertisements Received......................... 64
Advertisements Sent............................. 12
Advertisement Interval Errors................... 0
IP TTL Errors................................... 1
Last Protocol Error Reason...................... Version Error
Zero Priority Packets Received.................. 0
Zero Priority Packets Sent...................... 1
Invalid Type Packets Received................... 0
Address List Errors............................. 2
Packet Length Errors............................ 4
Row Discontinuity Time.......................... 0 days 0 hrs 0 mins 0 secs
Refresh Rate (in milliseconds).................. 0


(Routing)#show vrrp statistics

Router Checksum Errors.......................... 2
Router Version Errors........................... 3
Router VRID Errors.............................. 4
Global Statistics Discontinuity Time............ 0 days 0 hrs 0 mins 0 secs
```

7.11 DHCP and BOOTP Relay Commands

This section describes the commands you use to configure BootP/DHCP Relay on the switch. A DHCP relay agent operates at Layer 3 and forwards DHCP requests and replies between clients and servers when they are not on the same physical subnet.

7.11.0.1 bootpdhcprelay cidoptmode

This command enables the circuit ID option mode for BootP/DHCP Relay on the system.

Default disabled

Format `bootpdhcprelay cidoptmode`

Mode
- Global Config
- Virtual Router Config

7.11.0.1.1 no bootpdhcprelay cidoptmode

This command disables the circuit ID option mode for BootP/DHCP Relay on the system.

Format `no bootpdhcprelay cidoptmode`

Mode
- Global Config
- Virtual Router Config

7.11.0.2 bootpdhcprelay maxhopcount

This command configures the maximum allowable relay agent hops for BootP/DHCP Relay on the system. The `hops` parameter has a range of 1 to 16.

Default 4

Format `bootpdhcprelay maxhopcount` *`1-16`*

Mode
- Global Config
- Virtual Router Config

7.11.0.2.1 no bootpdhcprelay maxhopcount

This command configures the default maximum allowable relay agent hops for BootP/DHCP Relay on the system.

Format `no bootpdhcprelay maxhopcount`

Mode
- Global Config
- Virtual Router Config

7.11.0.3 bootpdhcprelay minwaittime

This command configures the minimum wait time in seconds for BootP/DHCP Relay on the system. When the BOOTP relay agent receives a BOOTREQUEST message, it MAY use the seconds-since-client-began-booting field of the request as a factor in deciding whether to relay the request or not. The parameter has a range of 0 to 100 seconds.

Default 0

Format `bootpdhcprelay minwaittime` *`0-100`*

Mode
- Global Config
- Virtual Router Config

7.11.0.3.1 no bootpdhcprelay minwaittime

This command configures the default minimum wait time in seconds for BootP/DHCP Relay on the system.

Format `no bootpdhcprelay minwaittime`

Mode
- Global Config
- Virtual Router Config

7.11.0.4 show bootpdhcprelay

This command displays the BootP/DHCP Relay information for the virtual router. If no router is specified, information for the default router is displayed.

Format `show bootpdhcprelay [vrf` *`vrf-name`*`]`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Maximum Hop Count	The maximum allowable relay agent hops.
Minimum Wait Time (Seconds)	The minimum wait time.
Admin Mode	Indicates whether relaying of requests is enabled or disabled.
Circuit Id Option Mode	The DHCP circuit Id option which may be enabled or disabled.

7.11.0.5 show ip bootpdhcprelay

This command displays BootP/DHCP Relay information.

Format `show ip bootpdhcprelay`

Modes User EXEC

Parameter	Definition
Maximum Hop Count	The maximum allowable relay agent hops.
Minimum Wait Time (Seconds)	The minimum wait time.
Admin Mode	Indicates whether relaying of requests is enabled or disabled.
Circuit Id Option Mode	The DHCP circuit Id option, which may be enabled or disabled.

Example: The following shows an example of the command.

```
(Routing) >show ip bootpdhcprelay

Maximum Hop Count.............................. 4
Minimum Wait Time(Seconds)..................... 0
Admin Mode..................................... Disable
```

```
Circuit Id Option Mode..................... Enable
```

7.12 IP Helper Commands

This section describes the commands to configure and monitor the IP Helper agent. IP Helper relays DHCP and other broadcast UDP packets from a local client to one or more servers which are not on the same network at the client.

The IP Helper feature provides a mechanism that allows a router to forward certain configured UDP broadcast packets to a particular IP address. This allows various applications to reach servers on non-local subnets, even if the application was designed to assume a server is always on a local subnet and uses broadcast packets (with either the limited broadcast address 255.255.255.255, or a network directed broadcast address) to reach the server.

The network administrator can configure relay entries both globally and on routing interfaces. Each relay entry maps an ingress interface and destination UDP port number to a single IPv4 address (the helper address). The network administrator may configure multiple relay entries for the same interface and UDP port, in which case the relay agent relays matching packets to each server address. Interface configuration takes priority over global configuration. That is, if a packet's destination UDP port matches any entry on the ingress interface, the packet is handled according to the interface configuration. If the packet does not match any entry on the ingress interface, the packet is handled according to the global IP helper configuration.

The network administrator can configure discard relay entries, which direct the system to discard matching packets. Discard entries are used to discard packets received on a specific interface when those packets would otherwise be relayed according to a global relay entry. Discard relay entries may be configured on interfaces, but are not configured globally.

In addition to configuring the server addresses, the network administrator also configures which UDP ports are forwarded. Certain UDP port numbers can be specified by name in the UI as a convenience, but the network administrator can configure a relay entry with any UDP port number. The network administrator may configure relay entries that do not specify a destination UDP port. The relay agent relays assumes these entries match packets with the UDP destination ports listed in Table 11. This is the list of default ports.

Table 11: Default Ports—UDP Port Numbers Implied by Wildcard

Protocol	UDP Port Number
IEN-116 Name Service	42
DNS	53
NetBIOS Name Server	137
NetBIOS Datagram Server	138
TACACS Server	49
Time Service	37
DHCP	67
Trivial File Transfer Protocol (TFTP)	69

The system limits the number of relay entries to four times the maximum number of routing interfaces. The network administrator can allocate the relay entries as he likes. There is no limit to the number of relay entries on an individual interface, and no limit to the number of servers for a given {interface, UDP port} pair.

The relay agent relays DHCP packets in both directions. It relays broadcast packets from the client to one or more DHCP servers, and relays to the client packets that the DHCP server unicasts back to the relay agent. For other protocols, the relay agent only relays broadcast packets from the client to the server. Packets from the server back to the client are assumed to be unicast directly to the client. Because there is no relay in the return direction for protocols other than DHCP, the relay agent retains the source IP address from the original client packet. The relay agent uses a local IP address as the source IP address of relayed DHCP client packets.

When a switch receives a broadcast UDP packet on a routing interface, the relay agent checks if the interface is configured to relay the destination UDP port. If so, the relay agent unicasts the packet to the configured server IP addresses. Otherwise, the relay agent checks if there is a global configuration for the destination UDP port. If so, the relay agent unicasts the packet to the configured server IP addresses. Otherwise the packet is not relayed. Note that if the packet matches a discard relay entry on the ingress interface, then the packet is not forwarded, regardless of the global configuration.

The relay agent only relays packets that meet the following conditions:

- The destination MAC address must be the all-ones broadcast address (FF:FF:FF:FF:FF:FF)
- The destination IP address must be the limited broadcast address (255.255.255.255) or a directed broadcast address for the receive interface.
- The IP time-to-live (TTL) must be greater than 1.
- The protocol field in the IP header must be UDP (17).
- The destination UDP port must match a configured relay entry.

7.12.0.1 clear ip helper statistics

Use this command to reset to zero the statistics displayed in the `show ip helper statistics` command for the specified virtual router. If no router is specified, the command is executed for the default router.

Format `clear ip helper statistics [vrf` *`vrf-name`*`]`

Mode Privileged EXEC

Example: The following shows an example of the command.

```
(Routing) #clear ip helper statistics
```

7.12.0.2 ip helper-address (Global Config)

Use this command to configure the relay of certain UDP broadcast packets received on any interface. This command can be invoked multiple times, either to specify multiple server addresses for a given UDP port number or to specify multiple UDP port numbers handled by a specific server.

Default `No helper addresses are configured.`

Format `ip helper-address server-address [dest-udp-port | dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp |tacacs | tftp | time]`

Mode Global Config

Parameter	Description
server-address	The IPv4 unicast or directed broadcast address to which relayed UDP broadcast packets are sent. The server address cannot be an IP address configured on any interface of the local router.
dest-udp-port	A destination UDP port number from 0 to 65535.

Parameter	Description
port-name	The destination UDP port may be optionally specified by its name. Whether a port is specified by its number or its name has no effect on behavior. The names recognized are as follows: ■ dhcp (port 67) ■ domain (port 53) ■ isakmp (port 500) ■ mobile-ip (port 434) ■ nameserver (port 42) ■ netbios-dgm (port 138) ■ netbios-ns (port 137) ■ ntp (port 123) ■ pim-auto-rp (port 496) ■ tacacs (port 49) ■ tftp (port 69) ■ time (port 37) Other ports must be specified by number.

Example: To relay DHCP packets received on any interface to two DHCP servers, 10.1.1.1 and 10.1.2.1, use the following commands:

```
(Routing) #config
(Routing) (config)#ip helper-address 10.1.1.1 dhcp
(Routing) (config)#ip helper-address 10.1.2.1 dhcp
```

Example: To relay UDP packets received on any interface for all default ports to the server at 20.1.1.1, use the following commands:

```
(Routing) #config
(Routing) (config)#ip helper-address 20.1.1.1
```

7.12.0.2.1 no ip helper-address (Global Config)

Use the `no` form of the command to delete an IP helper entry. The command `no ip helper-address` with no arguments clears all global IP helper addresses.

Format `no ip helper-address [server-address [dest-udp-port | dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp |tacacs | tftp | time]`

Mode Global Config

7.12.0.3 ip helper-address (Interface Config)

Use this command to configure the relay of certain UDP broadcast packets received on a specific interface or range of interfaces. This command can be invoked multiple times on a routing interface, either to specify multiple server addresses for a given port number or to specify multiple port numbers handled by a specific server.

Default `No helper addresses are configured.`

Format `ip helper-address {server-address | discard} [dest-udp-port | dhcp | domain | isakmp | mobile ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | tacacs | tftp | time]`

Mode Interface Config

Parameter	Description
server-address	The IPv4 unicast or directed broadcast address to which relayed UDP broadcast packets are sent. The server address cannot be in a subnet on the interface where the relay entry is configured, and cannot be an IP address configured on any interface of the local router.
discard	Matching packets should be discarded rather than relayed, even if a global ip helper-address configuration matches the packet.
dest-udp-port	A destination UDP port number from 0 to 65535.
port-name	The destination UDP port may be optionally specified by its name. Whether a port is specified by its number or its name has no effect on behavior. The names recognized are as follows: ■ dhcp (port 67) ■ domain (port 53) ■ isakmp (port 500) ■ mobile-ip (port 434) ■ nameserver (port 42) ■ netbios-dgm (port 138) ■ netbios-ns (port 137) ■ ntp (port 123) ■ pim-auto-rp (port 496) ■ tacacs (port 49) ■ tftp (port 69) ■ time (port 37) Other ports must be specified by number.

Example: To relay DHCP packets received on interface 0/2 to two DHCP servers, 192.168.10.1 and 192.168.20.1, use the following commands:

```
(Routing)#config
(Routing)(config)#interface 0/2
(Routing)(interface 0/2)#ip helper-address 192.168.10.1 dhcp
(Routing)(interface 0/2)#ip helper-address 192.168.20.1 dhcp
```

Example: To relay both DHCP and DNS packets to 192.168.30.1, use the following commands:

```
(Routing)#config
(Routing)(config)#interface 0/2
(Routing)(interface 0/2)#ip helper-address 192.168.30.1 dhcp
(Routing)(interface 0/2)#ip helper-address 192.168.30.1 dns
```

Example: This command takes precedence over an ip helper-address command given in global configuration mode. With the following configuration, the relay agent relays DHCP packets received on any interface other than 0/2 and 0/17 to 192.168.40.1, relays DHCP and DNS packets received on 0/2 to 192.168.40.2, relays SNMP traps (port 162) received on interface 0/17 to 192.168.23.1, and drops DHCP packets received on 0/17:

```
(Routing)#config
(Routing)(config)#ip helper-address 192.168.40.1 dhcp
(Routing)(config)#interface 0/2
(Routing)(interface 0/2)#ip helper-address 192.168.40.2 dhcp
(Routing)(interface 0/2)#ip helper-address 192.168.40.2 domain
(Routing)(interface 0/2)#exit
(Routing)(config)#interface 0/17
(Routing)(interface 0/17)#ip helper-address 192.168.23.1 162
(Routing)(interface 0/17)#ip helper-address discard dhcp
```

7.12.0.3.1 no ip helper-address (Interface Config)

Use this command to delete a relay entry on an interface. The `no` command with no arguments clears all helper addresses on the interface.

Format `no ip helper-address [server-address | discard ][dest-udp-port | dhcp | domain | isakmp | mobile ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | tacacs | tftp | time]`

Mode Interface Config

7.12.0.4 ip helper enable

Use this command to enable relay of UDP packets. This command can be used to temporarily disable IP helper without deleting all IP helper addresses. This command replaces the `bootpdhcprelay enable` command, but affects not only relay of DHCP packets, but also relay of any other protocols for which an IP helper address has been configured.

Default `disabled`

Format `ip helper enable`

Mode
- Global Config
- Virtual Router Config

Example: The following shows an example of the command.

```
(Routing)(config)#ip helper enable
```

7.12.0.4.1 no ip helper enable

Use the no form of this command to disable relay of all UDP packets.

Format `no ip helper enable`

Mode Global Config

7.12.0.5 show ip helper-address

Use this command to display the IP helper address configuration on the specified virtual router. If no virtual router is specified, the configuration of the default router is displayed.The argument `slot/port` corresponds to a physical routing interface or VLAN routing interface. The keyword **vlan** is used to specify the VLAN ID of the routing VLAN directly instead of a *slot/port* format.

Format `show ip helper-address [vrf` *`vrf-name`*`] [{`*`slot/port`*`|`*`vlan 1-4093`*`}]`

Mode
- Privileged EXEC
- Virtual Router Config

Parameter	Description
interface	The relay configuration is applied to packets that arrive on this interface. This field is set to `any` for global IP helper entries.
UDP Port	The relay configuration is applied to packets whose destination UDP port is this port. Entries whose UDP port is identified as any are applied to packets with the destination UDP ports listed in Table 4.

Parameter	Description
Discard	If Yes, packets arriving on the given interface with the given destination UDP port are discarded rather than relayed. Discard entries are used to override global IP helper address entries which otherwise might apply to a packet.
Hit Count	The number of times the IP helper entry has been used to relay or discard a packet.
Server Address	The IPv4 address of the server to which packets are relayed.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip helper-address

IP helper is enabled

   Interface   UDP Port     Discard   Hit Count   Server Address
--------------  -----------  --------  ----------  ---------------
       0/1              dhcp        No          10    10.100.1.254
                                                      10.100.2.254
       0/17              any       Yes           2
          any           dhcp        No           0    10.200.1.254
```

7.12.0.6 show ip helper statistics

Use this command to display the number of DHCP and other UDP packets processed and relayed by the UDP relay agent on the specified virtual router. If no virtual router is specified, the configuration of the default router is displayed.

Format `show ip helper statistics [vrf` *`vrf-name`*`]`

Mode Privileged EXEC

Parameter	Description
DHCP client messages received	The number of valid messages received from a DHCP client. The count is only incremented if IP helper is enabled globally, the ingress routing interface is up, and the packet passes a number of validity checks, such as having a TTL>1 and having valid source and destination IP addresses.
DHCP client messages relayed	The number of DHCP client messages relayed to a server. If a message is relayed to multiple servers, the count is incremented once for each server.
DHCP server messages received	The number of DHCP responses received from the DHCP server. This count only includes messages that the DHCP server unicasts to the relay agent for relay to the client.
DHCP server messages relayed	The number of DHCP server messages relayed to a client.
UDP clients messages received	The number of valid UDP packets received. This count includes DHCP messages and all other protocols relayed. Conditions are similar to those for the first statistic in this table.
UDP clients messages relayed	The number of UDP packets relayed. This count includes DHCP messages relayed as well as all other protocols. The count is incremented for each server to which a packet is sent.
DHCP message hop count exceeded max	The number of DHCP client messages received whose hop count is larger than the maximum allowed. The maximum hop count is a configurable value listed in show bootpdhcprelay. A log message is written for each such failure. The DHCP relay agent does not relay these packets.
DHCP message with secs field below min	The number of DHCP client messages received whose secs field is less than the minimum value. The minimum secs value is a configurable value and is displayed in show bootpdhcprelay. A log message is written for each such failure. The DHCP relay agent does not relay these packets.

Parameter	Description
DHCP message with giaddr set to local address	The number of DHCP client messages received whose gateway address, giaddr, is already set to an IP address configured on one of the relay agent's own IP addresses. In this case, another device is attempting to spoof the relay agent's address. The relay agent does not relay such packets. A log message gives details for each occurrence.
Packets with expired TTL	The number of packets received with TTL of 0 or 1 that might otherwise have been relayed.
Packets that matched a discard entry	The number of packets ignored by the relay agent because they match a discard relay entry.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip helper statistics

DHCP client messages received..................... 8
DHCP client messages relayed...................... 2
DHCP server messages received..................... 2
DHCP server messages relayed...................... 2
UDP client messages received...................... 8
UDP client messages relayed....................... 2
DHCP message hop count exceeded max............... 0
DHCP message with secs field below min............ 0
DHCP message with giaddr set to local address.. 0
Packets with expired TTL.......................... 0
Packets that matched a discard entry.............. 0
```

7.13 Open Shortest Path First Commands

This section describes the commands you use to view and configure Open Shortest Path First (OSPF), which is a link-state routing protocol that you use to route traffic within a network.

7.13.1 General OSPF Commands

7.13.1.1 router ospf

Use this command to enable OSPF routing in a specified virtual router and to enter Router OSPF mode. If no virtual router is specified, OSPF routing is enabled in the default router.

Format `router ospf [vrf vrf-name]`
Mode Global Config

Parameter	Description
vrf vrf-name	The virtual router on which to enable OSPF routing.

7.13.1.2 enable (OSPF)

This command resets the default administrative mode of OSPF in the router (active).

Default enabled
Format `enable`
Mode Router OSPF Config

7.13.1.2.1 no enable (OSPF)

This command sets the administrative mode of OSPF in the router to inactive.

Format `no enable`
Mode Router OSPF Config

7.13.1.3 network area (OSPF)

Use this command to enable OSPFv2 on an interface and set its area ID if the IP address of an interface is covered by this network command.

Default disabled
Format `network ip-address wildcard-mask area area-id`
Mode Router OSPF Config

7.13.1.3.1 no network area (OSPF)

Use this command to disable the OSPFv2 on a interface if the IP address of an interface was earlier covered by this network command.

Format `no network ip-address wildcard-mask area area-id`
Mode Router OSPF Config

7.13.1.4 1583compatibility

This command enables OSPF 1583 compatibility.

NOTE: 1583 compatibility mode is enabled by default. If all OSPF routers in the routing domain are capable of operating according to RFC 2328, OSPF 1583 compatibility mode should be disabled.

Default enabled

Format `1583compatibility`

Mode Router OSPF Config

7.13.1.4.1 no 1583compatibility

This command disables OSPF 1583 compatibility.

Format `no 1583compatibility`

Mode Router OSPF Config

7.13.1.5 area default-cost (OSPF)

This command configures the default cost for the stub area. You must specify the area ID and an integer value between 1-16777215.

Format `area` ***`areaid`*** `default-cost` ***`1-16777215`***

Mode Router OSPF Config

7.13.1.6 area nssa (OSPF)

This command configures the specified areaid to function as an NSSA.

Format `area` ***`areaid`*** `nssa`

Mode Router OSPF Config

7.13.1.6.1 no area nssa

This command disables nssa from the specified area id.

Format `no area` ***`areaid`*** `nssa`

Mode Router OSPF Config

7.13.1.7 area nssa default-info-originate (OSPF)

This command configures the metric value and type for the default route advertised into the NSSA. The optional metric parameter specifies the metric of the default route and is to be in a range of 1-16777214. If no metric is specified, the default value is ****. The metric type can be comparable (nssa-external 1) or non-comparable (nssa-external 2).

Format `area` ***`areaid`*** `nssa default-info-originate [`***`metric`***`] [{comparable | non-comparable}]`

Mode Router OSPF Config

7.13.1.7.1 no area nssa default-info-originate (OSPF)

This command disables the default route advertised into the NSSA.

Format `no area areaid nssa default-info-originate [metric] [{comparable | non-comparable}]`

Mode Router OSPF Config

7.13.1.8 area nssa no-redistribute (OSPF)

This command configures the NSSA Area Border router (ABR) so that learned external routes will not be redistributed to the NSSA.

Format `area areaid nssa no-redistribute`

Mode Router OSPF Config

7.13.1.8.1 no area nssa no-redistribute (OSPF)

This command disables the NSSA ABR so that learned external routes are redistributed to the NSSA.

Format `no area areaid nssa no-redistribute`

Mode Router OSPF Config

7.13.1.9 area nssa no-summary (OSPF)

This command configures the NSSA so that summary LSAs are not advertised into the NSSA.

Format `area areaid nssa no-summary`

Mode Router OSPF Config

7.13.1.9.1 no area nssa no-summary (OSPF)

This command disables nssa from the summary LSAs.

Format `no area areaid nssa no-summary`

Mode Router OSPF Config

7.13.1.10 area nssa translator-role (OSPF)

This command configures the translator role of the NSSA. A value of `always` causes the router to assume the role of the translator the instant it becomes a border router and a value of `candidate` causes the router to participate in the translator election process when it attains border router status.

Format `area areaid nssa translator-role {always | candidate}`

Mode Router OSPF Config

7.13.1.10.1 no area nssa translator-role (OSPF)

This command disables the nssa translator role from the specified area id.

Format `no area areaid nssa translator-role {always | candidate}`

Mode Router OSPF Config

7.13.1.11 area nssa translator-stab-intv (OSPF)

This command configures the translator `stabilityinterval` of the NSSA. The `stabilityinterval` is the period of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router.

Format `area areaid nssa translator-stab-intv stabilityinterval`

Mode Router OSPF Config

7.13.1.11.1 no area nssa translator-stab-intv (OSPF)

This command disables the nssa translator's `stabilityinterval` from the specified area id.

Format `no area areaid nssa translator-stab-intv stabilityinterval`

Mode Router OSPF Config

7.13.1.12 area range (OSPF)

Use the area range command in Router Configuration mode to configure a summary prefix that an area border router advertises for a specific area.

Default No area ranges are configured by default. No cost is configured by default.

Format `area areaid range prefix netmask {summarylink | nssaexternallink} [advertise | not-advertise] [cost cost]`

Mode OSPFv2 Router Configuration

Parameter	Description
area-id	The area identifier for the area whose networks are to be summarized.
prefix netmask	The summary prefix to be advertised when the ABR computes a route to one or more networks within this prefix in this area.
summarylink	When this keyword is given, the area range is used when summarizing prefixes advertised in type 3 summary LSAs.
nssaexternallink	When this keyword is given, the area range is used when translating type 7 LSAs to type 5 LSAs.
advertise	[Optional] When this keyword is given, the summary prefix is advertised when the area range is active. This is the default.
not-advertise	[Optional] When this keyword is given, neither the summary prefix nor the contained prefixes are advertised when the area range is active. When the not-advertise option is given, any static cost previously configured is removed from the system configuration.
cost	[Optional] If an optional cost is given, OSPF sets the metric field in the summary LSA to the configured value rather than setting the metric to the largest cost among the networks covered by the area range. A static cost may only be configured if the area range is configured to advertise the summary. The range is 0 to 16,777,215. If the cost is set to 16,777,215 for type 3 summarization, a type 3 summary LSA is not advertised, but contained networks are suppressed. This behavior is equivalent to specifying the **not-advertise** option. If the range is configured for type 7 to type 5 translation, a type 5 LSA is sent if the metric is set to 16,777,215; however, other routers will not compute a route from a type 5 LSA with this metric.

7.13.1.12.1 no area range

The **no** form of this command deletes a specified area range or reverts an option to its default.

Format `no area areaid range prefix netmask {summarylink | nssaexternallink} [advertise | not-advertise] [cost]`

Mode OSPFv2 Router Configuration

Example: The following shows an example of the command.

```
!! Create area range
(Routing) (Config-router)#area 1 range 10.0.0.0 255.0.0.0 summarylink
!! Delete area range
(Routing) (Config-router)#no area 1 range 10.0.0.0 255.0.0.0 summarylink
```

The **no** form may be used to revert the [**advertise | not-advertise**] option to its default without deleting the area range. Deleting and recreating the area range would cause OSPF to temporarily advertise the prefixes contained within the range. Note that using either the **advertise** or **not-advertise** keyword reverts the configuration to the default. For example:

```
!! Create area range. Suppress summary.
(Routing) (Config-router)#area 1 range 10.0.0.0 255.0.0.0 summarylink not-advertise
!! Advertise summary.
(Routing) (Config-router)#no area 1 range 10.0.0.0 255.0.0.0 summarylink not-advertise
```

The **no** form may be use to remove a static area range cost, so that OSPF sets the cost to the largest cost among the contained routes.

```
!! Create area range with static cost.
(Routing) (Config-router)#area 1 range 10.0.0.0 255.0.0.0 summarylink cost 1000
!! Remove static cost.
(Routing) (Config-router)#no area 1 range 10.0.0.0 255.0.0.0 summarylink cost
```

7.13.1.13 area stub (OSPF)

This command creates a stub area for the specified area ID. A stub area is characterized by the fact that AS External LSAs are not propagated into the area. Removing AS External LSAs and Summary LSAs can significantly reduce the link state database of routers within the stub area.

Format `area areaid stub`

Mode Router OSPF Config

7.13.1.13.1 no area stub

This command deletes a stub area for the specified area ID.

Format `no area areaid stub`

Mode Router OSPF Config

7.13.1.14 area stub no-summary (OSPF)

This command configures the Summary LSA mode for the stub area identified by `areaid`. Use this command to prevent LSA Summaries from being sent.

Default disabled

Format `area areaid stub no-summary`

Mode Router OSPF Config

7.13.1.14.1 no area stub no-summary

This command configures the default Summary LSA mode for the stub area identified by `areaid`.

Format `no area areaid stub no-summary`

Mode Router OSPF Config

7.13.1.15 area virtual-link (OSPF)

This command creates the OSPF virtual interface for the specified `areaid` and `neighbor`. The `neighbor` parameter is the Router ID of the neighbor.

Format `area areaid virtual-link neighbor`

Mode Router OSPF Config

7.13.1.15.1 no area virtual-link

This command deletes the OSPF virtual interface from the given interface, identified by `areaid` and `neighbor`. The `neighbor` parameter is the Router ID of the neighbor.

Format `no area areaid virtual-link neighbor`

Mode Router OSPF Config

7.13.1.16 area virtual-link authentication

This command configures the authentication type and key for the OSPF virtual interface identified by `areaid` and `neighbor`. The `neighbor` parameter is the Router ID of the neighbor. The value for `type` is either none, simple, or encrypt. The `key` is composed of standard displayable, non-control keystrokes from a Standard 101/102-key keyboard. The authentication key must be 8 bytes or less if the authentication type is simple. If the type is encrypt, the key may be up to 16 bytes. Unauthenticated interfaces do not need an authentication key. If the type is encrypt, a key id in the range of 0 and 255 must be specified.The default value for authentication type is none. Neither the default password key nor the default key id are configured.

Default none

Format `area areaid virtual-link neighbor authentication {none | {simple key} | {encrypt key keyid}}`

Mode Router OSPF Config

7.13.1.16.1 no area virtual-link authentication

This command configures the default authentication type for the OSPF virtual interface identified by `areaid` and `neighbor`. The `neighbor` parameter is the Router ID of the neighbor.

Format `no area areaid virtual-link neighbor authentication`

Mode Router OSPF Config

7.13.1.17 area virtual-link dead-interval (OSPF)

This command configures the dead interval for the OSPF virtual interface on the virtual interface identified by `areaid` and `neighbor`. The `neighbor` parameter is the Router ID of the neighbor. The range for seconds is 1 to 65535.

Default 40

Format `area areaid virtual-link neighbor dead-interval seconds`

Mode Router OSPF Config

7.13.1.17.1 no area virtual-link dead-interval

This command configures the default dead interval for the OSPF virtual interface on the virtual interface identified by `areaid` and `neighbor`. The `neighbor` parameter is the Router ID of the neighbor.

Format `no area` ***areaid*** `virtual-link` ***neighbor*** `dead-interval`

Mode Router OSPF Config

7.13.1.18 area virtual-link hello-interval (OSPF)

This command configures the hello interval for the OSPF virtual interface on the virtual interface identified by `areaid` and `neighbor`. The `neighbor` parameter is the Router ID of the neighbor. The range for `seconds` is 1 to 65535.

Default 10

Format `area` ***areaid*** `virtual-link` ***neighbor*** `hello-interval` ***1-65535***

Mode Router OSPF Config

7.13.1.18.1 no area virtual-link hello-interval

This command configures the default hello interval for the OSPF virtual interface on the virtual interface identified by `areaid` and `neighbor`. The `neighbor` parameter is the Router ID of the neighbor.

Format `no area` ***areaid*** `virtual-link` ***neighbor*** `hello-interval`

Mode Router OSPF Config

7.13.1.19 area virtual-link retransmit-interval (OSPF)

This command configures the retransmit interval for the OSPF virtual interface on the virtual interface identified by `areaid` and `neighbor`. The `neighbor` parameter is the Router ID of the neighbor. The range for seconds is 0 to 3600.

Default 5

Format `area` ***areaid*** `virtual-link` ***neighbor*** `retransmit-interval` ***seconds***

Mode Router OSPF Config

7.13.1.19.1 no area virtual-link retransmit-interval

This command configures the default retransmit interval for the OSPF virtual interface on the virtual interface identified by `areaid` and `neighbor`. The `neighbor` parameter is the Router ID of the neighbor.

Format `no area` ***areaid*** `virtual-link` ***neighbor*** `retransmit-interval`

Mode Router OSPF Config

7.13.1.20 area virtual-link transmit-delay (OSPF)

This command configures the transmit delay for the OSPF virtual interface on the virtual interface identified by `areaid` and `neighbor`. The `neighbor` parameter is the Router ID of the neighbor. The range for seconds is 0 to 3600 (1 hour).

Default 1

Format `area` ***areaid*** `virtual-link` ***neighbor*** `transmit-delay` ***seconds***

Mode Router OSPF Config

7.13.1.20.1 no area virtual-link transmit-delay

This command resets the default transmit delay for the OSPF virtual interface to the default value.

Format `no area` *`areaid`* `virtual-link` *`neighbor`* `transmit-delay`

Mode Router OSPF Config

7.13.1.21 auto-cost (OSPF)

By default, OSPF computes the link cost of each interface from the interface bandwidth. Faster links have lower metrics, making them more attractive in route selection. The configuration parameters in the `auto-cost reference bandwidth` and `bandwidth` commands give you control over the default link cost. You can configure for OSPF an interface bandwidth that is independent of the actual link speed. A second configuration parameter allows you to control the ratio of interface bandwidth to link cost. The link cost is computed as the ratio of a reference bandwidth to the interface bandwidth (ref_bw / interface bandwidth), where interface bandwidth is defined by the `bandwidth` command. Because the default reference bandwidth is 100 Mbps, OSPF uses the same default link cost for all interfaces whose bandwidth is 100 Mbps or greater. Use the `auto-cost` command to change the reference bandwidth, specifying the reference bandwidth in megabits per second (Mbps). The reference bandwidth range is 1-4294967 Mbps.

Default 100 Mbps

Format `auto-cost reference-bandwidth` *`1-4294967`*

Mode Router OSPF Config

7.13.1.21.1 no auto-cost reference-bandwidth (OSPF)

Use this command to set the reference bandwidth to the default value.

Format `no auto-cost reference-bandwidth`

Mode Router OSPF Config

7.13.1.22 capability opaque

Use this command to enable Opaque Capability on the Router. The information contained in Opaque LSAs may be used directly by OSPF or indirectly by an application wishing to distribute information throughout the OSPF domain. EFOS supports the storing and flooding of Opaque LSAs of different scopes. The default value of `enabled` means that OSPF will forward opaque LSAs by default. If you want to upgrade from a previous release, where the default was disabled, opaque LSA forwarding will be enabled. If you want to disable opaque LSA forwarding, then you should enter the command no capability opaque in OSPF router configuration mode after the software upgrade.

Default enabled

Format `capability opaque`

Mode Router Config

7.13.1.22.1 no capability opaque

Use this command to disable opaque capability on the router.

Format `no capability opaque`

Mode Router Config

7.13.1.23 clear ip ospf

Use this command to disable and reenable OSPF for the specified virtual router. If no virtual router is specified, the default router is disabled and re-enabled.

Format `clear ip ospf [vrf vrf-name]`
Mode Privileged EXEC

7.13.1.24 clear ip ospf configuration

Use this command to reset the OSPF configuration to factory defaults for the specified virtual router. If no virtual router is specified, the default router is cleared.

Format `clear ip ospf configuration [vrf vrf-name]`
Mode Privileged EXEC

7.13.1.25 clear ip ospf counters

Use this command to reset global and interface statistics for the specified virtual router. If no virtual router is specified, the global and interface statistics are reset for the default router.

Format `clear ip ospf counters [vrf vrf-name]`
Mode Privileged EXEC

7.13.1.26 clear ip ospf neighbor

Use this command to drop the adjacency with all OSPF neighbors for the specified virtual router. On each neighbor's interface, send a one-way hello. Adjacencies may then be re-established. If no router is specified, adjacency with all OSPF neighbors is dropped for the default router. To drop all adjacencies with a specific router ID, specify the neighbor's Router ID using the optional parameter `[neighbor-id]`.

Format `clear ip ospf neighbor [neighbor-id] [vrf vrf-name]`
Mode Privileged EXEC

7.13.1.27 clear ip ospf neighbor interface

To drop adjacency with all neighbors on a specific interface, use the optional parameter [`slot/port`]. To drop adjacency with a specific router ID on a specific interface, use the optional parameter [`neighbor-id`].

Format `clear ip ospf neighbor interface [slot/port] [neighbor-id]`
Mode Privileged EXEC

7.13.1.28 clear ip ospf redistribution

Use this command to flush all self-originated external LSAs for the specified virtual router. If no router is specified, the command is executed for the default router. Reapply the redistribution configuration and reoriginate prefixes as necessary.

Format `clear ip ospf redistribution [vrf vrf-name]`

Mode Privileged EXEC

7.13.1.29 default-information originate (OSPF)

This command is used to control the advertisement of default routes.

Default
- metric—unspecified
- type—2

Format `default-information originate [always] [metric 0-16777214] [metric-type {1 | 2}]`

Mode Router OSPF Config

7.13.1.29.1 no default-information originate (OSPF)

This command is used to control the advertisement of default routes.

Format `no default-information originate [metric] [metric-type]`

Mode Router OSPF Config

7.13.1.30 default-metric (OSPF)

This command is used to set a default for the metric of distributed routes.

Format `default-metric 1-16777214`

Mode Router OSPF Config

7.13.1.30.1 no default-metric (OSPF)

This command is used to set a default for the metric of distributed routes.

Format `no default-metric`

Mode Router OSPF Config

7.13.1.31 distance ospf (OSPF)

This command sets the route preference value of OSPF in the router. Lower route preference values are preferred when determining the best route. The type of OSPF route can be *intra, inter*, or *external*. All the external type routes are given the same preference value. The range of *preference* value is 1 to 255.

Default 110

Format `distance ospf {intra-area 1-255 | inter-area 1-255 | external 1-255}`

Mode Router OSPF Config

7.13.1.31.1 no distance ospf

This command sets the default route preference value of OSPF routes in the router. The type of OSPF can be intra, inter, or external. All the external type routes are given the same preference value.

Format `no distance ospf {intra-area | inter-area | external}`

Mode Router OSPF Config

7.13.1.32 distribute-list out (OSPF)

Use this command to specify the access list to filter routes received from the source protocol.

Format `distribute-list 1-199 out {bgp | static | connected}`
Mode Router OSPF Config

7.13.1.32.1 no distribute-list out

Use this command to specify the access list to filter routes received from the source protocol.

Format `no distribute-list 1-199 out {bgp | static | connected}`
Mode Router OSPF Config

7.13.1.33 exit-overflow-interval (OSPF)

This command configures the exit overflow interval for OSPF. It describes the number of seconds after entering overflow state that a router will wait before attempting to leave the overflow state. This allows the router to again originate non-default AS-external-LSAs. When set to 0, the router will not leave overflow state until restarted. The range for seconds is 0 to 2147483647 seconds.

Default 0
Format `exit-overflow-interval seconds`
Mode Router OSPF Config

7.13.1.33.1 no exit-overflow-interval

This command configures the default exit overflow interval for OSPF.

Format `no exit-overflow-interval`
Mode Router OSPF Config

7.13.1.34 external-lsdb-limit (OSPF)

This command configures the external LSDB limit for OSPF. If the value is -1, then there is no limit. When the number of non-default AS-external-LSAs in a router's link-state database reaches the external LSDB limit, the router enters overflow state. The router never holds more than the external LSDB limit non-default AS-external-LSAs in it database. The external LSDB limit MUST be set identically in all routers attached to the OSPF backbone and/or any regular OSPF area. The range for limit is -1 to 2147483647.

Default -1
Format `external-lsdb-limit limit`
Mode Router OSPF Config

7.13.1.34.1 no external-lsdb-limit

This command configures the default external LSDB limit for OSPF.

Format `no external-lsdb-limit`
Mode Router OSPF Config

7.13.1.35 log-adjacency-changes

To enable logging of OSPFv2 neighbor state changes, use the log-adjacency-changes command in router configuration mode. State changes are logged with INFORMATIONAL severity.

Default Adjacency state changes are logged, but without the detail option.
Format `log-adjacency-changes [detail]`
Mode OSPFv2 Router Configuration

Parameter	Description
detail	(Optional) When this keyword is specified, all adjacency state changes are logged. Otherwise, OSPF only logs transitions to FULL state and when a backwards transition occurs.

7.13.1.35.1 no log-adjacency-changes

Use the no form of the command to disable state change logging.

Format `no log-adjacency-changes [detail]`
Mode OSPFv2 Router Configuration

7.13.1.36 prefix-suppression (Router OSPF Config)

This command suppresses the advertisement of all the IPv4 prefixes except for prefixes that are associated with secondary IPv4 addresses, loopbacks, and passive interfaces from the OSPFv2 router advertisements.

To suppress a loopback or passive interface, use the Section 7.13.2.9, ip ospf prefix-suppression command in interface configuration mode. Prefixes associated with secondary IPv4 addresses can never be suppressed.

Default Prefix suppression is disabled.
Format `prefix-suppression`
Mode Router OSPF Config

7.13.1.36.1 no prefix-suppression

This command disables prefix-suppression. No prefixes are suppressed from getting advertised.

Format `no prefix-suppression`
Mode Router OSPF Config

7.13.1.37 prefix-suppression (Router OSPFv3 Config)

This command suppresses the advertisement of all the IPv6 prefixes except for prefixes that are associated with secondary IPv6 addresses, loopbacks, and passive interfaces from the OSPFv3 router advertisements.

To suppress a loopback or passive interface, use the `ipv ospf prefix-suppression` command in interface configuration mode. Prefixes associated with secondary IPv6 addresses can never be suppressed.

Default Prefix suppression is disabled.

Format `prefix-suppression`
Mode Router OSPFv3 Config

7.13.1.37.1 no prefix-suppression

This command disables prefix-suppression. No prefixes are suppressed from getting advertised.

Format `no prefix-suppression`
Mode Router OSPFv3 Config

7.13.1.38 router-id (OSPF)

This command sets a 4-digit dotted-decimal number uniquely identifying the router ospf id. The `ipaddress` is a configured value.

Format `router-id` *`ipaddress`*
Mode Router OSPF Config

7.13.1.39 redistribute (OSPF)

This command configures OSPF protocol to allow redistribution of routes from the specified source protocol/routers.

Default
- metric—unspecified
- type—2
- tag—0

Format `redistribute {bgp | static | connected} [metric` *`0-16777214`*`] [metric-type {1 | 2}] [tag` *`0-4294967295`*`] [subnets]`
Mode Router OSPF Config

7.13.1.39.1 no redistribute

This command configures OSPF protocol to prohibit redistribution of routes from the specified source protocol/routers.

Format `no redistribute {bgp | static | connected} [metric] [metric-type] [tag] [subnets]`
Mode Router OSPF Config

7.13.1.40 maximum-paths (OSPF)

This command sets the number of paths that OSPF can report for a given destination where `maxpaths` is platform dependent.

Default 4
Format `maximum-paths` *`maxpaths`*
Mode Router OSPF Config

7.13.1.40.1 no maximum-paths

This command resets the number of paths that OSPF can report for a given destination back to its default value.

Format `no maximum-paths`
Mode Router OSPF Config

7.13.1.41 passive-interface default (OSPF)

Use this command to enable global passive mode by default for all interfaces. It overrides any interface level passive mode. OSPF will not form adjacencies over a passive interface.

Default disabled

Format `passive-interface default`

Mode Router OSPF Config

7.13.1.41.1 no passive-interface default

Use this command to disable the global passive mode by default for all interfaces. Any interface previously configured to be passive reverts to non-passive mode.

Format `no passive-interface default`

Mode Router OSPF Config

7.13.1.42 passive-interface (OSPF)

Use this command to set the interface as passive. It overrides the global passive mode that is currently effective on the interface.

Default disabled

Format `passive-interface {`*`slot/port`* `| vlan` *`vlan-id`*`}`

Mode Router OSPF Config

7.13.1.42.1 no passive-interface

Use this command to set the interface as non-passive. It overrides the global passive mode that is currently effective on the interface.

Format `no passive-interface {`*`slot/port`* `| vlan` *`vlan-id`*`}`

Mode Router OSPF Config

7.13.1.43 timers pacing flood

To adjust the rate at which OSPFv2 sends LS Update packets, use the timers pacing flood command in router OSPFv2 global configuration mode. OSPF distributes routing information in Link State Advertisements (LSAs), which are bundled into Link State Update (LS Update) packets. To reduce the likelihood of sending a neighbor more packets than it can buffer, OSPF rate limits the transmission of LS Update packets. By default, OSPF sends up to 30 updates per second on each interface (1/the pacing interval). Use this command to adjust this packet rate.

Default `33 milliseconds`

Format `timers pacing flood milliseconds`

Mode OSPFv2 Router Configuration

Parameter	Description
milliseconds	The average time between transmission of LS Update packets. The range is from 5 ms to 100 ms. The default is 33 ms.

7.13.1.43.1 no timers pacing flood

To revert LSA transmit pacing to the default rate, use the no timers pacing flood command.

Format `no timers pacing flood`
Mode OSPFv2 Router Configuration

7.13.1.44 timers pacing lsa-group

To adjust how OSPF groups LSAs for periodic refresh, use the timers pacing lsa-group command in OSPFv2 Router Configuration mode. OSPF refreshes self-originated LSAs approximately once every 30 minutes. When OSPF refreshes LSAs, it considers all self-originated LSAs whose age is from 1800 to 1800 plus the pacing group size. Grouping LSAs for refresh allows OSPF to combine refreshed LSAs into a minimal number of LS Update packets. Minimizing the number of Update packets makes LSA distribution more efficient.

When OSPF originates a new or changed LSA, it selects a random refresh delay for the LSA. When the refresh delay expires, OSPF refreshes the LSA. By selecting a random refresh delay, OSPF avoids refreshing a large number of LSAs at one time, even if a large number of LSAs are originated at one time.

Default `60 seconds`
Format `timers pacing lsa-group` *`10-1800`*
Mode OSPFv2 Router Configuration

Parameter	Description
seconds	Width of the window in which LSAs are refreshed. The range for the pacing group window is from 10 to 1800 seconds.

7.13.1.45 timers spf

Use this command to configure the SPF delay time and hold time. The valid range for both parameters is 0-65535 seconds.

Default
- delay-time—5
- hold-time—10

Format `timers spf` *`delay-time hold-time`*
Mode Router OSPF Config

7.13.1.46 trapflags (OSPF)

Use this command to enable individual OSPF traps, enable a group of trap flags at a time, or enable all the trap flags at a time. The different groups of trapflags, and each group's specific trapflags to enable or disable, are listed in Table 12.

Table 12: Trapflags Groups

Group	Flags
errors	■ authentication-failure ■ bad-packet ■ config-error ■ virt-authentication-failure ■ virt-bad-packet ■ virt-config-error
lsa	■ lsa-maxage ■ lsa-originate
overflow	■ lsdb-overflow ■ lsdb-approaching-overflow
retransmit	■ packets ■ virt-packets
state-change	■ if-state-change ■ neighbor-state-change ■ virtif-state-change ■ virtneighbor-state-change

- To enable the individual flag, enter the `group name` followed by that particular flag.
- To enable all the flags in that group, give the group name followed by `all`.
- To enable all the flags, give the command as `trapflags all`.

Default disabled

Format
```
trapflags {
all | errors {all | authentication-failure | bad-packet | config-error | virt-
authentication-failure | virt-bad-packet | virt-config-error} |
lsa {all | lsa-maxage | lsa-originate} |
overflow {all | lsdb-overflow | lsdb-approaching-overflow} |
retransmit {all | packets | virt-packets} |
state-change {all | if-state-change | neighbor-state-change | virtif-state-change |
virtneighbor-state-change}
}
```

Mode Router OSPF Config

7.13.1.46.1 no trapflags

Use this command to revert to the default reference bandwidth.

- To disable the individual flag, enter the `group name` followed by that particular flag.
- To disable all the flags in that group, give the group name followed by `all`.
- To disable all the flags, give the command as `trapflags all`.

Format

```
no trapflags {
all |
errors {all | authentication-failure | bad-packet | config-error | virt-
authentication-failure | virt-bad-packet | virt-config-error} |
lsa {all | lsa-maxage | lsa-originate} |
overflow {all | lsdb-overflow | lsdb-approaching-overflow} |
retransmit {all | packets | virt-packets} |
state-change {all | if-state-change | neighbor-state-change | virtif-state-
change | virtneighbor-state-change}
}
```

Mode Router OSPF Config

7.13.2 OSPF Interface Commands

7.13.2.1 ip ospf area

Use this command to enable OSPFv2 and set the area ID of an interface or range of interfaces. The `area-id` is an IP address formatted as a 4-digit dotted-decimal number or a decimal value in the range of 0-4294967295. This command supersedes the effects of the `network area` command. It can also be used to configure the advertiseability of the secondary addresses on this interface into the OSPFv2 domain.

Default disabled

Format `ip ospf area` ***area-id*** `[secondaries none]`

Mode Interface Config

7.13.2.1.1 no ip ospf area

Use this command to disable OSPF on an interface.

Format `no ip ospf area [secondaries none]`

Mode Interface Config

7.13.2.2 bandwidth

By default, OSPF computes the link cost of an interface as the ratio of the reference bandwidth to the interface bandwidth. Reference bandwidth is specified with the `auto-cost` command. For the purpose of the OSPF link cost calculation, use the bandwidth command to specify the interface bandwidth. The bandwidth is specified in kilobits per second. If no bandwidth is configured, the bandwidth defaults to the actual interface bandwidth for port-based routing interfaces and to 10 Mbps for VLAN routing interfaces. This command does not affect the actual speed of an interface. You can use this command to configure a single interface or a range of interfaces.

Default actual interface bandwidth

Format `bandwidth` ***1-10000000***

Mode Interface Config

7.13.2.2.1 no bandwidth

Use this command to set the interface bandwidth to its default value.

Format `no bandwidth`

Mode Interface Config

7.13.2.3 ip ospf authentication

This command sets the OSPF Authentication Type and Key for the specified interface or range of interfaces. The value of `type` is either none, simple or encrypt. The `key` is composed of standard displayable, non-control keystrokes from a Standard 101/102-key keyboard. The authentication key must be 8 bytes or less if the authentication type is simple. If the type is encrypt, the key may be up to 16 bytes. If the type is encrypt a `keyid` in the range of 0 and 255 must be specified. Unauthenticated interfaces do not need an authentication key or authentication key ID. There is no default value for this command.

Format `ip ospf authentication {none | {simple` ***key***`} | {encrypt` ***key keyid***`}}`

Mode Interface Config

7.13.2.3.1 no ip ospf authentication

This command sets the default OSPF Authentication Type for the specified interface.

Format `no ip ospf authentication`

Mode Interface Config

7.13.2.4 ip ospf cost

This command configures the cost on an OSPF interface or range of interfaces. The `cost` parameter has a range of 1 to 65535.

Default 10

Format `ip ospf cost` *`1-65535`*

Mode Interface Config

7.13.2.4.1 no ip ospf cost

This command configures the default cost on an OSPF interface.

Format `no ip ospf cost`

Mode Interface Config

7.13.2.5 ip ospf database-filter all out

Use the **ip ospf database-filter all out** command in Interface Configuration mode to disable OSPFv2 LSA flooding on an interface.

Default Disabled

Format `ip ospf database-filter all out`

Mode Interface Configuration

7.13.2.5.1 no ip ospf database-filter all out

Use the **no ip ospf database-filter all out** command in Interface Configuration mode to enable OSPFv2 LSA flooding on an interface.

Default Disabled

Format `ip ospf database-filter all out`

Mode Interface Configuration

7.13.2.6 ip ospf dead-interval

This command sets the OSPF dead interval for the specified interface or range of interfaces. The value for `seconds` is a valid positive integer, which represents the length of time in seconds that a router's Hello packets have not been seen before its neighbor routers declare that the router is down. The value for the length of time must be the same for all routers attached to a common network. This value should be some multiple of the Hello Interval (i.e. 4). Valid values range in seconds from 1 to 65535.

7.13.2.6.1 no ip ospf dead-interval

This command sets the default OSPF dead interval for the specified interface.

Format `no ip ospf dead-interval`

Mode Interface Config

7.13.2.7 ip ospf hello-interval

This command sets the OSPF hello interval for the specified interface or range of interfaces. The value for seconds is a valid positive integer, which represents the length of time in seconds. The value for the length of time must be the same for all routers attached to a network. Valid values range from 1 to 65535.

Default 10

Format `ip ospf hello-interval` *seconds*

Mode Interface Config

7.13.2.7.1 no ip ospf hello-interval

This command sets the default OSPF hello interval for the specified interface.

Format `no ip ospf hello-interval`

Mode Interface Config

7.13.2.8 ip ospf network

Use this command to configure OSPF to treat an interface or range of interfaces as a point-to-point rather than broadcast interface. The `broadcast` option sets the OSPF network type to broadcast. The `point-to-point` option sets the OSPF network type to point-to-point. OSPF treats interfaces as broadcast interfaces by default. (Loopback interfaces have a special loopback network type, which cannot be changed.) When there are only two routers on the network, OSPF can operate more efficiently by treating the network as a point-to-point network. For point-to-point networks, OSPF does not elect a designated router or generate a network link state advertisement (LSA). Both endpoints of the link must be configured to operate in point-to-point mode.

Default broadcast

Format `ip ospf network {broadcast | point-to-point}`

Mode Interface Config

7.13.2.8.1 no ip ospf network

Use this command to return the OSPF network type to the default.

Format `no ip ospf network`

Mode Interface Config

7.13.2.9 ip ospf prefix-suppression

This command suppresses the advertisement of the IPv4 prefixes that are associated with an interface, except for those associated with secondary IPv4 addresses. This command takes precedence over the global configuration. If this configuration is not specified, the global prefix-suppression configuration applies.

prefix-suppression can be disabled at the interface level by using the disable option. The disable option is useful for excluding specific interfaces from performing prefix-suppression when the feature is enabled globally.

Note that the disable option disable is not equivalent to not configuring the interface specific prefix-suppression. If prefix-suppression is not configured at the interface level, the global prefix-suppression configuration is applicable for the IPv4 prefixes associated with the interface.

Default Prefix-suppression is not configured.

Format `ip ospf prefix-suppression [disable]`

Mode Interface Config

7.13.2.9.1 no ip ospf prefix-suppression

This command removes prefix-suppression configurations at the interface level. When `no ip ospf prefix-suppression` command is used, global prefix-suppression applies to the interface. Not configuring the command is not equal to disabling interface level prefix-suppression.

Format `no ip ospf prefix-suppression`

Mode Interface Config

7.13.2.10 ip ospf priority

This command sets the OSPF priority for the specified router interface or range of interfaces. The priority of the interface is a priority integer from 0 to 255. A value of 0 indicates that the router is not eligible to become the designated router on this network.

Default 1, which is the highest router priority

Format `ip ospf priority` *`0-255`*

Mode Interface Config

7.13.2.10.1 no ip ospf priority

This command sets the default OSPF priority for the specified router interface.

Format `no ip ospf priority`

Mode Interface Config

7.13.2.11 ip ospf retransmit-interval

This command sets the OSPF retransmit Interval for the specified interface or range of interfaces. The retransmit interval is specified in seconds. The value for `seconds` is the number of seconds between link-state advertisement retransmissions for adjacencies belonging to this router interface. This value is also used when retransmitting database description and link-state request packets. Valid values range from 0 to 3600 (1 hour).

Default 5

Format `ip ospf retransmit-interval` *`0-3600`*

Mode Interface Config

7.13.2.11.1 no ip ospf retransmit-interval

This command sets the default OSPF retransmit Interval for the specified interface.

Format `no ip ospf retransmit-interval`

Mode Interface Config

7.13.2.12 ip ospf transmit-delay

This command sets the OSPF Transit Delay for the specified interface or range of interfaces. The transmit delay is specified in seconds. In addition, it sets the estimated number of seconds it takes to transmit a link state update packet over this interface. Valid values for `seconds` range from 1 to 3600 (1 hour).

Default 1

Format `ip ospf transmit-delay` *`1-3600`*

Mode Interface Config

7.13.2.12.1 no ip ospf transmit-delay

This command sets the default OSPF Transit Delay for the specified interface.

Format `no ip ospf transmit-delay`

Mode Interface Config

7.13.2.13 ip ospf mtu-ignore

This command disables OSPF maximum transmission unit (MTU) mismatch detection on an interface or range of interfaces. OSPF Database Description packets specify the size of the largest IP packet that can be sent without fragmentation on the interface. When a router receives a Database Description packet, it examines the MTU advertised by the neighbor. By default, if the MTU is larger than the router can accept, the Database Description packet is rejected and the OSPF adjacency is not established.

Default enabled

Format `ip ospf mtu-ignore`

Mode Interface Config

7.13.2.13.1 no ip ospf mtu-ignore

This command enables the OSPF MTU mismatch detection.

Format `no ip ospf mtu-ignore`

Mode Interface Config

7.13.3 OSPF Graceful Restart Commands

The OSPF protocol can be configured to participate in the checkpointing service, so that these protocols can execute a “graceful restart” when the management unit fails. In a graceful restart, the hardware to continues forwarding IPv4 packets using OSPF routes while a backup switch takes over management unit responsibility

Graceful restart uses the concept of “helpful neighbors”. A fully adjacent router enters helper mode when it receives a link state announcement (LSA) from the restarting management unit indicating its intention of performing a graceful restart. In helper mode, a switch continues to advertise to the rest of the network that they have full adjacencies with the restarting router, thereby avoiding announcement of a topology change and the potential for flooding of LSAs and shortest-path-first (SPF) runs (which determine OSPF routes). Helpful neighbors continue to forward packets through the restarting router. The restarting router relearns the network topology from its helpful neighbors.

Graceful restart can be enabled for either planned or unplanned restarts, or both. A planned restart is initiated by the operator through the management command `initiate failover`. The operator may initiate a failover in order to take the management unit out of service (for example, to address a partial hardware failure), to correct faulty system behavior which cannot be corrected through less severe management actions, or other reasons. An unplanned restart is an unexpected failover caused by a fatal hardware failure of the management unit or a software hang or crash on the management unit.

7.13.3.1 nsf

Use this command to enable the OSPF graceful restart functionality on an interface. To disable graceful restart, use the no form of the command.

Default Disabled

Format `nsf [ietf] [planned-only]`

Modes OSPF Router Configuration

Parameter	Description
ietf	This keyword is accepted but not required.
planned-only	This optional keyword indicates that OSPF should only perform a graceful restart when the restart is planned (i.e., when the restart is a result of the initiate failover command).

7.13.3.1.1 no nsf

Use this command to disable graceful restart for all restarts.

7.13.3.2 nsf restart-interval

Use this command to configure the number of seconds that the restarting router asks its neighbors to wait before exiting helper mode. This is referred to as the grace period. The restarting router includes the grace period in its grace LSAs. For planned restarts (using the `initiate failover` command), the grace LSAs are sent prior to restarting the management unit, whereas for unplanned restarts, they are sent after reboot begins.

The grace period must be set long enough to allow the restarting router to reestablish all of its adjacencies and complete a full database exchange with each of those neighbors.

Default 120 seconds

Format `nsf [ietf] restart-interval` ***1-1800***

Modes OSPF Router Configuration

Parameter	Description
ietf	This keyword is accepted but not required.
seconds	The number of seconds that the restarting router asks its neighbors to wait before exiting helper mode. The range is from 1 to 1800 seconds.

7.13.3.2.1 no nsfrestart-interval

Use this command to revert the grace period to its default value.

Format `no [ietf] nsf restart-interval`
Modes OSPF Router Configuration

7.13.3.3 nsf helper

Use this command to enable helpful neighbor functionality for the OSPF protocol. You can enable this functionality for planned or unplanned restarts, or both.

Default OSPF may act as a helpful neighbor for both planned and unplanned restarts
Format `nsf helper [planned-only]`
Modes OSPF Router Configuration

Parameter	Description
planned-only	This optional keyword indicates that OSPF should only help a restarting router performing a planned restart.

7.13.3.3.1 no nsf helper

Use this command to disable helpful neighbor functionality for OSPF.

Format `no nsf helper`
Modes OSPF Router Configuration

7.13.3.4 nsf ietf helper disable

Use this command to disable helpful neighbor functionality for OSPF.

NOTE: The commands `no nsf helper` and `nsf ietf helper disable` are functionally equivalent. The command `nsf ietf helper disable` is supported solely for compatibility with other network software CLI.

Format `nsf ietf helper disable`
Modes OSPF Router Configuration

7.13.3.5 nsf helper strict-lsa-checking

The restarting router is unable to react to topology changes. In particular, the restarting router will not immediately update its forwarding table; therefore, a topology change may introduce forwarding loops or black holes that persist until the graceful restart completes. By exiting the graceful restart on a topology change, a router tries to eliminate the loops or black holes as quickly as possible by routing around the restarting router. A helpful neighbor considers a link down with the restarting router to be a topology change, regardless of the strict LSA checking configuration.

Use this command to require that an OSPF helpful neighbor exit helper mode whenever a topology change occurs.

Default Enabled.

Format `nsf [ietf] helper strict-lsa-checking`

Modes OSPF Router Configuration

Parameter	Description
ietf	This keyword is accepted but not required.

7.13.3.5.1 no nsf [ietf] helper strict-lsa-checking

Use this command to allow OSPF to continue as a helpful neighbor in spite of topology changes.

Default Enabled.

Format `nsf [ietf] helper strict-lsa-checking`

Modes OSPF Router Configuration

7.13.4 OSPFv2 Stub Router Commands

7.13.4.1 max-metric router-lsa

To configure OSPF to enter stub router mode, use this command in Router OSPF Global Configuration mode. When OSPF is in stub router mode, as defined by RFC 3137, OSPF sets the metric in the non-stub links in its router LSA to LsInfinity. Other routers therefore compute very long paths through the stub router, and prefer any alternate path. Doing so eliminates all transit traffic through the stub router, when alternate routes are available. Stub router mode is useful when adding or removing a router from a network or to avoid transient routes when a router reloads.

You can administratively force OSPF into stub router mode. OSPF remains in stub router mode until you take OSPF out of stub router mode. Alternatively, you can configure OSPF to start in stub router mode for a configurable period of time after the router boots up.

If you set the summary LSA metric to 16,777,215, other routers will skip the summary LSA when they compute routes.

If you have configured the router to enter stub router mode on startup (max-metric router-lsa on-startup), and then enter max-metric router lsa, there is no change. If OSPF is administratively in stub router mode (the max-metric router-lsa command has been given), and you configure OSPF to enter stub router mode on startup (max-metric router-lsa on-startup), OSPF exits stub router mode (assuming the startup period has expired) and the configuration is updated.

Default `OSPF is not in stub router mode by default`

Format `max-metric router-lsa [on-startup seconds] [summary-lsa {metric}]`

Mode OSPFv2 Router Configuration

Parameter	Description
on-startup	(Optional) OSPF starts in stub router mode after a reboot.
seconds	(Required if on-startup) The number of seconds that OSPF remains in stub router mode after a reboot. The range is 5 to 86,400 seconds. There is no default value.
summary-lsa	(Optional) Set the metric in type 3 and type 4 summary LSAs to LsInfinity (0xFFFFFF).
metric	(Optional) Metric to send in summary LSAs when in stub router mode. The range is 1 to 16,777,215. The default is 16,711,680 (0xFF0000).

7.13.4.1.1 no max-metric router-lsa

Use this command in OSPFv2 Router Configuration mode to disable stub router mode. The command clears either type of stub router mode (always or on-startup) and resets the **summary-lsa** option. If OSPF is configured to enter global configuration mode on startup, and during normal operation you want to immediately place OSPF in stub router mode, issue the command **no max-metric router-lsa on-startup**. The command **no max-metric router-lsa summary-lsa** causes OSPF to send summary LSAs with metrics computed using normal procedures defined in RFC 2328.

Format `no max-metric router-lsa [on-startup] [summary-lsa]`

Mode OSPFv2 Router Configuration

7.13.4.2 clear ip ospf stub-router

Use the clear ip ospf stub-router command in Privileged EXEC mode to force OSPF to exit stub router mode for the specified virtual router when it has automatically entered stub router mode because of a resource limitation. OSPF only exits stub router mode if it entered stub router mode because of a resource limitation or it if is in stub router mode at startup. If no virtual router is specified, the command is executed for the default router. This command has no effect if OSPF is configured to be in stub router mode permanently.

Format `clear ip ospf stub-router [vrf` *`vrf-name`*`]`

Mode Privileged EXEC

7.13.5 OSPF Show Commands

7.13.5.1 show ip ospf

This command displays OSPF global configuration information for the specified virtual router. If no router is specified, it displays information for the default router.

Format `show ip ospf [vrf vrf-name]`

Mode Privileged EXEC

NOTE: Some of the information below displays only if you enable OSPF and configure certain features.

Term	Definition
Router ID	A 32-bit integer in dotted decimal format identifying the router, about which information is displayed. This is a configured value.
OSPF Admin Mode	Shows whether the administrative mode of OSPF in the router is enabled or disabled. This is a configured value.
RFC 1583 Compatibility	Indicates whether 1583 compatibility is enabled or disabled. This is a configured value.
External LSDB Limit	The maximum number of nondefault AS-external-LSA (link state advertisement) entries that can be stored in the link-state database.
Exit Overflow Interval	The number of seconds that, after entering overflow state, a router will attempt to leave overflow state.
Spf Delay Time	The number of seconds between two subsequent changes of LSAs, during which time the routing table calculation is delayed.
Spf Hold Time	The number of seconds between two consecutive spf calculations.
Flood Pacing Interval	The average time, in milliseconds, between LS Update packet transmissions on an interface. This is the value configured with the Section 7.13.1.43, timers pacing flood command.
LSA Refresh Group Pacing Time	The size in seconds of the LSA refresh group window. This is the value configured with the Section 7.13.1.44, timers pacing lsa-group command.
Opaque Capability	Shows whether the router is capable of sending Opaque LSAs. This is a configured value.
Autocost Ref BW	Shows the value of auto-cost reference bandwidth configured on the router.
Default Passive Setting	Shows whether the interfaces are passive by default.
Maximum Paths	The maximum number of paths that OSPF can report for a given destination.
Default Metric	Default value for redistributed routes.
Stub Router Configuration	When OSPF runs out of resources to store the entire link state database, or any other state information, OSPF goes into stub router mode. As a stub router, OSPF reoriginates its own router LSAs, setting the cost of all nonstub interfaces to infinity. Use this field to set stub router configuration to one of **Always**, **Startup**, **None**.
Stub Router Startup Time	Configured value in seconds. This row is only listed if OSPF is configured to be a stub router at startup.
Summary LSA Metric Override	One of **Enabled (***met***)**, **Disabled**, where *met* is the metric to be sent in summary LSAs when in stub router mode.
BFD Enabled	Displays the BFD status.
Default Route Advertise	Indicates whether the default routes received from other source protocols are advertised or not.
Always	Shows whether default routes are always advertised.
Metric	The metric of the routes being redistributed. If the metric is not configured, this field is blank.
Metric Type	Shows whether the routes are External Type 1 or External Type 2.

Term	Definition
Number of Active Areas	The number of active OSPF areas. An “active” OSPF area is an area with at least one interface up.
ABR Status	Shows whether the router is an OSPF Area Border Router.
ASBR Status	Reflects whether the ASBR mode is enabled or disabled. Enable implies that the router is an autonomous system border router. The router automatically becomes an ASBR when it is configured to redistribute routes learned from other protocols. The possible values for the ASBR status is enabled (if the router is configured to redistribute routes learned by other protocols) or disabled (if the router is not configured for the same).
Stub Router Status	One of **Active**, **Inactive**.
Stub Router Reason	One of **Configured**, **Startup**, **Resource Limitation**. **NOTE:** The row is only listed if stub router is active.
Stub Router Startup Time Remaining	The remaining time, in seconds, until OSPF exits stub router mode. This row is only listed if OSPF is in startup stub router mode.
Stub Router Duration	The time elapsed since the router last entered the stub router mode. The row is only listed if stub router is active and the router entered stub mode because of a resource limitation. The duration is displayed in DD:HH:MM:SS format.
External LSDB Overflow	When the number of nondefault external LSAs exceeds the configured limit, External LSDB Limit, OSPF goes into LSDB overflow state. In this state, OSPF withdraws all of its self-originated nondefault external LSAs. After the Exit Overflow Interval, OSPF leaves the overflow state, if the number of external LSAs has been reduced.
External LSA Count	The number of external (LS type 5) link-state advertisements in the link-state database.
External LSA Checksum	The sum of the LS checksums of external link-state advertisements contained in the link-state database.
AS_OPAQUE LSA Count	Shows the number of AS Opaque LSAs in the link-state database.
AS_OPAQUE LSA Checksum	Shows the sum of the LS Checksums of AS Opaque LSAs contained in the link-state database.
New LSAs Originated	The number of new link-state advertisements that have been originated.
LSAs Received	The number of link-state advertisements received determined to be new instantiations.
LSA Count	The total number of link state advertisements currently in the link state database.
Maximum Number of LSAs	The maximum number of LSAs that OSPF can store.
LSA High Water Mark	The maximum size of the link state database since the system started.
AS Scope LSA Flood List Length	The number of LSAs currently in the global flood queue waiting to be flooded through the OSPF domain. LSAs with AS flooding scope, such as type 5 external LSAs and type 11 Opaque LSAs.
Retransmit List Entries	The total number of LSAs waiting to be acknowledged by all neighbors. An LSA may be pending acknowledgment from more than one neighbor.
Maximum Number of Retransmit Entries	The maximum number of LSAs that can be waiting for acknowledgment at any given time.
Retransmit Entries High Water Mark	The maximum number of LSAs on all neighbors’ retransmit lists at any given time.
NSF Support	Indicates whether nonstop forwarding (NSF) is enabled for the OSPF protocol for planned restarts, unplanned restarts or both (“Always”).
NSF Restart Interval	The user-configurable grace period during which a neighboring router will be in the helper state after receiving notice that the management unit is performing a graceful restart.
NSF Restart Status	The current graceful restart status of the router. ■ Not Restarting ■ Planned Restart ■ Unplanned Restart
NSF Restart Age	Number of seconds until the graceful restart grace period expires.

Term	Definition
NSF Restart Exit Reason	Indicates why the router last exited the last restart: ■ None—Graceful restart has not been attempted. ■ In Progress—Restart is in progress. ■ Completed—The previous graceful restart completed successfully. ■ Timed Out—The previous graceful restart timed out. ■ Topology Changed—The previous graceful restart terminated prematurely because of a topology change.
NSF Help Support	Indicates whether helpful neighbor functionality has been enabled for OSPF for planned restarts, unplanned restarts, or both (Always).
NSF help Strict LSA checking	Indicates whether strict LSA checking has been enabled. If enabled, then an OSPF helpful neighbor will exit helper mode whenever a topology change occurs. If disabled, an OSPF neighbor will continue as a helpful neighbor in spite of topology changes.
Prefix-suppression	Displays whether prefix-suppression is enabled or disabled.

Example: The following shows example CLI display output for the command.

```
(alpha3) #show ip ospf

Router ID..................................... 3.3.3.3
OSPF Admin Mode............................... Enable
RFC 1583 Compatibility........................ Enable
External LSDB Limit........................... No Limit
Exit Overflow Interval........................ 0
Spf Delay Time................................ 5
Spf Hold Time................................. 10
Flood Pacing Interval......................... 33 ms
LSA Refresh Group Pacing Time................. 60 sec
Opaque Capability............................. Enable
AutoCost Ref BW............................... 100 Mbps
Default Passive Setting....................... Disabled
Maximum Paths................................. 4
Default Metric................................ Not configured
Stub Router Configuration..................... <val>
Stub Router Startup Time...................... <val> seconds
Summary LSA Metric Override................... Enabled (<met>)

Default Route Advertise....................... Disabled
Always........................................ FALSE
Metric........................................ Not configured
Metric Type................................... External Type 2


Number of Active Areas........................ 1 (1 normal, 0 stub, 0 nssa)
ABR Status.................................... Disable
ASBR Status................................... Disable
Stub Router................................... FALSE
Stub Router Status............................ Inactive
Stub Router Reason............................ <reason>
Stub Router Startup Time Remaining............. <duration> seconds
Stub Router Duration.......................... <duration>
External LSDB Overflow........................ FALSE
External LSA Count............................ 0
External LSA Checksum......................... 0
AS_OPAQUE LSA Count........................... 0
AS_OPAQUE LSA Checksum........................ 0
```

```
New LSAs Originated.......................... 55
LSAs Received................................ 82
LSA Count.................................... 1
Maximum Number of LSAs....................... 24200
LSA High Water Mark.......................... 9
AS Scope LSA Flood List Length............... 0
Retransmit List Entries...................... 0
Maximum Number of Retransmit Entries......... 96800
Retransmit Entries High Water Mark........... 1
NSF Helper Support........................... Always
NSF Helper Strict LSA Checking............... Enabled
Prefix-suppression........................... Disabled
```

7.13.5.2 show ip ospf abr

This command displays the internal OSPF routing table entries to Area Border Routers (ABR) for the specified virtual router. If no router is specified, it displays information for the default router.

Format `show ip ospf abr [vrf vrf-name]`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Type	The type of the route to the destination. It can be either: ■ intra — Intra-area route ■ inter — Inter-area route
Router ID	Router ID of the destination.
Cost	Cost of using this route.
Area ID	The area ID of the area from which this route is learned.
Next Hop	Next hop toward the destination.
Next Hop Intf	The outgoing router interface to use when forwarding traffic to the next hop.

7.13.5.3 show ip ospf area

This command displays information about the area for the specified virtual router. If no router is specified, it displays information for the default router. The *areaid* identifies the OSPF area that is being displayed.

Format `show ip ospf area areaid [vrf vrf-name]`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
AreaID	The area id of the requested OSPF area.
External Routing	A number representing the external routing capabilities for this area.
Spf Runs	The number of times that the intra-area route table has been calculated using this area's link-state database.
Area Border Router Count	The total number of area border routers reachable within this area.
Area LSA Count	Total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.

Term	Definition
Area LSA Checksum	A number representing the Area LSA Checksum for the specified AreaID excluding the external (LS type 5) link-state advertisements.
Flood List Length	The number of LSAs waiting to be flooded within the area.
Import Summary LSAs	Shows whether to import summary LSAs.
OSPF Stub Metric Value	The metric value of the stub area. This field displays only if the area is a configured as a stub area.

The following OSPF NSSA specific information displays only if the area is configured as an NSSA:

Term	Definition
Import Summary LSAs	Shows whether to import summary LSAs into the NSSA.
Redistribute into NSSA	Shows whether to redistribute information into the NSSA.
Default Information Originate	Shows whether to advertise a default route into the NSSA.
Default Metric	The metric value for the default route advertised into the NSSA.
Default Metric Type	The metric type for the default route advertised into the NSSA.
Translator Role	The NSSA translator role of the ABR, which is always or candidate.
Translator Stability Interval	The amount of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router.
Translator State	Shows whether the ABR translator state is disabled, always, or elected.

Example: The following shows example CLI display output for the command.

```
(R1) #show ip ospf area 1


AreaID..................................... 0.0.0.1
External Routing........................... Import External LSAs
Spf Runs................................... 10
Area Border Router Count................... 0
Area LSA Count............................. 3004
Area LSA Checksum.......................... 0x5e0abed
Flood List Length.......................... 0
Import Summary LSAs........................ Enable
```

7.13.5.4 show ip ospf asbr

This command displays the internal OSPF routing table entries to Autonomous System Boundary Routers (ASBR) for the specified virtual router. If no router is specified, it displays information for the default router.

Format `show ip ospf asbr [vrf` *`vrf-name`*`]`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Type	The type of the route to the destination. It can be one of the following values: intra — Intra-area route inter — Inter-area route
Router ID	Router ID of the destination.
Cost	Cost of using this route.
Area ID	The area ID of the area from which this route is learned.
Next Hop	Next hop toward the destination.
Next Hop Intf	The outgoing router interface to use when forwarding traffic to the next hop.

7.13.5.5 show ip ospf database

This command displays information about the link state database when OSPF is enabled for the specified virtual router. If no router is specified, it displays information for the default router. If you do not enter any parameters, the command displays the LSA headers for all areas. Use the optional *areaid* parameter to display database information about a specific area. Use the optional parameters to specify the type of link state advertisements to display.

Parameter	Description
vrf-name	Specifies the virtual router for which to display information.
asbr-summary	Use *asbr-summary* to show the autonomous system boundary router (ASBR) summary LSAs.
external	Use *external* to display the external LSAs.
network	Use *network* to display the network LSAs.
nssa-external	Use *nssa-external* to display NSSA external LSAs.
opaque-area	Use *opaque-area* to display area opaque LSAs.
opaque-as	Use *opaque-as* to display AS opaque LSAs.
opaque-link	Use *opaque-link* to display link opaque LSAs.
router	Use *router* to display router LSAs.
summary	Use *summary* to show the LSA database summary information.
lsid	Use *lsid* to specify the link state ID (LSID). The value of *lsid* can be an IP address or an integer in the range of 0-4294967295.
adv-router	Use *adv-router* to show the LSAs that are restricted by the advertising router.
self-originate	Use *self-originate* to display the LSAs in that are self originated. The information below is only displayed if OSPF is enabled

The information below is only displayed if OSPF is enabled.

Format `show ip ospf [areaid] database [vrf vrf-name] [{database-summary | [{asbr-summary | external | network | nssa-external | opaque-area | opaque-as | opaque-link | router | summary}] [lsid] [{adv-router [ipaddr] | self-originate}]}]`

Mode
- Privileged EXEC
- User EXEC

For each link-type and area, the following information is displayed:

Term	Definition
Link Id	A number that uniquely identifies an LSA that a router originates from all other self originated LSAs of the same LS type.
Adv Router	The Advertising Router. Is a 32-bit dotted decimal number representing the LSDB interface.
Age	A number representing the age of the link state advertisement in seconds.
Sequence	A number that represents which LSA is more recent.
Checksum	The total number LSA checksum.
Options	This is an integer. It indicates that the LSA receives special handling during routing calculations.
Rtr Opt	Router Options are valid for router links only.

7.13.5.6 show ip ospf database database-summary

Use this command to display the number of each type of LSA in the database for each area and for the router. The command also displays the total number of LSAs in the database.

Format `show ip ospf database database-summary`

Modes
- Privileged EXEC
- User EXEC

Parameter	Definition
Router	Total number of router LSAs in the OSPF link state database.
Network	Total number of network LSAs in the OSPF link state database.
Summary Net	Total number of summary network LSAs in the database.
Summary ASBR	Number of summary ASBR LSAs in the database.
Type-7 Ext	Total number of Type-7 external LSAs in the database.
Self-Originated Type-7	Total number of self originated AS external LSAs in the OSPF link state database.
Opaque Link	Number of opaque link LSAs in the database.
Opaque Area	Number of opaque area LSAs in the database.
Subtotal	Number of entries for the identified area.
Opaque AS	Number of opaque AS LSAs in the database.
Total	Number of entries for all areas.

7.13.5.7 show ip ospf interface

This command displays the information for the IFO object or virtual interface tables.

Format `show ip ospf interface {`*`slot/port`* `| vlan` *`vlan-id`* `| loopback` *`loopback-id`*`}`

Mode
- Privileged EXEC
- User EXEC

Parameter	Definition
IP Address	The IP address for the specified interface.
Subnet Mask	A mask of the network and host portion of the IP address for the OSPF interface.

Parameter	Definition
Secondary IP Address(es)	The secondary IP addresses if any are configured on the interface.
OSPF Admin Mode	States whether OSPF is enabled or disabled on a router interface.
OSPF Area ID	The OSPF Area ID for the specified interface.
OSPF Network Type	The type of network on this interface that the OSPF is running on.
Router Priority	A number representing the OSPF Priority for the specified interface.
Retransmit Interval	A number representing the OSPF Retransmit Interval for the specified interface.
Hello Interval	A number representing the OSPF Hello Interval for the specified interface.
Dead Interval	A number representing the OSPF Dead Interval for the specified interface.
LSA Ack Interval	A number representing the OSPF LSA Acknowledgment Interval for the specified interface.
Transmit Delay	A number representing the OSPF Transmit Delay Interval for the specified interface.
Authentication Type	The OSPF Authentication Type for the specified interface are: none, simple, and encrypt.
Metric Cost	The cost of the OSPF interface.
Passive Status	Shows whether the interface is passive or not.
OSPF MTU-ignore	Indicates whether to ignore MTU mismatches in database descriptor packets sent from neighboring routers.
Flood Blocking	Indicates whether flood blocking is enabled on the interface.

The information below will only be displayed if OSPF is enabled.

Parameter	Definition
OSPF Interface Type	Broadcast LANs, such as Ethernet and IEEE 802.5, take the value `broadcast`. The OSPF Interface Type will be 'broadcast'.
State	The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router.
Designated Router	The router ID representing the designated router.
Backup Designated Router	The router ID representing the backup designated router.
Number of Link Events	The number of link events.
Local Link LSAs	The number of Link Local Opaque LSAs in the link-state database.
Local Link LSA Checksum	The sum of LS Checksums of Link Local Opaque LSAs in the link-state database.
Prefix-suppression	Displays whether prefix-suppression is enabled, disabled, or unconfigured on the given interface.

Example: The following shows example CLI display output for the command when the OSPF Admin Mode is disabled.

```
(Routing) >show ip ospf interface 0/1

IP Address..................................... 0.0.0.0
Subnet Mask.................................... 0.0.0.0
Secondary IP Address(es).......................
OSPF Admin Mode................................ Disable
OSPF Area ID................................... 0.0.0.0
OSPF Network Type.............................. Broadcast
Router Priority................................ 1
Retransmit Interval............................ 5
Hello Interval................................. 10
Dead Interval.................................. 40
LSA Ack Interval............................... 1
Transmit Delay................................. 1
Authentication Type............................ None
Metric Cost.................................... 1  (computed)
```

```
Passive Status.............................. Non-passive interface
OSPF Mtu-ignore............................. Disable
Flood Blocking.............................. Disable

OSPF is not enabled on this interface.

(Routing) #
```

7.13.5.8 show ip ospf interface brief

This command displays brief information for the IFO object or virtual interface tables for the specified virtual router. If no router is specified, it displays information for the default router.

Format `show ip ospf interface brief [vrf vrf-name]`

Mode
- Privileged EXEC
- User EXEC

Parameter	Definition
Interface	*slot/port*
OSPF Admin Mode	States whether OSPF is enabled or disabled on a router interface.
OSPF Area ID	The OSPF Area Id for the specified interface.
Router Priority	A number representing the OSPF Priority for the specified interface.
Cost	The metric cost of the OSPF interface.
Hello Interval	A number representing the OSPF Hello Interval for the specified interface.
Dead Interval	A number representing the OSPF Dead Interval for the specified interface.
Retransmit Interval	A number representing the OSPF Retransmit Interval for the specified interface.
Interface Transmit Delay	A number representing the OSPF Transmit Delay for the specified interface.
LSA Ack Interval	A number representing the OSPF LSA Acknowledgment Interval for the specified interface.

7.13.5.9 show ip ospf interface stats

This command displays the statistics for a specific interface. The information below will only be displayed if OSPF is enabled.

Format `show ip ospf interface stats {slot/port |vlan vlan-id}`

Modes
- Privileged EXEC
- User EXEC

Parameter	Definition
OSPF Area ID	The area id of this OSPF interface.
Area Border Router Count	The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF pass.
AS Border Router Count	The total number of Autonomous System border routers reachable within this area.
Area LSA Count	The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.
IP Address	The IP address associated with this OSPF interface.
OSPF Interface Events	The number of times the specified OSPF interface has changed its state, or an error has occurred.

Parameter	Definition
Virtual Events	The number of state changes or errors that occurred on this virtual link.
Neighbor Events	The number of times this neighbor relationship has changed state, or an error has occurred.
Sent Packets	The number of OSPF packets transmitted on the interface.
Received Packets	The number of valid OSPF packets received on the interface.
Discards	The number of received OSPF packets discarded because of an error in the packet or an error in processing the packet.
Bad Version	The number of received OSPF packets whose version field in the OSPF header does not match the version of the OSPF process handling the packet.
Source Not On Local Subnet	The number of received packets discarded because the source IP address is not within a subnet configured on a local interface. **NOTE:** This field applies only to OSPFv2.
Virtual Link Not Found	The number of received OSPF packets discarded where the ingress interface is in a non-backbone area and the OSPF header identifies the packet as belonging to the backbone, but OSPF does not have a virtual link to the packet's sender.
Area Mismatch	The number of OSPF packets discarded because the area ID in the OSPF header is not the area ID configured on the ingress interface.
Invalid Destination Address	The number of OSPF packets discarded because the packet's destination IP address is not the address of the ingress interface and is not the AllDrRouters or AllSpfRouters multicast addresses.
Wrong Authentication Type	The number of packets discarded because the authentication type specified in the OSPF header does not match the authentication type configured on the ingress interface. **NOTE:** This field applies only to OSPFv2.
Authentication Failure	The number of OSPF packets dropped because the sender is not an existing neighbor or the sender's IP address does not match the previously recorded IP address for that neighbor. **NOTE:** This field applies only to OSPFv2.
No Neighbor at Source Address	The number of OSPF packets dropped because the sender is not an existing neighbor or the sender's IP address does not match the previously recorded IP address for that neighbor. **NOTE:** Does not apply to Hellos.
Invalid OSPF Packet Type	The number of OSPF packets discarded because the packet type field in the OSPF header is not a known type.
Hellos Ignored	The number of received Hello packets that were ignored by this router from the new neighbors after the limit has been reached for the number of neighbors on an interface or on the system as a whole.

Table 13 lists the number of OSPF packets of each type sent and received on the interface.

Table 13: Type of OSPF Packets Sent and Received on the Interface

Packet Type	Sent	Received
Hello	6960	6960
Database Description	3	3
LS Request	1	1
LS Update	141	42
LS Acknowledgment	40	135

7.13.5.10 show ip ospf lsa-group

This command displays the number of self-originated LSAs within each LSA group for the specified virtual router. If no router is specified, it displays information for the default router.

Format `show ip ospf lsa-group [vrf vrf-name]`

Modes
- Privileged EXEC
- User EXEC

Field	Description
Total self-originated LSAs	The number of LSAs the router is currently originating.
Average LSAs per group	The number of self-originated LSAs divided by the number of LSA groups. The number of LSA groups is the refresh interval (1800 seconds) divided by the pacing interval (configured with timers pacing lsa-group) plus two.
Pacing group limit	The maximum number of self-originated LSAs in one LSA group. If the number of LSAs in a group exceeds this limit, OSPF redistributes LSAs throughout the refresh interval to achieve better balance.
Groups	For each LSA pacing group, the output shows the range of LSA ages in the group and the number of LSAs in the group.

7.13.5.11 show ip ospf neighbor

This command displays information about OSPF neighbors for the specified virtual router. If no router is specified, it displays information for the default router. If you do not specify a neighbor IP address, the output displays summary information in a table. If you specify an interface or tunnel, only the information for that interface or tunnel displays, if the interface is a physical routing interface and vlan format if the interface is a routing vlan. The *ip-address* is the IP address of the neighbor, and when you specify this, detailed information about the neighbor displays. The information below only displays if OSPF is enabled and the interface has a neighbor.

Format `show ip ospf neighbor [vrf vrf-name][interface {slot/port|vlan 1-4093}] [ip-address]`

Modes
- Privileged EXEC
- User EXEC

If you do not specify an IP address, a table with the following columns displays for all neighbors or the neighbor associated with the interface that you specify:

Parameter	Definition
Router ID	The 4-digit dotted-decimal number of the neighbor router.
Priority	The OSPF priority for the specified interface. The priority of an interface is a priority integer from 0 to 255. A value of '0' indicates that the router is not eligible to become the designated router on this network.
IP Address	The IP address of the neighbor.
Interface	The physical routing interface or VLAN routing interface of the local router in *slot/port* format
State	The state of the neighboring routers. Possible values are: ■ Down—Initial state of the neighbor conversation; no recent information has been received from the neighbor. ■ Attempt—No recent information has been received from the neighbor but a more concerted effort should be made to contact the neighbor. ■ Init—An Hello packet has recently been seen from the neighbor, but bidirectional communication has not yet been established. ■ 2 way—Communication between the two routers is bidirectional. ■ Exchange start—The first step in creating an adjacency between the two neighboring routers, the goal is to decide which router is the master and to decide upon the initial DD sequence number. ■ Exchange—The router is describing its entire link state database by sending Database Description packets to the neighbor. ■ Loading—Link State Request packets are sent to the neighbor asking for the more recent LSAs that have been discovered (but not yet received) in the Exchange state. ■ Full—The neighboring routers are fully adjacent and they will now appear in router-LSAs and network-LSAs.
Dead Time	The amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.

If you specify an IP address for the neighbor router, the following fields display:

Parameter	Definition
Interface	*slot/port*
Neighbor IP Address	The IP address of the neighbor router.
Interface Index	The interface ID of the neighbor router.
Area ID	The area ID of the OSPF area associated with the interface.
Options	An integer value that indicates the optional OSPF capabilities supported by the neighbor. The neighbor's optional OSPF capabilities are also listed in its Hello packets. This enables received Hello Packets to be rejected (i.e., neighbor relationships will not even start to form) if there is a mismatch in certain crucial OSPF capabilities.
Router Priority	The OSPF priority for the specified interface. The priority of an interface is a priority integer from 0 to 255. A value of '0' indicates that the router is not eligible to become the designated router on this network.
Dead Timer Due	The amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.
Up Time	Neighbor uptime; how long since the adjacency last reached the Full state.
State	The state of the neighboring routers.
Events	The number of times this neighbor relationship has changed state, or an error has occurred.
Retransmitted LSAs	The number of LSAs retransmitted to this neighbor.
Retransmission Queue Length	An integer representing the current length of the retransmission queue of the specified neighbor router Id of the specified interface.
Restart Helper Status	Indicates the status of this router as a helper during a graceful restart of the router specified in the command line: ■ Helping—This router is acting as a helpful neighbor to this neighbor. A helpful neighbor does not report an adjacency change during graceful restart, but continues to advertise the restarting router as a FULL adjacency. A helpful neighbor continues to forward data packets to the restarting router, trusting that the restarting router's forwarding table is maintained during the restart. ■ Not Helping—This router is not a helpful neighbor at this time.

Parameter	Definition
Restart Reason	When this router is in helpful neighbor mode, this indicates the reason for the restart as provided by the restarting router: ■ Unknown (0) ■ Software restart (1) ■ Software reload/upgrade (2) ■ Switch to redundant control processor (3) ■ Unrecognized - a value not defined in RFC 3623 When EFOS sends a grace LSA, it sets the Restart Reason to Software Restart on a planned warm restart (when the `initiate failover` command is invoked), and to Unknown on an unplanned warm restart.
Remaining Grace Time	The number of seconds remaining the in current graceful restart interval. This is displayed only when this router is currently acting as a helpful neighbor for the router specified in the command.
Restart Helper Exit Reason	Indicates the reason that the specified router last exited a graceful restart. ■ None—Graceful restart has not been attempted ■ In Progress—Restart is in progress ■ Completed—The previous graceful restart completed successfully ■ Timed Out—The previous graceful restart timed out ■ Topology Changed—The previous graceful restart terminated prematurely because of a topology change

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip ospf neighbor 170.1.1.50

Interface.....................................0/17
Neighbor IP Address...........................170.1.1.50
Interface Index...............................17
Area Id.......................................0.0.0.2
Options.......................................0x2
Router Priority...............................1
Dead timer due in (secs)......................15
Up Time.......................................0 days 2 hrs 8 mins 46 secs
State.........................................Full/BACKUP-DR
Events........................................4
Retransmitted LSAs............................32
Retransmission Queue Length...................0
Restart Helper Status..........................  Helping
Restart Reason.................................  Software Restart (1)
Remaining Grace Time...........................  10 sec
Restart Helper Exit Reason.....................  In Progress
```

7.13.5.12 show ip ospf range

This command displays the set of OSPFv2 area ranges configured for a given area for the specified virtual router. If no router is specified, it displays information for the default router.

Format `show ip ospf range` ***areaid*** `[vrf` ***vrf-name***`]`

Modes Privileged EXEC

Term	Definition
Prefix	The summary prefix.
Subnet Mask	The subnetwork mask of the summary prefix.

Term	Definition
Type	**S** (Summary Link) or **E** (External Link)
Action	**Advertise** or **Suppress**
Cost	Metric to be advertised when the range is active. If a static cost is not configured, the field displays **Auto**. If the action is **Suppress**, the field displays **N/A**.
Active	Whether the range is currently active. **Y** or **N**.

Example: The following shows example CLI display output for the command.

```
(R1) #show ip ospf range 0

          Prefix      Subnet Mask   Type     Action       Cost   Active
        10.1.0.0      255.255.0.0      S  Advertise       Auto        N
      172.20.0.0      255.255.0.0      S  Advertise        500        Y
```

7.13.5.13 show ip ospf statistics

This command displays information about recent Shortest Path First (SPF) calculations for the specified virtual router. If no router is specified, it displays information for the default router. The SPF is the OSPF routing table calculation. The output lists the number of times the SPF has run for each OSPF area. A table follows this information. For each of the 15 most recent SPF runs, the command shows statistics for how long ago the SPF ran, how long the SPF took, the reasons why the SPF was scheduled, the individual components of the routing table calculation time and to show the RIB update time. The most recent statistics are displayed at the end of the table.

Format `show ip ospf statistics [vrf` *`vrf-name`*`]`

Modes Privileged EXEC

Term	Definition
Delta T	The time since the routing table was computed. The time is in the format hours, minutes, and seconds (hh:mm:ss).
Intra	The time taken to compute intra-area routes, in milliseconds.
Summ	The time taken to compute inter-area routes, in milliseconds.
Ext	The time taken to compute external routes, in milliseconds.
SPF Total	The total time to compute routes, in milliseconds. The total may exceed the sum of the Intra, Summ, and Ext times.
RIB Update	The time from the completion of the routing table calculation until all changes have been made in the common routing table [the Routing Information Base (RIB)], in milliseconds.
Reason	The event or events that triggered the SPF. Reason codes are as follows: ■ R - new router LSA ■ N - new network LSA ■ SN - new network summary LSA ■ SA - new ASBR summary LSA ■ X - new external LSA

Example: The following shows example CLI display output for the command.

```
(Router) #show ip ospf statistics

 Area 0.0.0.0: SPF algorithm executed 15 times
```

```
Delta T         Intra       Summ        Ext    SPF Total   RIB Update  Reason

00:05:33            0          0          0            0            0  R
00:05:30            0          0          0            0            0  R
00:05:19            0          0          0            0            0  N, SN
00:05:15            0         10          0           10            0  R, N, SN
00:05:11            0          0          0            0            0  R
00:04:50            0         60          0           60          460  R, N
00:04:46            0         90          0          100           60  R, N
00:03:42            0         70         10           90          160  R
00:03:39            0         70         40          120          240  X
00:03:36            0         60         60          130          160  X
00:01:28            0         60         50          130          240  X
00:01:25            0         30         50          110          310  SN
00:01:22            0          0         40           50          260  SN
00:01:19            0          0         20           20          190  X
00:01:16            0          0          0            0          110  R, X
```

7.13.5.14 show ip ospf stub table

This command displays the OSPF stub table for the virtual router. If no router is specified, the information for the default router will be displayed. The information below will only be displayed if OSPF is initialized on the switch.

Format `show ip ospf stub table [vrf` *`vrf-name`*`]`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Area ID	A 32-bit identifier for the created stub area.
Type of Service	The type of service associated with the stub metric. EFOS only supports Normal TOS.
Metric Val	The metric value is applied based on the TOS. It defaults to the least metric of the type of service among the interfaces to other areas. The OSPF cost for a route is a function of the metric value.
Import Summary LSA	Controls the import of summary LSAs into stub areas.

7.13.5.15 show ip ospf traffic

This command displays OSPFv2 packet and LSA statistics and OSPFv2 message queue statistics for the virtual router. If no router is specified, the information for the default router will be displayed. Packet statistics count packets and LSAs since OSPFv2 counters were last cleared (using the Section 7.13.1.25, clear ip ospf counters command).

NOTE: The Section 7.13.1.25, clear ip ospf counters command does not clear the message queue high water marks.

Format `show ip ospf traffic [vrf` *`vrf-name`*`]`

Modes Privileged EXEC

Parameter	Description
OSPFv2 Packet Statistics	The number of packets of each type sent and received since OSPF counters were last cleared.
LSAs Retransmitted	The number of LSAs retransmitted by this router since OSPF counters were last cleared.

Parameter	Description
LS Update Max Receive Rate	The maximum rate of LS Update packets received during any 5-second interval since OSPF counters were last cleared. The rate is in packets per second.
LS Update Max Send Rate	The maximum rate of LS Update packets transmitted during any 5-second interval since OSPF counters were last cleared. The rate is in packets per second.
Number of LSAs Received	The number of LSAs of each type received since OSPF counters were last cleared.
OSPFv2 Queue Statistics	For each OSPFv2 message queue, the current count, the high water mark, the number of packets that failed to be enqueued, and the queue limit. The high water marks are not cleared when OSPF counters are cleared.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip ospf traffic

Time Since Counters Cleared:  4000 seconds

OSPFv2 Packet Statistics

         Hello   Database Desc   LS Request   LS Update    LS ACK   Total
Recd:      500              10           20          50        20     600
Sent:      400               8           16          40        16     480

LSAs Retransmitted.................0
LS Update Max Receive Rate........20 pps
LS Update Max Send Rate...........10 pps

Number of LSAs Received

T1 (Router).......................10
T2 (Network)......................0
T3 (Net Summary)..................300
T4 (ASBR Summary).................15
T5 (External).....................20
T7 (NSSA External)................0
T9 (Link Opaque)..................0
T10 (Area Opaque).................0
T11 (AS Opaque)...................0
Total............................345

OSPFv2 Queue Statistics

             Current       Max     Drops   Limit
Hello              0        10         0     500
ACK                2        12         0    1680
Data              24        47         0     500
Event              1         8         0    1000
```

7.13.5.16 show ip ospf virtual-link

This command displays the OSPF Virtual Interface information for a specific area and neighbor for the virtual router. If no router is specified, the information for the default router will be displayed. The *areaid* parameter identifies the area and the *neighbor* parameter identifies the neighbor's Router ID.

Format `show ip ospf virtual-link [vrf` *vrf-name*`]` *areaid neighbor*

Modes
- Privileged EXEC
- User EXEC

Parameter	Definition
Area ID	The area id of the requested OSPF area.
Neighbor Router ID	The input neighbor Router ID.
Hello Interval	The configured hello interval for the OSPF virtual interface.
Dead Interval	The configured dead interval for the OSPF virtual interface.
Interface Transmit Delay	The configured transmit delay for the OSPF virtual interface.
Retransmit Interval	The configured retransmit interval for the OSPF virtual interface.
Authentication Type	The configured authentication type of the OSPF virtual interface.
State	The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router. This is the state of the OSPF interface.
Neighbor State	The neighbor state.

7.13.5.17 show ip ospf virtual-link brief

This command displays the OSPF Virtual Interface information for all areas in the system.

Format `show ip ospf virtual-link brief`

Modes
- Privileged EXEC
- User EXEC

Parameter	Definition
Area ID	The area id of the requested OSPF area.
Neighbor	The neighbor interface of the OSPF virtual interface.
Hello Interval	The configured hello interval for the OSPF virtual interface.
Dead Interval	The configured dead interval for the OSPF virtual interface.
Retransmit Interval	The configured retransmit interval for the OSPF virtual interface.
Transmit Delay	The configured transmit delay for the OSPF virtual interface.

7.14 ICMP Throttling Commands

This section describes the commands you use to configure options for the transmission of various types of ICMP messages.

7.14.0.1 ip unreachables

Use this command to enable the generation of ICMP Destination Unreachable messages on an interface or range of interfaces. By default, the generation of ICMP Destination Unreachable messages is enabled.

Default enable

Format `ip unreachables`

Mode Interface Config

7.14.0.1.1 no ip unreachables

Use this command to prevent the generation of ICMP Destination Unreachable messages.

Format `no ip unreachables`

Mode Interface Config

7.14.0.2 ip redirects

Use this command to enable the generation of ICMP Redirect messages by the router. By default, the generation of ICMP Redirect messages is enabled. You can use this command to configure an interface, a range of interfaces, or all interfaces.

Default enable

Format `ip redirects`

Mode
- Global Config
- Interface Config
- Virtual Router Config

7.14.0.2.1 no ip redirects

Use this command to prevent the generation of ICMP Redirect messages by the router.

Format `no ip redirects`

Mode
- Global Config
- Interface Config

7.14.0.3 ipv6 redirects

Use this command to enable the generation of ICMPv6 Redirect messages by the router. By default, the generation of ICMP Redirect messages is enabled. You can use this command to configure an interface, a range of interfaces, or all interfaces.

Default enable

Format `ipv6 redirects`

Mode Interface Config

7.14.0.3.1 no ipv6 redirects

Use this command to prevent the generation of ICMPv6 Redirect messages by the router.

Format `no ipv6 redirects`
Mode Interface Config

7.14.0.4 ip icmp echo-reply

Use this command to enable the generation of ICMP Echo Reply messages by the router. By default, the generation of ICMP Echo Reply messages is enabled.

Default enable
Format `ip icmp echo-reply`
Mode
- Global Config
- Virtual Router Config

7.14.0.4.1 no ip icmp echo-reply

Use this command to prevent the generation of ICMP Echo Reply messages by the router.

Format `no ip icmp echo-reply`
Mode Global Config

7.14.0.5 ip icmp error-interval

Use this command to limit the rate at which IPv4 ICMP error messages are sent. The rate limit is configured as a token bucket, with two configurable parameters, *burst-size* and *burst-interval*.

The *burst-interval* specifies how often the token bucket is initialized with *burst-size* tokens. *burst-interval* is from 0 to 2147483647 milliseconds (msec). The *burst-size* is the number of ICMP error messages that can be sent during one *burst-interval*. The range is from 1 to 200 messages. To disable ICMP rate limiting, set *burst-interval* to zero (0).

Default
- *burst-interval* of 1000 msec.
- *burst-size* of 100 messages

Format `ip icmp error-interval` *`burst-interval [burst-size]`*
Mode
- Global Config
- Virtual Router Config

7.14.0.5.1 no ip icmp error-interval

Use the **no** form of the command to return *burst-interval* and *burst-size* to their default values.

Format `no ip icmp error-interval`
Mode
- Global Config
- Virtual Router Config

7.15 Bidirectional Forwarding Detection Commands

Bidirectional Forwarding Detection (BFD) verifies bidirectional connectivity between forwarding engines, which can be a single or multi-hop away. The protocol works over any underlying transmission mechanism and protocol layer with a wide range of detection times, especially in scenarios where fast failure detection is required in data plane level for multiple concurrent sessions.

Use the following commands to configure Bidirectional Forwarding Detection commands (BFD).

7.15.0.1 bfd

This command enables BFD on all interfaces associated with the OSPF process. BFD must be enabled on the individual interface to trigger BFD on that interface.

Default	Disabled
Format	`bfd`
Mode	Router OSPF Config

Example: Do the following to trigger BFD processing through OSPF globally on all the interfaces that are associated with it.

```
(Router) (Config)# router ospf
(Router) (Config-router)# bfd
(Router) (Config-router)# exit
```

7.15.0.1.1 no bfd

This command disables BFD globally on all interfaces associated with the OSPF process.

Format	`no bfd`
Mode	Router OSPF Config

7.15.0.2 feature bfd

This command enables BFD on the device. Note that BFD must be enabled in order to configure other protocol and interface parameters.

Default	Disabled
Format	`feature bfd`
Mode	Global Config

7.15.0.2.1 no feature bfd

Disables BFD globally and removes runtime session data. Static configurations are retained.

Format	`no feature bfd`
Mode	Global Config

Example:

```
(Router)# configure
(Router) (Config)# feature bfd
(Router) (Config)# exit
```

7.15.0.3 bfd echo

This command enables BFD echo mode on an IP interface.

Default Disabled

Format `bfd echo`

Mode Interface Config

Example:

```
(Router) (Config)# interface 0/1
(Router) (Interface 0/1)# no bfd echo
(Router) (Interface 0/1)# exit
```

7.15.0.3.1 no bfd echo

This command disables BFD echo mode on an IP interface.

Format `no bfd echo`

Mode Interface Config

7.15.0.4 bfd interval

This command configures the BFD session parameters for all available interfaces on the device (Global Config mode) or IP interface (Interface Config mode). It overwrites any BFD configurations present on individual interfaces (Global Config mode) or globally configured BFD session parameters (Interface Config).

Default None

Format `bfd interval` ***`transmit-interval`*** `min_rx` ***`minimum-receive-interval`*** `multiplier` ***`detection-time-multiplier`***

Mode
- Global Config
- Interface Config

Parameters	Description
transmit-interval	The desired minimum transmit interval, which is the minimum interval that the user wants to use while transmitting BFD control packets. It is represented in milliseconds. Its range is 100 ms to 1000 ms (with a change granularity of 100) a with default value of 100 ms.
minimum-receive-interval	The required minimum receive interval, which is the minimum interval at which the system can receive BFD control packets. It is represented in milliseconds. Its range is 100 ms to 1000 ms (with a change granularity of 100) with a default value of 100 ms.
detection-time-multiplier	The number of BFD control packets that must be missed in a row to declare a session down. Its range is 1 to 50 with default value of 3.

Example: The following steps configure BFD session parameters on the device, in Privileged EXEC mode.

```
(Router)# configure
(Router) (Config)# bfd interval 100 min_rx 200 multiplier 5
```

```
(Router) (Config)# exit
```

Example: The following steps configure BFD session parameters on an interface (for example, 0/1).

```
(Router) (Config)# interface 0/1
(Router) (Interface 0/1)# bfd interval 100 min_rx 200 multiplier 5
(Router) (Interface 0/1)# exit
```

7.15.0.4.1 no bfd interval

In Global Config mode, this command resets the BFD session parameters for all available interfaces on the device to their default values. In Interface Config mode, this command resets the BFD session parameters for all sessions on an IP interface to their default values.

Format `no bfd interval`

Mode
- Global Config
- Interface Config

7.15.0.5 bfd slow-timer

This command sets up the required echo receive interval preference value. This value determines the interval the asynchronous sessions use for BFD control packets the when echo function is enabled. The slow-timer value is used as the new control packet interval, while the echo packets use the configured BFD intervals.

Default 2000

Format `bfd slow-timer` *`echo-receive-interval`*

Mode Global Config

Parameters	Description
echo-receive-interval	The value is represented in milliseconds. Its range is 1000 ms to 30000 ms (with a change granularity of 100) with default value of 2000 ms.

Example:

```
(Router)# configure
(Router) (Config)# bfd slow-timer 10000
(Router) (Config)# exit
```

7.15.0.5.1 no bfd slow-timer

This command resets the BFD slow-timer preference value to its default.

Format `no bfd slow-timer`

Mode Global Config

7.15.0.6 ip ospf bfd

This command enables BFD on interfaces associated with the OSPF process.

Default Disabled

Format `ip ospf bfd`

Mode Interface Config

7.15.0.6.1 ip ospf bfd

This command disables BFD on interfaces associated with the OSPF process.

Default Disabled
Format `no ip ospf bfd`
Mode Interface Config

7.15.0.7 neighbor fall-over bfd

This command enables BFD support for fast failover for a BGP neighbor.

Default Disabled
Format `neighbor` *`ipaddress`* `fall-over bfd`
Mode Router BGP Config

Example: Do the following to trigger BFD processing through BGP on an interface that is associated with it.

```
(Router) (Config)# router bgp
(Router) (Config-router)# neighbor 172.16.11.6 fall-over bfd
(Router) (Config-router)# exit
```

7.15.0.7.1 no bfd

This command disables BFD support for fast failover for a BGP neighbor.

Format `neighbor` *`ipaddress`* `fall-over bfd`
Mode Router BGP Config

7.15.0.8 show bfd neighbors

This command displays the BFD adjacency list showing the active BFD neighbors.

Format `show bfd neighbors [details]`
Mode Privileged EXEC

Parameters	Description
details	Provides additional details with the routing protocol BFD has registered and displays the Admin Mode status as Enabled or Disabled.

The following information is displayed.

Parameters	Description
Our IP address	The current IP address.
Neighbor IP address	The IP address of the active BFD neighbor.

Parameters	Description
State	The current state, either Up or Down.
Interface	The current interface.
Uptime	The amount of time the interface has been up.
Registered Protocol	The protocol from which the BFD session was initiated and that is registered to receive events from BFD. (for example, BGP).
Local Diag	The diagnostic state specifying the reason for the most recent change in the local session state.
Demand mode	Indicates if the system wishes to use Demand mode. **NOTE:** Demand mode is not supported in the current EFOS release.
Minimum transmit interval	The minimum interval to use when transmitting BFD control packets.
Actual TX Interval	The transmitting interval being used for control packets.
Actual TX Echo interval	The transmitting interval being used for echo packets.
Minimum receive interval	The minimum interval at which the system can receive BFD control packets.
Detection interval multiplier	The number of BFD control packets that must be missed in a row to declare a session down.
My discriminator	Unique Session Identifier for Local BFD Session.
Your discriminator	Unique Session Identifier for Remote BFD Session.
Tx Count	The number of transmitted BFD packets.
Rx Count	The number of received BFD packets.
Drop Count	The number of dropped packets.

Example:

```
(Router)# show bfd neighbors

Admin Mode: Enabled

OurAddr          NeighAddr        State       Interface    Uptime
--------------   --------------   ----------  ----------   ----------
192.168.20.1     192.168.20.2     Up          0/77         0:0:21:30
2001::1          2001::2          Up          0/78         0:0:0:18
(Router)# show bfd neighbors details

Admin Mode: Enabled

Our IP address................................ 2.1.1.1
Neighbor IP address........................... 2.1.1.2
State......................................... Up
Interface..................................... 0/15
Uptime........................................ 0:0:0:10
Registered Protocol........................... BGP
Local Diag.................................... None
Demand mode................................... FALSE
Minimum transmit interval..................... 100
Minimum receive interval...................... 100
Actual tx interval............................ 100
Actual tx echo interval....................... 0
Detection interval multiplier................. 3
My discriminator.............................. 1
Your discriminator............................ 1
Tx Count...................................... 105
Rx Count...................................... 107
Drop Count.................................... 0
```

7.15.0.9 debug bfd event

This command displays BFD state transition information.

Format	`debug bfd event`
Mode	Privileged EXEC

7.15.0.10 debug bfd packet

This command displays BFD control packet debugging information.

Format	`debug bfd packet`
Mode	Privileged EXEC

7.16 IP Service Level Agreement Commands

The IP service-level agreement (SLA) feature allows users to monitor network performance between routers or from a router to a remote IP device. EFOS 3.4.3 supports the following measurement capabilities:

- Remote IP reachability tracking.
- Round-trip-time threshold monitoring

These metrics are collected by measuring ICMP response time and connectivity. This feature is deployed mostly in Enterprise networks on multi-homed customer edge devices, where there is a need to automatically switch to the next priority ISP in case of reachability issues with the current ISP.

7.16.0.1 ip sla

Use this command to start configuring an IP Service Level Agreements (SLAs) operation and enter the IP SLA configuration mode.

Default	No IP SLA operation is configured.
Format	`ip sla` *`operation-number`*
Mode	Global Config

Parameters	Description
operation-number	Identifies the IP SLAs operation being configured. The range is from 1 to 128.

Usage Guidelines

Start configuring an IP SLA operation by using the `ip sla` command. This command specifies an identification number for the operation to being configured. Once this command is entered, the router enters IP SLA configuration mode.

This command is supported in IPv4 networks and also for IPv6 networks where IPv6 addresses are supported.

The maximum number of IP SLAs supported is 128 (IPv4 and IPv6 combined).

Once an operation is configured it needs to be scheduled to be started. Refer to the `ip sla schedule` global configuration command for more details on scheduling of an operation.

NOTE: The configuration of an operation cannot be modified after an operation has been scheduled to start. For modifying the configuration of the operation after it is scheduled, the operation must either be stopped or must be deleted first (using the `no ip sla` command) and then reconfigured with new operation parameters.

To display the current operational state of an IP SLA operation, use the `show ip sla configuration` command in user EXEC or privileged EXEC mode.

Example:

The following example shows an operation 55 being configured as an ICMP Echo operation in an IPv4 network and being scheduled to start. In the below example the `ip sla` command being used in an IPv4 network is shown.

```
(Routing)(config)# ip sla 55
(Routing)(config-ip-sla)#icmp-echo 172.16.1.175
(Routing)  (config-ip-sla-echo)#exit
(Routing)(config-ip-sla)#exit
(Routing)(config)# ip sla schedule 55
```

NOTE: In case the operation 55 is already configured and has not been scheduled, the command line interface will enter IP SLA configuration mode for operation 55. If the operation already exists and has been scheduled, this command will fail.

7.16.0.1.1 no ip sla

Use this command to remove all the configuration information of an IP SLA operation, which also includes removing the schedule of the operation.

Format `no ip sla` *`operation-number`*
Mode Global Config

7.16.0.2 ip sla schedule

After configuring an IP SLA operation, the IP SLA is in pending state and needs to be started using the `ip sla schedule` global configuration command. To stop the operation and place it in the default state (pending), use the no form of this command.

Default By default the operation is put in a pending state. In the pending state the operation is enabled but does not actively probe and collect information.
Format `ip sla schedule` *`operation-number`*
Mode Global Config

Parameters	Description
operation-number	Identifies the IP SLAs operation being configured. The range is from 1 to 128.

Usage Guidelines

By default IP SLAs are not scheduled to start. Once an IP SLA object is created using the `ip sla` global configuration command it needs to be started (with a lifetime of forever) by using the `ip sla schedule` CLI configuration command. When an `ip sla schedule` command is issued the ip sla operation transitions from pending state to active and immediately begins probing and collecting information. The IP SLA probes can be stopped by unconfiguring the IP SLA schedule config by using the `no ip sla schedule` command.

This command is supported in IPv4 networks and also for IPv6 networks where IPv6 addresses are supported.

NOTE: After you schedule an operation, you cannot modify the configuration of the operation. To modify the configuration of the operation after it is scheduled, you must first stop the operation by using the `no ip schedule` command and then modify the configuration. Or else you must first delete the IP SLAs operation (using the `no ip sla` command) and then reconfigure the operation with the new operation parameters.

To display the current configuration settings of the operation, use the `show ip sla configuration` command in user EXEC or privileged EXEC mode.

Example:

In the following example, operation 55 is configured as a ICMP Echo operation in an IPv4 network and is scheduled to start. The example shows the `ip sla schedule` command being used in an IPv4 network.

```
(Routing)(config)# ip sla 55
(Routing)(config-ip-sla)# icmp-echo 172.16.1.175
(Routing)  (config-ip-sla-echo)#exit
(Routing)(config-ip-sla)#exit
(Routing)(config)# ip sla schedule 55
```

7.16.0.2.1 no ip sla schedule

Use this command to stop the operation and place it in the default state (pending).

Format `no ip sla schedule` *`operation-number`*
Mode Global Config

7.16.0.3 track ip sla

Use this command to track the state of an IP Service Level Agreements (SLAs) operation and to enter tracking configuration mode.

Default Disabled
Format `track object-number ip sla operation-number [reachability | state]`
Mode Global Config

Parameters	Description
object-number	Identifies the object to be tracked. The range is from 1 to 128.
operation-number	Identifies the IP SLAs operation to be tracked.
reachability	Tracks whether the route is reachable.
state	Tracks the operation return code.

Usage Guidelines

An operation return-code value is maintained by every IP SLAs operation. This return code is interpreted by the tracking process. The return code may return OK, OverThreshold, and Timeout.

Two facets of an IP SLAs operation can be tracked: reachability and state. The acceptance of the OverThreshold return code is the difference between these facets. Table 1 below shows the comparision between the reachability and state facets of IP SLAs operations that can be tracked.

Table 14: Comparison of Reachability and State Operations

Tracking	Return Code	Track State
Reachability	OK or OverThreshold Timeout	Up Down
State	OK Timeout, OverThreshold	Up Down

Tracking of a maximum of 128 (IPv4 and IPv6 combined) track objects is supported. If neither of the optional keywords (`reachability` or `state`) is specified in a configured `track ip sla` CLI command, then the default tracking type value `reachability` gets configured.

Example:

In the following example, the tracking process is configured to track the *state* of IP SLAs operation 5:

```
(Routing)(config)# track 2 ip sla 5 state
```

In the following example, the tracking process is configured to track the *reachability* of IP SLAs operation 6:

```
(Routing)(config)# track 3 ip sla 6 reachability
```

7.16.0.3.1 no track ip sla

Use this command to remove the tracking.

Format `no track object-number`
Mode Global Config

7.16.1 Track Configuration Mode Commands

7.16.1.1 delay

To configure a delay for acting upon a track object reachability state changes, use the delay command in Track configuration mode.

Default None
Format `delay {up` *`seconds`* `[down` *`seconds`*`] | [down` *`seconds`*`] up` *`seconds`*`}`
Mode Track Config

Parameters	Description
up *seconds*	Time to delay the notification of an up event. Delay value, in seconds. The range is from 0 to 180. The default is 0.
down *seconds*	Time to delay the notification of an down event. Delay value, in seconds. The range is from 0 to 180. The default is 0.

Usage Guidelines

To minimize flapping of the reachability state (Up/Down), use the `delay` command to introduce a non-zero delay in seconds between the UP and DOWN state transitions per Track object.

Delay time specifies the hold interval for an (UP/DOWN) state before taking action on the associated static routes.

Example:

In the following example, Track object 10 is created and is associated with the IP SLAs operation 11 and then an up delay of 5 seconds and a down delay of 3 seconds is configured:

```
(Routing)(config)#track 10 ip sla 11
(Routing)(config-track)#delay up 5 down 3
```

7.16.1.1.1 no delay

Use this command to reset the delay for acting upon a track object reachability state changes to the default value.

Format	`no delay`
Mode	Track Config

7.16.2 IP SLA Configuration Mode Commands

7.16.2.1 icmp-echo

Use this command in IP SLA configuration mode, to configure an IP Service Level Agreements (SLAs) Internet Control Message Protocol (ICMP) echo operation.

Default	No IP SLAs operation type is configured for the operation being configured.
Format	`icmp-echo` ***`destination-ip-address`*** `[source-interface {`***`interface-name`*** `| vlan` ***`vlan-id`***`}]`
Mode	IP SLA Config

Parameters	Description
destination-ip-address	Destination IPv4 or IPv6 address.
source-interface {interface-name | vlan vlan-id}	Used to specify the source interface for the operation.

Usage Guidelines

You must configure the type of IP SLAs operation (ICMP echo) before you can configure any of the other parameters of the operation. To change the operation values (`destination-ip-address` or `source-interface-name`) of an existing scheduled IP SLAs ICMP echo operation, you must stop the IP SLA operation by using the `no ip sla schedule operation-number`. Or else you must first delete the IP SLAs operation (using the `no ip sla global configuration` command) and then reconfigure the operation with the new operation values.

IP SLAs ICMP echo operations support both IPv4 and IPv6 addresses.

Example:

In the following example, IP SLAs operation 12 is created and configured as an echo operation using the ICMP protocol and the destination IPv4 address 143.1.16.125:

```
(Routing)(config)#ip sla 12
(Routing)(config-ip-sla)#icmp-echo 143.1.16.125
```

In the following example, IP SLAs operation 13 is created and configured as an echo operation using the ICMP protocol and the destination IPv6 address 3001:CD6:200::1:

```
(Routing)(config)#ip sla 13
(Routing)(config-ip-sla)#icmp-echo 3001:CD6:200::1
```

7.16.3 IP SLA ICMP ECHO Configuration Mode Commands

7.16.3.1 frequency

Use this command to set the rate at which a specified IP Service Level Agreements (SLAs) operation repeats in the ICMP echo configuration sub-mode of IP SLA configuration mode.

Default 60 seconds

Format `frequency` *seconds*

Mode IP SLA ICMP ECHO Config

Parameters	Description
seconds	Number of seconds between the IP SLAs operations. Range is 1 to 3600.

Usage Guidelines

A single IP SLAs operation will repeat at a given frequency for the lifetime of the operation. For example, the ICMP Echo operation with a frequency of 60 sends an ICMP Echo Request packet once every 60 seconds, for the lifetime of the operation. This packet is sent when the operation is started, then is sent again 60 seconds later.

If an individual IP SLAs operation takes longer to execute than the specified frequency value, a statistics counter called “busy” is incremented rather than immediately repeating the operation.

Following are the recommended guidelines for configuring the `frequency`, `timeout` and `threshold` commands of the IP SLAs ICMP Echo operation:

`(frequency` *seconds*`)` → `(timeout` *milliseconds*`)` → `(threshold` *milliseconds*`)`

NOTE: It is recommended to not to set the frequency value to less than 60 seconds because the potential overhead from numerous active operations could significantly affect network performance.

This command is supported in IPv4 networks and also for IPv6 networks where IPv6 addresses are supported.

Example:

The following example shows how to configure an IP SLAs ICMP echo operation (operation 11) to repeat every 80 seconds. This example shows the frequency (IP SLA) command being used in an IPv4 network in ICMP echo configuration mode within IP SLA configuration mode:

```
(Routing)(config)#ip sla 11
```

```
(Routing)(config-ip-sla)#icmp-echo 152.15.10.145
(Routing)(config-ip-sla-echo)#frequency 80
```

7.16.3.1.1 no frequency

Use this command to return the frequency to the default value.

Format `no frequency`
Mode IP SLA ICMP ECHO Config

7.16.3.2 timeout

Use this command to set the amount of time an IP Service Level Agreements (SLAs) operation waits for a response from its request packet. This command is available in the ICMP echo configuration sub-mode of IP SLA configuration mode.

Default 5000 milliseconds
Format `timeout` *`milliseconds`*
Mode IP SLA ICMP ECHO Config

Parameters	Description
milliseconds	Length of time the operation waits to receive a response from its request packet, in milliseconds (ms). The range is 50 to 300000. The value of the milliseconds argument should be based on the sum of both the maximum round-trip time (RTT) value for the packets and the processing time of the IP SLAs operation.

Usage Guidelines

It is recommended that the value of the milliseconds argument be based on the sum of both the maximum round-trip time (RTT) value for the packets and the processing time of the IP SLAs operation.

Use the `timeout` (IP SLA) command to set how long the operation waits to receive a response from its request packet, and use the `frequency` (IP SLA) command to set the rate at which the IP SLAs operation restarts. The value specified for the `timeout` (IP SLA) command cannot be greater than the value specified for the `frequency` (IP SLA) command.

Following are the recommended guidelines for configuring the `frequency`, `timeout` and `threshold` commands of the IP SLAs ICMP Echo operation:

`(frequency` *`seconds`*`)` → `(timeout` *`milliseconds`*`)` → `(threshold` *`milliseconds`*`)`

This command is supported in IPv4 networks and also for IPv6 networks where IPv6 addresses are supported.

Example:

In the following example, the timeout value for an IP SLAs operation 11 is set for 2500 ms:

```
(Routing)(config)#ip sla 11
(Routing)(config-ip-sla)#icmp-echo 152.17.10.145
(Routing)(config-ip-sla-echo)#timeout 2500
```

7.16.3.2.1 no timeout

Use this command to return the timeout to the default value.

Format `timeout` *`milliseconds`*
Mode IP SLA ICMP ECHO Config

7.16.3.3 threshold

Use this command in the ICMP echo configuration sub-mode of IP SLA configuration to set the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.

Default 5000 milliseconds
Format `threshold` *`milliseconds`*
Mode IP SLA ICMP ECHO Config

Parameters	Description
milliseconds	Length of the time in milliseconds, required for a rising threshold to be declared. Range is 50 to 60000. Default is 5000.

Usage Guidelines

The value specified for this command must not be greater than the value specified for the `timeout` command. The threshold value configured by this command is used only to calculate network monitoring statistics created by an IP SLAs operation.

For the IP SLAs ICMP Echo operation, the `threshold` (IP SLA) command sets the upper threshold value for the round-trip time (**RTT**) measurement.

Following are the recommended guidelines for configuring the `frequency`, `timeout` and `threshold` commands of the IP SLAs ICMP Echo operation:

`(frequency` *`seconds`*`) → (timeout` *`milliseconds`*`) → (threshold` *`milliseconds`*`)`

This command is supported in IPv4 networks and also for IPv6 networks where IPv6 addresses are supported.

Example:

The following example shows how to configure the threshold of the IP SLAs ICMP echo operation to 3500. This example shows the threshold (IP SLA) command being used in an IPv4 network in ICMP echo configuration mode within IP SLA configuration mode:

```
(Routing)(config)#ip sla 11
(Routing)(config-ip-sla)#icmp-echo 152.17.10.145
(Routing)(config-ip-sla-echo)#threshold 3500
```

7.16.3.3.1 no threshold

Use this command to reset the threshold to the default value.

Format `no threshold`
Mode IP SLA ICMP ECHO Config

7.16.3.4 vrf (IP SLA)

Use this command in the ICMP echo configuration sub-mode of IP SLA configuration mode to allow reachability monitoring within Virtual Private Networks (VPNs) using IP Service Level Agreements (SLAs) operations.

Default By default, every IP SLA operation is used to monitor in the Default VRF.

Format `vrf vrf-name`

Mode IP SLA ICMP ECHO Config

Parameters	Description
vrf-name	VPN routing and forwarding (VRF) name.

Usage Guidelines

This command identifies the VPN for the operation being configured.

Use this command only if the response time over the VPN tunnel needs to be measured.

The `vrf` (IP SLA) command is supported only in IPv4 networks. This command is **not** supported in IPv6 networks to configure an IP SLAs operation that supports IPv6 addresses.

Example:

How to configure an IP SLAs operation for a VPN is shown in the following example. This example shows how test traffic can be sent in an already existing VPN tunnel between two endpoints.

```
(Routing)(config)#ip sla 11
(Routing)(config-ip-sla)#icmp-echo 35.1.10.2
(Routing)(config-ip-sla-echo)#vrf vpn1
```

7.16.3.4.1 no vrf (IP SLA)

Use this command to un-configure the VRF association previously configured.

Format `no vrf`

Mode IP SLA ICMP ECHO Config

7.16.4 Clear Commands

7.16.4.1 clear ip sla statistics

Use this command to clear IP SLA statistical information for given IP SLA operation or all IP SLAs.

Format `clear ip sla statistics [operation-number]`

Mode Privileged Exec

Parameters	Description
operation-number	IP SLA number of a specific operation whose statistics needs to be cleared.

7.16.5 Show Commands

7.16.5.1 show ip sla configuration

Use this command in user EXEC or privileged EXEC mode to see the configuration values (including all defaults) for a specified IP SLAs operation or all operations.

Format `show ip sla configuration [operation-number]`
Mode Privileged Exec

Parameters	Description
operation-number	IP SLA number of a specific operation associated with the statistics to display.

Example:

IP SLAs Internet Control Message Protocol (ICMP) echo operations support both IPv4 and IPv6 addresses. The sample outputs from the `show ip sla configuration` command for different IP SLAs operations in IPv4 and IPv6 networks are shown below.

```
(Routing)#show ip sla configuration 3

Entry number: 3
Type of operation: echo
Target address/Source address: 1.1.1.1/0.0.0.0
Operation timeout (milliseconds): 5000
Vrf Name:
Schedule:
    Next Scheduled Start Time: Start Time already passed
    Operation frequency (seconds): 60
    Life: Forever
Threshold (milliseconds): 5000
```

In the following example the output from the `show ip sla configuration` command when the specified operation is an ICMP echo operation in an IPv6 network is shown:

```
(Routing)#show ip sla configuration 5

Entry number: 3
Type of operation: echo
Target address/Source address: 2001:DB8:100::1/2001:0DB8:200::FFFE
Operation timeout (milliseconds): 5000
Vrf Name:
Schedule:
    Next Scheduled Start Time: Pending Trigger
    Operation frequency (seconds): 60
    Life: Forever
Threshold (milliseconds): 5000
```

7.16.5.2 show ip sla statistics

Use this command in user EXEC or privileged EXEC mode to see the statistics and the current operational status of a specified IP SLA operation or of all operations.

Format `show ip sla statistics [operation-number] [details]`

Mode Privileged Exec

Parameters	Description
operation-number	IP SLA operation number for which statistics and the operational status are displayed.
details	Include this option to display statistics and the operational status in greater detail.

Usage Guidelines

This command shows the current state of IP SLAs operations, including whether the operation is active and also the monitoring data returned for the last (most recently completed) operation.

Example:

```
(Routing)# show ip sla statistics details

Round Trip Time (RTT) for       Index 1
Type of operation: icmp-echo
        Latest RTT: 1 ms
Latest operation start time: 47 milliseconds
Latest operation return code: OK
Over thresholds occurred: FALSE
Number of successes: 14
Number of failures: 0
Operation time to live: Forever
Operational state of entry: Active
```

7.16.5.3 show ip route track-table

This command displays information for all tracked IPv4 static routes for a given VRF or the default the VRF.

Format `show ip route [vrf vrf-name] track-table`

Mode Privileged Exec

Parameters	Description
vrf vrf-name	Displays all tracked static routes associated with a specific VRF.

Example:

```
(Routing)#show ip route track-table

ip route 0.0.0.0 0.0.0.0 10.130.167.129 track 10 state is [up]
```

7.16.5.4 show ipv6 route track-table

This command displays information about all IPv6 static routes being tracked.

Format `show ipv6 route track-table`

Mode Privileged Exec

Example:

```
(Routing)#show ipv6 route track-table

ipv6 route 2001:B66::/32 4001::1 track 15 state is [up]
```

7.16.5.5 show track

This command is used display detailed information for all track objects or for a specific track-object. This command is also used to display brief information for all track objects or for track-objects associated with a given IP SLA operation.

Format `show track [brief | track-number | {ip sla operation-number}]`

Mode Privileged Exec

Parameters	Description
brief	Displays brief information for all track objects.
track-number	The track object's number with the detailed information to display.
ip sla operation-number>	IP SLA operation number of whose associated track-objects related brief information needs to be displayed.

Example: The following example shows detailed information for all track objects.

```
(Routing)#show track

Track 10
  IP SLA 1 reachability
  Reachability is Up
    1 change, last change 01:12:36
  Delay up 5 secs, down 5 secs
  Latest operation return code: OK
  Latest RTT (millisecs) 1500

Track 11
  IP SLA 2 state
  State is Up
    1 change, last change 00:41:55
  Delay up 10 secs, down 10 secs
  Latest operation return code: OK
  Latest RTT (millisecs) 1000

Track 13
  IP SLA 1 state
  State is Up
    1 change, last change 00:34:08
  Delay up 5 secs, down 5 secs
  Latest operation return code: OK
  Latest RTT (millisecs) 1500
```

Example: The following example shows detailed information for track object 10.

```
(Routing)#show track 10

Track 10
  IP SLA 1 reachability
```

```
  Reachability is Up
    1 change, last change 01:12:36
  Delay up 5 secs, down 5 secs
  Latest operation return code: OK
  Latest RTT (millisecs) 1500
```

Example: The following example shows brief information for all track objects associated with IP SLA operation 1.

```
(Routing)#show track ip sla 1

Track   Object                  Parameter        Value Last Change
10      ip sla      1           reachability     Up    01:12:36
13      ip sla      1           state            Up    00:34:08
```

Example: The following example shows brief information for all track objects.

```
(Routing)#show track brief

Track   Object                  Parameter        Value Last Change
10      ip sla      1           reachability     Up    01:12:36
11      ip sla      2           state            Up    00:41:55
```

13 ip sla 1 state Up 00:34:08

Chapter 8: IPv6 Routing Commands

This section describes the IPv6 routing commands available in the EFOS CLI.

8.1 Loopback Interface Commands

The commands in this section describe how to create, delete, and manage loopback interfaces. A loopback interface is always expected to be up. This interface can provide the source address for sent packets and can receive both local and remote packets. The loopback interface is typically used by routing protocols.

To assign an IP address to the loopback interface, see Section 7.2.0.3, ip address.

8.1.0.1 interface loopback

Use this command to enter the Interface Config mode for a loopback interface. The range of the loopback ID is 0 to 7.

Format `interface loopback` *`loopback-id`*
Mode Global Config

8.1.0.1.1 no interface loopback

This command removes the loopback interface and associated configuration parameters for the specified loopback interface.

Format `no interface loopback` *`loopback-id`*
Mode Global Config

8.1.0.2 show interface loopback

This command displays information about configured loopback interfaces.

Format `show interface loopback [`*`loopback-id`*`]`
Mode Privileged EXEC

If you do not specify a loopback ID, the following information appears for each loopback interface on the system:

Parameter	Definition
Loopback ID	The loopback ID associated with the rest of the information in the row.
Interface	The interface name.
IP Address	The IPv4 address of the interface.

If you specify a loopback ID, the following information appears:

Term	Definition
Interface Link Status	Shows whether the link is up or down.

Term	Definition
IP Address	The IPv4 address of the interface.
MTU size	The maximum transmission size for packets on this interface, in bytes.

8.2 Tunnel Interface Commands

The commands in this section describe how to create, delete, and manage tunnel interfaces.Several different types of tunnels provide functionality to facilitate the transition of IPv4 networks to IPv6 networks. These tunnels are divided into two classes: configured and automatic. The distinction is that configured tunnels are explicitly configured with a destination or endpoint of the tunnel. Automatic tunnels, in contrast, infer the endpoint of the tunnel from the destination address of packets routed into the tunnel. To assign an IP address to the tunnel interface, see Section 7.2.0.3, ip address. To assign an IPv6 address to the tunnel interface, see Section 8.3.0.4, ipv6 address.

8.2.0.1 interface tunnel

Use this command to enter the Interface Config mode for a tunnel interface. The *tunnel-id* range is 0 to 7.

Format `interface tunnel 0-7`
Mode Global Config

8.2.0.1.1 no interface tunnel

This command removes the tunnel interface and associated configuration parameters for the specified tunnel interface.

Format `no interface tunnel tunnel-id`
Mode Global Config

8.2.0.2 tunnel source

This command specifies the source transport address of the tunnel, either explicitly or by reference to an interface.

Format `tunnel source {ipv4-address | ethernet slot/port}`
Mode Interface Config

8.2.0.3 tunnel destination

This command specifies the destination transport address of the tunnel.

Format `tunnel destination {ipv4-address}`
Mode Interface Config

8.2.0.4 tunnel mode ipv6ip

This command specifies the mode of the tunnel. With the optional 6to4 argument, the tunnel mode is set to 6to4 automatic. Without the optional 6to4 argument, the tunnel mode is configured.

Format `tunnel mode ipv6ip [6to4]`
Mode Interface Config

8.2.0.5 show interface tunnel

This command displays the parameters related to tunnel such as tunnel mode, tunnel source address and tunnel destination address.

Format `show interface tunnel [tunnel-id]`

Mode Privileged EXEC

If you do not specify a tunnel ID, the command shows the following information for each configured tunnel:

Term	Definition
Tunnel ID	The tunnel identification number.
Interface	The name of the tunnel interface.
Tunnel Mode	The tunnel mode.
Source Address	The source transport address of the tunnel.
Destination Address	The destination transport address of the tunnel.

If you specify a tunnel ID, the command shows the following information for the tunnel:

Term	Definition
Interface Link Status	Shows whether the link is up or down.
MTU Size	The maximum transmission unit for packets on the interface.
IPv6 Address/Length	If you enable IPv6 on the interface and assign an address, the IPv6 address and prefix display.

8.3 IPv6 Routing Commands

This section describes the IPv6 commands you use to configure IPv6 on the system and on the interfaces. This section also describes IPv6 management commands and show commands.

8.3.0.1 ipv6 hop-limit

This command defines the unicast hop count used in ipv6 packets originated by the node. The value is also included in router advertisements. Valid values for *hops* are 1-255 inclusive. The default “not configured” means that a value of zero is sent in router advertisements and a value of 64 is sent in packets originated by the node. Note that this is not the same as configuring a value of 64.

Default not configured
Format `ipv6 hop-limit` *`1-255`*
Mode Global Config

8.3.0.1.1 no ipv6 hop-limit

This command returns the unicast hop count to the default.

Format `no ipv6 hop-limit`
Mode Global Config

8.3.0.2 ipv6 unicast-routing

Use this command to enable the forwarding of IPv6 unicast datagrams.

Default disabled
Format `ipv6 unicast-routing`
Mode Global Config

8.3.0.2.1 no ipv6 unicast-routing

Use this command to disable the forwarding of IPv6 unicast datagrams.

Format `no ipv6 unicast-routing`
Mode Global Config

8.3.0.3 ipv6 enable

Use this command to enable IPv6 routing on an interface or range of interfaces, including tunnel and loopback interfaces, that has not been configured with an explicit IPv6 address. When you use this command, the interface is automatically configured with a link-local address. You do not need to use this command if you configured an IPv6 global address on the interface.

Default disabled
Format `ipv6 enable`
Mode Interface Config

8.3.0.3.1 no ipv6 enable

Use this command to disable IPv6 routing on an interface.

Format	`no ipv6 enable`
Mode	Interface Config

8.3.0.4 ipv6 address

Use this command to configure an IPv6 address on an interface or range of interfaces, including tunnel and loopback interfaces, and to enable IPv6 processing on this interface. You can assign multiple globally reachable addresses to an interface by using this command. You do not need to assign a link-local address by using this command since one is automatically created. The *`prefix`* field consists of the bits of the address to be configured. The *`prefix_length`* designates how many of the high-order contiguous bits of the address make up the prefix.

You can express IPv6 addresses in eight blocks. Also of note is that instead of a period, a colon now separates each block. For simplification, leading zeros of each 16 bit block can be omitted. One sequence of 16 bit blocks containing only zeros can be replaced with a double colon "::", but not more than one at a time (otherwise it is no longer a unique representation).

- Dropping zeros: `3ffe:ffff:100:f101:0:0:0:1` becomes `3ffe:ffff:100:f101::1`
- Local host: `0000:0000:0000:0000:0000:0000:0000:0001` becomes `::1`
- Any host: `0000:0000:0000:0000:0000:0000:0000:0000` becomes `::`

The hexadecimal letters in the IPv6 addresses are not case-sensitive. An example of an IPv6 prefix and prefix length is `3ffe:1::1234/64`.

The optional `[eui-64]` field designates that IPv6 processing on the interfaces was enabled using an EUI-64 interface ID in the low order 64 bits of the address. If you use this option, the value of *`prefix_length`* must be 64 bits.

Format	`ipv6 address` *`prefix/prefix_length`* `[eui64]`
Mode	Interface Config

8.3.0.4.1 no ipv6 address

Use this command to remove all IPv6 addresses on an interface or specified IPv6 address. The *`prefix`* parameter consists of the bits of the address to be configured. The *`prefix_length`* designates how many of the high-order contiguous bits of the address comprise the prefix.The optional *`[eui-64]`* field designates that IPv6 processing on the interfaces was enabled using an EUI-64 interface ID in the low order 64 bits of the address.

If you do not supply any parameters, the command deletes all the IPv6 addresses on an interface.

Format	`no ipv6 address [`*`prefix/prefix_length`*`] [eui64]`
Mode	Interface Config

8.3.0.5 ipv6 address autoconfig

Use this command to allow an in-band interface to acquire an IPv6 address through IPv6 Neighbor Discovery Protocol (NDP) and through the use of Router Advertisement messages.

Default	disabled
Format	`ipv6 address autoconfig`
Mode	Interface Config

8.3.0.5.1 no ipv6 address autoconfig

This command the IPv6 autoconfiguration status on an interface to the default value.

Format	`no ipv6 address autoconfig`
Mode	Interface Config

8.3.0.6 ipv6 address dhcp

This command enables the DHCPv6 client on an in-band interface so that it can acquire network information, such as the IPv6 address, from a network DHCP server.

Default	disabled
Format	`ipv6 address dhcp`
Mode	Interface Config

8.3.0.6.1 no ipv6 address dhcp

This command releases a leased address and disables DHCPv6 on an interface.

Format	`no ipv6 address dhcp`
Mode	Interface Config

8.3.0.7 ipv6 route

Use this command to configure an IPv6 static route. The *`ipv6-prefix`* is the IPv6 network that is the destination of the static route. The *`prefix_length`* is the length of the IPv6 prefix — a decimal value (usually 0-64) that shows how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the *`prefix_length`*. The *`next-hop-address`* is the IPv6 address of the next hop that can be used to reach the specified network. Specifying `Null0` as nexthop parameter adds a static reject route. The *`preference`* parameter is a value the router uses to compare this route with routes from other route sources that have the same destination. The range for *`preference`* is 1–255, and the default value is 1. The argument `slot/port` corresponds to a physical routing interface or VLAN routing interface. The keyword `vlan` is used to specify the VLAN ID of the routing VLAN directly instead of a *slot/port* format. You can specify a *`slot/port`* or vlan `vlan-id` or *`tunnel tunnel_id`* interface to identify direct static routes from point-to-point and broadcast interfaces. The interface must be specified when using a link-local address as the next hop. A route with a preference of 255 cannot be used to forward traffic.

This command also enables static provisioning of MPLS tunnels based on the MPLS label(s) parameters. Up to three MPLS labels can be specified as part of this command. The unique identifier for the tunnel is the nexthop IPv4 address and the MPLS label(s). The label-1 appears first in the packet (outer label) followed by the optional labels, label-2 and label-3. The mplsd-label values are 20-bit MPLS labels. The valid range of an MPLS label is 16 to 1048575.

Use the `track object-number` to specify that the static route is installed only if the configured track object is up. When the track object is down the static route is removed from the Route Table. Use the no form of this command to delete the tracked static route. The `object-number` parameter is the object number representing the object to be tracked. The range is from 1 to 128. Only one track object can be associated with a specific static route. If you configure a different track object, the previously configured track object is replaced by the newly configured track object. To display the IPv6 static routes that being tracked by track objects, use the `show ipv6 route track-table` command.

NOTE: The nexthop IPv6 address along with MPLS-labels define the nexthop. So, you can configure a route to the same network with the same nexthop IPv6 address but with different MPLS-labels.

Default disabled

Format `ipv6 route` *`ipv6-prefix/prefix_length`* {*`next-hop-address`* | `Null0` | `interface` {*`slot/port`* | *`vlan vlan-id`* |`tunnel` *`tunnel_id`*}} *`[mplsd-label label-1] [mplsd-label label-2] [mplsd-label label-3] [preference]`* [`track` *`object-number`*]

Mode Global Config

8.3.0.7.1 no ipv6 route

Use this command to delete an IPv6 static route. Use the command without the optional parameters to delete all static routes to the specified destination. Use the *`preference`* parameter to revert the preference of a route to the default preference.

Format `no ipv6 route` *`ipv6-prefix/prefix_length`* [{*`next-hop-address`* | `Null0` | `interface` {*`slot/port`* | *`vlan vlan-id`* | `tunnel` *`tunnel_id`*} | *`preference`*}]

Mode Global Config

8.3.0.8 ipv6 route distance

This command sets the default distance (preference) for IPv6 static routes. Lower route distance values are preferred when determining the best route. The `ipv6 route` command allows you to optionally set the distance (preference) of an individual static route. The default distance is used when no distance is specified in this command.

Changing the default distance does not update the distance of existing static routes, even if they were assigned the original default distance. The new default distance will only be applied to static routes created after invoking the `ipv6 route distance` command.

Default 1

Format `ipv6 route distance` *`1-255`*

Mode Global Config

8.3.0.8.1 no ipv6 route distance

This command resets the default static route preference value in the router to the original default preference. Lower route preference values are preferred when determining the best route.

Format `no ipv6 route distance`

Mode Global Config

8.3.0.9 ipv6 route net-prototype

This command adds net prototype IPv6 routes to the hardware.

Format `ip route net-prototype` *`prefix/prefix-length nexthopip num-routes`*
Mode Global Config

Parameter	Description
prefix/prefix-length	The destination network and mask for the route.
nexthopip	The next-hop ip address, It must belong to an active routing interface, but it does not need to be resolved.
num-routes	The number of routes need to added into hardware starting from the given prefix argument and within the given prefix-length.

8.3.0.9.1 no ipv6 route net-prototype

This command deletes all the net prototype IPv6 routes added to the hardware.

Format `ip route net-prototype` *`prefix/prefix-length nexthopip num-routes`*
Mode Global Config

8.3.0.10 ipv6 route static bfd interface

This command sets up a BFD session between two directly connected neighbors specified by the local interface and the neighbor's IPv6 address. The IPv6 address can be a global or a link-local address. The BFD session parameters can be set on the interface by using the existing command

`bfd interval` *`milliseconds`* `min_rx` *`milliseconds`* `multiplier` *`interval-multiplier`*

This command is supported in IPv6 networks. The maximum number of IP static BFD sessions that can be supported is limited by the max BFD sessions configurable per DUT.

Format `ipv6 route static bfd interface` *`unit/slot/port`* `|` `vlan` *`id neighbor ip address`* `[`*`global`* `|` *`link-local`*`]`
Mode Global Config

Parameter	Description
interface	Specify the local interface either in unit/slot/port format or as a VLAN ID.
neighbor IPv6 address	Specify the other end of the BFD session, peer address.

Example:

```
(localhost) #configure
(localhost) (Config)#interface 0/29
(localhost) (Interface 0/29)#routing
(localhost) (Interface 0/29)#ipv6 address 2001::1/64
(localhost) (Interface 0/29)#bfd interval 100 min_rx 100 multiplier 5
(localhost) (Interface 0/29)#exit
```

```
(localhost) (Config)#show running-config interface 0/29

!Current Configuration:
!
interface  0/29
no shutdown
routing
ipv6 address 2001::1/64
bfd interval 100 min_rx 100 multiplier 5
exit

(localhost) (Config)#ipv6 route static bfd interface 0/29 2001::2
```

8.3.0.11 ipv6 mtu

This command sets the maximum transmission unit (MTU) size, in bytes, of IPv6 packets on an interface or range of interfaces. This command replaces the default or link MTU with a new MTU value.

NOTE: The default MTU value for a tunnel interface is 1480. You cannot change this value.

Default	0 or link speed (MTU value (1500))
Format	`ipv6 mtu` *`1280-12270`*
Mode	Interface Config

8.3.0.11.1 no ipv6 mtu

This command resets maximum transmission unit value to default value.

Format	`no ipv6 mtu`
Mode	Interface Config

8.3.0.12 ipv6 nd dad attempts

This command sets the number of duplicate address detection probes transmitted on an interface or range of interfaces. Duplicate address detection verifies that an IPv6 address on an interface is unique.

Default	1
Format	`ipv6 nd dad attempts` *`0 - 600`*
Mode	Interface Config

8.3.0.12.1 no ipv6 nd dad attempts

This command resets to number of duplicate address detection value to default value.

Format	`no ipv6 nd dad attempts`
Mode	Interface Config

8.3.0.13 ipv6 nd managed-config-flag

This command sets the “managed address configuration” flag in router advertisements on the interface or range of interfaces. When the value is true, end nodes use DHCPv6. When the value is false, end nodes automatically configure addresses.

Default false
Format `ipv6 nd managed-config-flag`
Mode Interface Config

8.3.0.13.1 no ipv6 nd managed-config-flag

This command resets the “managed address configuration” flag in router advertisements to the default value.

Format `no ipv6 nd managed-config-flag`
Mode Interface Config

8.3.0.14 ipv6 nd ns-interval

This command sets the interval between router advertisements for advertised neighbor solicitations, in milliseconds. An advertised value of 0 means the interval is unspecified. This command can configure a single interface or a range of interfaces.

Default 0
Format `ipv6 nd ns-interval {`*`1000-4294967295`* `|` *`0`*`}`
Mode Interface Config

8.3.0.14.1 no ipv6 nd ns-interval

This command resets the neighbor solicit retransmission interval of the specified interface to the default value.

Format `no ipv6 nd ns-interval`
Mode Interface Config

8.3.0.15 ipv6 nd other-config-flag

This command sets the “other stateful configuration” flag in router advertisements sent from the interface.

Default false
Format `ipv6 nd other-config-flag`
Mode Interface Config

8.3.0.15.1 no ipv6 nd other-config-flag

This command resets the “other stateful configuration” flag back to its default value in router advertisements sent from the interface.

Format `no ipv6 nd other-config-flag`

Mode Interface Config

8.3.0.16 ipv6 nd ra-interval

This command sets the transmission interval between router advertisements on the interface or range of interfaces.

Default 600
Format `ipv6 nd ra-interval-max` *4- 1800*
Mode Interface Config

8.3.0.16.1 no ipv6 nd ra-interval

This command sets router advertisement interval to the default.

Format `no ipv6 nd ra-interval-max`
Mode Interface Config

8.3.0.17 ipv6 nd raguard attach-policy

This command enables IPv6 RA Guard host mode on the configured interface. All router advertisement and router redirect packets received on this interface will be dropped by the hardware

Default Not configured
Format `ipv6 nd raguard attach-policy`
Mode Interface Config

8.3.0.17.1 no ipv6 nd raguard attach-policy

This command disables IPv6 RA Guard host mode on the interface.

Format `no ipv6 nd raguard attach-policy`
Mode Interface Config

8.3.0.18 ipv6 nd ra-lifetime

This command sets the value, in seconds, that is placed in the Router Lifetime field of the router advertisements sent from the interface or range of interfaces. The *lifetime* value must be zero, or it must be an integer between the value of the router advertisement transmission interval and 9000. A value of zero means this router is not to be used as the default router.

Default 1800
Format `ipv6 nd ra-lifetime` *lifetime*
Mode Interface Config

8.3.0.18.1 no ipv6 nd ra-lifetime

This command resets router lifetime to the default value.

Format `no ipv6 nd ra-lifetime`

Mode Interface Config

8.3.0.19 ipv6 nd ra hop-limit unspecified

This command configures the router to send Router Advertisements on an interface with an unspecified (0) Current Hop Limit value. This tells the hosts on that link to ignore the Hop Limit from this Router.

Default Disable
Format `ipv6 nd ra hop-limit unspecified`
Mode Interface Config

8.3.0.19.1 no ipv6 nd ra hop-limit unspecified

This command configures the router to send Router Advertisements on an interface with the global configured Hop Limit value.

Format `no ipv6 nd ra hop-limit unspecified`
Mode Interface Config

8.3.0.20 ipv6 nd reachable-time

This command sets the router advertisement time to consider a neighbor reachable after neighbor discovery confirmation. Reachable time is specified in milliseconds. A value of zero means the time is unspecified by the router. This command can configure a single interface or a range of interfaces.

Default 0
Format `ipv6 nd reachable-time` *`0-4294967295`*
Mode Interface Config

8.3.0.20.1 no ipv6 nd reachable-time

This command means reachable time is unspecified for the router.

Format `no ipv6 nd reachable-time`
Mode Interface Config

8.3.0.21 ipv6 nd router-preference

Use this command to configure default router preferences that the interface advertises in router advertisement messages.

Default medium
Format `ipv6 nd router-preference { low | medium | high}`
Mode Interface Config

8.3.0.21.1 no ipv6 nd router-preference

This command resets the router preference advertised by the interface to the default value.

Format `no ipv6 nd router-preference`
Mode Interface Config

8.3.0.22 ipv6 nd suppress-ra

This command suppresses router advertisement transmission on an interface or range of interfaces.

Default disabled
Format `ipv6 nd suppress-ra`
Mode Interface Config

8.3.0.22.1 no ipv6 nd suppress-ra

This command enables router transmission on an interface.

Format `no ipv6 nd suppress-ra`
Mode Interface Config

8.3.0.23 ipv6 nd prefix

Use the `ipv6 nd prefix` command to configure parameters associated with prefixes the router advertises in its router advertisements. The first optional parameter is the valid lifetime of the router, in seconds. You can specify a value or indicate that the lifetime value is infinite. The second optional parameter is the preferred lifetime of the router.

This command can be used to configure a single interface or a range of interfaces.

The router advertises its global IPv6 prefixes in its router advertisements (RAs). An RA only includes the prefixes of the IPv6 addresses configured on the interface where the RA is transmitted. Addresses are configured using the `ipv6 address` interface configuration command. Each prefix advertisement includes information about the prefix, such as its lifetime values and whether hosts should use the prefix for on-link determination or address auto-configuration. Use the `ipv6 nd prefix` command to configure these values.

The `ipv6 nd prefix` command allows you to preconfigure RA prefix values before you configure the associated interface address. In order for the prefix to be included in RAs, you must configure an address that matches the prefix using the `ipv6 address` command. Prefixes specified using `ipv6 nd prefix` without associated interface address will not be included in RAs and will not be committed to the device configuration.

Default
- valid-lifetime—2592000
- preferred-lifetime— 604800
- autoconfig—enabled
- on-link—enabled

Format `ipv6 nd prefix` *`prefix/prefix_length`* `[{`*`0-4294967295`* `| infinite} {`*`0-4294967295`* `| infinite}] [no-autoconfig off-link]`
Mode Interface Config

8.3.0.23.1 no ipv6 nd prefix

This command sets prefix configuration to default values.

Format `no ipv6 nd prefix` *`prefix/prefix_length`*
Mode Interface Config

8.3.0.24 ipv6 neighbor

Configures a static IPv6 neighbor with the given IPv6 address and MAC address on a routing or host interface.

Format `ipv6 neighbor` *`ipv6address`* `{`*`slot/port`*`|vlan` *`1-4093`*`}` *`macaddr`*
Mode Global Config

Term	Definition
ipv6address	The IPv6 address of the neighbor.
slot/port	The *`slot/port`* for the interface.
vlan	The VLAN for the interface.
macaddr	The MAC address for the neighbor.

8.3.0.24.1 no ipv6 neighbor

Removes a static IPv6 neighbor with the given IPv6 address on a routing or host interface.

Format `no ipv6 neighbor` *`ipv6address`* `{`*`slot/port`*`|vlan` *`1-4093`*`}`
Mode Global Config

8.3.0.25 ipv6 neighbors dynamicrenew

Use this command to automatically renew the IPv6 neighbor entries. Enables/disables the periodic NUD (neighbor unreachability detection) to be run on the existing IPv6 neighbor entries based on the activity of the entries in the hardware. If the setting is disabled, only those entries that are actively used in the hardware are triggered for NUD at the end of STALE timeout of 1200 seconds. If the setting is enabled, periodically every 40 seconds a set of 300 entries are triggered for NUD irrespective of their usage in the hardware.

Default `Disabled`
Format `ipv6 neighbors dynamicrenew`
Mode Global Config

8.3.0.25.1 no ipv6 neighbors dynamicrenew

Disables automatic renewing of IPv6 neighbor entries.

Format `no ipv6 neighbors dynamicrenew`
Mode Global Config

8.3.0.26 ipv6 nud

Use this command to configure Neighbor Unreachability Detection (NUD). NUD verifies that communication with a neighbor exists.

Format `ipv6 nud {backoff-multiple | max-multicast-solicits | max-unicast-solicits}`

Mode Global Config

Term	Definition
backoff-multiple	Sets the exponential backoff multiple to calculate time outs in NS transmissions during NUD. The value ranges from 1 to 5. 1 is the default. The next timeout value is limited to a maximum value of 60 seconds if the value with exponential backoff calculation is greater than 60 seconds.
max-multicast-solicits	Sets the maximum number of multicast solicits sent during Neighbor Unreachability Detection. The value ranges from 3 to 255. 3 is the default.
max-unicast-solicits	Sets the maximum number of unicast solicits sent during Neighbor Unreachability Detection. The value ranges from 3 to 10. 3 is the default.

8.3.0.27 ipv6 prefix-list

To create a prefix list or add a prefix list entry, use the `ipv6 prefix-list` command in Global Configuration mode. Prefix lists allow matching of route prefixes with those specified in the prefix list. Each prefix list includes a sequence of prefix list entries ordered by their sequence numbers. A router sequentially examines each prefix list entry to determine if the route's prefix matches that of the entry. An empty or nonexistent prefix list permits all prefixes. An implicit deny is assume if a given prefix does not match any entries of a prefix list. Once a match or deny occurs the router does not go through the rest of the list.

Up to 128 prefix lists may be configured. The maximum number of statements allowed in prefix list is 64.

Default No prefix lists are configured by default. When neither the **ge** nor the **le** option is configured, the destination prefix must match the network/length exactly. If the **ge** option is configured without the **le** option, any prefix with a network mask greater than or equal to the **ge** value is considered a match. Similarly, if the **le** option is configured without the **ge** option, a prefix with a network mask less than or equal to the **le** value is considered a match.

Format `ip prefix-list` *`list-name`* `{[seq` *`number`*`] {permit | deny}` *`ipv6-prefix/prefix-length`* `[ge` *`length`*`] [le` *`length`*`] | renumber` *`renumber-interval first-statement-number`*`}`

Mode Global Configuration

Parameter	Description
list-name	The text name of the prefix list. Up to 32 characters.
seq number	(Optional) The sequence number for this prefix list statement. Prefix list statements are ordered from lowest sequence number to highest and applied in that order. If you do not specify a sequence number, the system will automatically select a sequence number five larger than the last sequence number in the list. Two statements may not be configured with the same sequence number. The value ranges from 1 to 4,294,967,294.
permit	Permit routes whose destination prefix matches the statement.
deny	Deny routes whose destination prefix matches the statement.
ipv6-prefix/prefix-length	Specifies the match criteria for routes being compared to the prefix list statement. The ipv6-prefix can be any valid IP prefix. The length is any IPv6 prefix length from 0 to 32.
ge length	(Optional) If this option is configured, then a prefix is only considered a match if its network mask length is greater than or equal to this value. This value must be longer than the network length and less than or equal to 32.
le length	(Optional) If this option is configured, then a prefix is only considered a match if its network mask length is less than or equal to this value. This value must be longer than the **ge** length and less than or equal to 32.

Parameter	Description
renumber	(Optional) Provides the option to renumber the sequence numbers of the IP prefix list statements with a given interval starting from a particular sequence number. The valid range for *renumber-interval* is 1–100, and the valid range for *first-statement-number* is 1–1000.

8.3.0.27.1 no ipv6 prefix-list

To delete a prefix list or a statement in a prefix list, use the **no** form of this command. The command **no ip prefix-list list-name** deletes the entire prefix list. To remove an individual statement from a prefix list, you must specify the statement exactly, with all its options.

Format `no ipv6 prefix-list` *list-name* `[seq` *number*`] {permit | deny}` *network/length* `[ge` *length*`] [le` *length*`]`

Mode Global Configuration

8.3.0.28 ipv6 unreachables

Use this command to enable the generation of ICMPv6 Destination Unreachable messages on the interface or range of interfaces. By default, the generation of ICMPv6 Destination Unreachable messages is enabled.

Default enable

Format `ipv6 unreachables`

Mode Interface Config

8.3.0.28.1 no ipv6 unreachables

Use this command to prevent the generation of ICMPv6 Destination Unreachable messages.

Format `no ipv6 unreachables`

Mode Interface Config

8.3.0.29 ipv6 unresolved-traffic

Use this command to control the rate at which IPv6 data packets come into the CPU. By default, rate limiting is disabled. When enabled, the rate can range from 50 to 1024 packets per second.

Default enable

Format `ipv6 unresolved-traffic rate-limit` *50-1024*

Mode Global Config

8.3.0.29.1 no ipv6 unresolved-traffic

Use this command to disable the rate limiting.

Format `no ipv6 unresolved-traffic rate-limit`

Mode Global Config

8.3.0.30 ipv6 icmp error-interval

Use this command to limit the rate at which ICMPv6 error messages are sent. The rate limit is configured as a token bucket, with two configurable parameters, *burst-size* and *burst-interval*.

The *burst-interval* specifies how often the token bucket is initialized with *burst-size* tokens. *burst-interval* is from 0 to 2147483647 milliseconds (msec).

The *burst-size* is the number of ICMPv6 error messages that can be sent during one *burst-interval*. The range is from 1 to 200 messages.

To disable ICMP rate limiting, set *burst-interval* to zero (0).

Default
- *burst-interval* of 1000 msec.
- *burst-size* of 100 messages

Format `ipv6 icmp error-interval` *`burst-interval`* `[`*`burst-size`*`]`

Mode Global Config

8.3.0.30.1 no ipv6 icmp error-interval

Use the **no** form of the command to return *burst-interval* and *burst-size* to their default values.

Format `no ipv6 icmp error-interval`

Mode Global Config

8.3.0.31 show ipv6 brief

Use this command to display the IPv6 status of forwarding mode and IPv6 unicast routing mode.

Format `show ipv6 brief`

Mode Privileged EXEC

Term	Definition
IPv6 Forwarding Mode	Shows whether the IPv6 forwarding mode is enabled.
IPv6 Unicast Routing Mode	Shows whether the IPv6 unicast routing mode is enabled.
IPv6 Hop Limit	Shows the unicast hop count used in IPv6 packets originated by the node. For more information, see Section 8.3.0.1, ipv6 hop-limit.
ICMPv6 Rate Limit Error Interval	Shows how often the token bucket is initialized with burst-size tokens. For more information, see Section 8.3.0.30, ipv6 icmp error-interval.
ICMPv6 Rate Limit Burst Size	Shows the number of ICMPv6 error messages that can be sent during one *burst-interval.* For more information, see Section 8.3.0.30, ipv6 icmp error-interval.
Maximum Routes	Shows the maximum IPv6 route table size.
IPv6 Unresolved Data Rate Limit	Shows the rate in packets-per-second for the number of IPv6 data packets trapped to CPU when the packet fails to be forwarded in the hardware due to unresolved hardware address of the destined IPv6 node.
IPv6 Neighbors Dynamic Renew	Shows the dynamic renewal mode for the periodic NUD (neighbor unreachability detection) run on the existing IPv6 neighbor entries based on the activity of the entries in the hardware.

Term	Definition
IPv6 NUD Maximum Unicast Solicits	Shows the maximum number of unicast Neighbor Solicitations sent during NUD (neighbor unreachabililty detection) before switching to multicast Neighbor Solicitations.
IPv6 NUD Maximum Multicast Solicits	Shows the maximum number of multicast Neighbor Solicitations sent during NUD (neighbor unreachabililty detection) when in UNREACHABLE state.
IPv6 NUD Exponential Backoff Multiple	Shows the exponential backoff multiple to be used in the calculation of the next timeout value for Neighbor Solicitation transmission during NUD (neighbor unreachabililty detection) following the exponential backoff algorithm.
System uRPF Mode	Shows whether unicast Reverse Path Forwarding (uRPF) is enabled.

Example: The following shows example CLI display output for the command.

```
(Switch) #show ipv6 brief

IPv6 Unicast Routing Mode..................... Disable
IPv6 Hop Limit................................ 0
ICMPv6 Rate Limit Error Interval.............. 1000 msec
ICMPv6 Rate Limit Burst Size.................. 100 messages
Maximum Routes................................ 4096

IPv6 Unresolved Data Rate Limit............... 1024 pps
IPv6 Neighbors Dynamic Renew.................. Disable
IPv6 NUD Maximum Unicast Solicits............. 3
IPv6 NUD Maximum Multicast Solicits........... 3
IPv6 NUD Exponential Backoff Multiple......... 1
System uRPF Mode.............................. Enabled
```

8.3.0.32 show ipv6 interface

Use this command to show the usability status of IPv6 interfaces and whether ICMPv6 Destination Unreachable messages may be sent. The argument `slot/port` corresponds to a physical routing interface or VLAN routing interface. The keyword **vlan** is used to specify the VLAN ID of the routing VLAN directly instead of a *slot/port* format. The keyword **loopback** specifies the loopback interface directly. The keyword tunnel specifies the IPv6 tunnel interface.

Format `show ipv6 interface {brief | slot/port|vlan 1-4093|loopback 0-7|tunnel 0-7}`

Mode Privileged EXEC

If you use the *brief* parameter, the following information displays for all configured IPv6 interfaces:

Term	Definition
Interface	The interface in *slot/port* format.
IPv6 Operational Mode	Shows whether the mode is enabled or disabled.
IPv6 Address/Length	Shows the IPv6 address and length on interfaces with IPv6 enabled.
Method	Indicates how each IP address was assigned. The field contains one of the following values: ■ **DHCP** - The address is leased from a DHCP server. ■ **Manual** - The address is manually configured. Global addresses with no annotation are assumed to be manually configured.

If you specify an interface, the following information also appears.

Term	Definition
Routing Mode	Shows whether IPv6 routing is enabled or disabled.
IPv6 Enable Mode	Shows whether IPv6 is enabled on the interface.
Administrative Mode	Shows whether the interface administrative mode is enabled or disabled.
Bandwidth	Shows bandwidth of the interface.
Interface Maximum Transmission Unit	The MTU size, in bytes.
Router Duplicate Address Detection Transmits	The number of consecutive duplicate address detection probes to transmit.
Address Autoconfigure Mode	Shows whether the autoconfigure mode is enabled or disabled.
Address DHCP Mode	Shows whether the DHCPv6 client is enabled on the interface.
IPv6 Hop Limit Unspecified	Indicates if the router is configured on this interface to send Router Advertisements with unspecified (0) as the Current Hop Limit value.
Router Advertisement NS Interval	The interval, in milliseconds, between router advertisements for advertised neighbor solicitations.
Router Advertisement Lifetime	Shows the router lifetime value of the interface in router advertisements.
Router Advertisement Reachable Time	The amount of time, in milliseconds, to consider a neighbor reachable after neighbor discovery confirmation.
Router Advertisement Interval	The frequency, in seconds, that router advertisements are sent.
Router Advertisement Managed Config Flag	Shows whether the managed configuration flag is set (enabled) for router advertisements on this interface.
Router Advertisement Other Config Flag	Shows whether the other configuration flag is set (enabled) for router advertisements on this interface.
Router Advertisement Router Preference	Shows the router preference.
Router Advertisement Suppress Flag	Shows whether router advertisements are suppressed (enabled) or sent (disabled).
IPv6 Destination Unreachables	Shows whether ICMPv6 Destination Unreachable messages may be sent (enabled) or not (disabled). For more information, see Section 8.3.0.28, ipv6 unreachables.
ICMPv6 Redirect	Specifies if ICMPv6 redirect messages are sent back to the sender by the Router in the redirect scenario is enabled on this interface.

If an IPv6 prefix is configured on the interface, the following information also appears.

Term	Definition
IPv6 Prefix is	The IPv6 prefix for the specified interface.
Preferred Lifetime	The amount of time the advertised prefix is a preferred prefix.
Valid Lifetime	The amount of time the advertised prefix is valid.
Onlink Flag	Shows whether the onlink flag is set (enabled) in the prefix.
Autonomous Flag	Shows whether the autonomous address-configuration flag (autoconfig) is set (enabled) in the prefix.

Example: The following shows example CLI display output for the command.

```
(alpha-stack) #show ipv6 interface brief

           Oper.
Interface  Mode     IPv6 Address/Length
---------- -------- --------------------------------
0/33       Enabled  FE80::211:88FF:FE2A:3E3C/128
                    2033::211:88FF:FE2A:3E3C/64
0/17       Enabled  FE80::211:88FF:FE2A:3E3C/128
```

```
                    2017::A42A:26DB:1049:43DD/128                    [DHCP]
4/1        Enabled  FE80::211:88FF:FE2A:3E3C/128
                    2001::211:88FF:FE2A:3E3C/64                      [AUTO]
4/2        Disabled FE80::211:88FF:FE2A:3E3C/128                    [TENT]
```

Example: The following shows example CLI display output for the command.

```
(Switch) #show ipv6 interface 0/4/1

IPv6 is enabled
IPv6 Prefix is ................................ fe80::210:18ff:fe00:1105/128
                                                2001::1/64
Routing Mode................................... Enabled
IPv6 Enable Mode............................... Enabled
Administrative Mode............................ Enabled
IPv6 Operational Mode.......................... Enabled
Bandwidth...................................... 10000  kbps
Interface Maximum Transmit Unit................ 1500
Router Duplicate Address Detection Transmits... 1
Address DHCP Mode.............................. Disabled
IPv6 Hop Limit Unspecified..................... Enabled
Router Advertisement NS Interval............... 0
Router Advertisement Lifetime.................. 1800
Router Advertisement Reachable Time............ 0
Router Advertisement Interval.................. 600
Router Advertisement Managed Config Flag....... Disabled
Router Advertisement Other Config Flag......... Disabled
Router Advertisement Router Preference......... medium
Router Advertisement Suppress Flag............. Disabled
IPv6 Destination Unreachables.................. Enabled
ICMPv6 Redirects............................... Enabled


Prefix 2001::1/64
Preferred Lifetime............................. 604800
Valid Lifetime................................. 2592000
Onlink Flag.................................... Enabled
Autonomous Flag................................ Enabled
```

8.3.0.33 show ipv6 dhcp interface

This command displays a list of all IPv6 addresses currently leased from a DHCP server on a specific in-band interface. The argument `slot/port` corresponds to a physical routing interface or VLAN routing interface. The keyword `vlan` is used to specify the VLAN ID of the routing VLAN directly instead of a *slot/port* format.

Format `show ipv6 dhcp [interface` ***slot/port*** `|` ***vlan 1-4093***`]`

Modes Privileged EXEC

Term	Definition
Mode	Displays whether the specified interface is in Client mode or not.
State	State of the DHCPv6 Client on this interface.The valid values are: INACTIVE, SOLICIT, REQUEST, ACTIVE, RENEW, REBIND, RELEASE.
Server DUID	DHCPv6 Unique Identifier of the DHCPv6 Server on this interface.

(Continued)

Term	Definition
T1 Time	The T1 time specified by the DHCPv6 server. After the client has held the address for this length of time, the client tries to renew the lease.
T2 Time	The T2 time specified by the DHCPv6 server. If the lease renewal fails, then when the client has held the lease for this length of time, the client sends a Rebind message to the server.
Interface IAID	An identifier for an identity association chosen by this client.
Leased Address	The IPv6 address leased by the DHCPv6 Server for this interface.
Preferred Lifetime	The preferred lifetime of the IPv6 address, as defined in RFC 2462.
Valid Lifetime	The valid lifetime of the IPv6 address, as defined by RFC 2462.
Renew Time	The time until the client tries to renew the lease
Expiry Time	The time until the address expires.

8.3.0.34 show ipv6 nd raguard policy

This command shows the status of IPv6 RA GUARD feature on the switch. It lists the ports/interfaces on which this feature is enabled and the associated device role.

Format `show ipv6 nd raguard policy`

Mode Privileged EXEC

Term	Definition
Interface	The port/interface on which this feature is enabled.
Role	The associated device role for the interface.

Example:

```
(Switching) # show ipv6 nd raguard policy

          Configured Interfaces

          Interface        Role
          ---------------  -------
            0/1          Host
```

8.3.0.35 show ipv6 neighbors

Use this command to display information about the IPv6 neighbors.

Format `show ipv6 neighbor [interface {`*`slot/port`* `| tunnel` *`0-7`* `| vlan` *`1-4093`*`}]`

Mode Privileged EXEC

Term	Definition
Interface	The interface in *slot/port* format.
IPv6 Address	IPV6 address of neighbor or interface.
MAC Address	Link-layer Address.

Term	Definition
IsRtr	Shows whether the neighbor is a router. If the value is TRUE, the neighbor is known to be a router, and FALSE otherwise. A value of FALSE might mean that routers are not always *known* to be routers.
Neighbor State	State of neighbor cache entry. Possible values are Incomplete, Reachable, Stale, Delay, Probe, and Unknown.
Last Updated	The time in seconds that has elapsed since an entry was added to the cache.
Type	The type of neighbor entry. The type is Static if the entry is manually configured and Dynamic if dynamically resolved.

8.3.0.36 clear ipv6 neighbors

Use this command to clear all entries IPv6 neighbor table or an entry on a specific interface. Use the *slot/port* parameter to specify an interface, the *ipv6address* parameter to specify an IPV6 address, or the vlan parameter to specify a VLAN.

Format `clear ipv6 neighbors [{slot/port | ipv6address | vlan id}]`

Mode Privileged EXEC

8.3.0.37 show ipv6 protocols

This command lists a summary of the configuration and status for the active IPv6 routing protocols. The command lists routing protocols that are configured and enabled. If a protocol is selected on the command line, the display is limited to that protocol.

Format `show ipv6 protocols [bgp|ospf]`

Mode Privileged EXEC

Parameter	Description
BGP Section:	
Routing Protocol	BGP.
Router ID	The router ID configured for BGP.
Local AS Number	The AS number that the local router is in.
BGP Admin Mode	Whether BGP is globally enabled or disabled.
Maximum Paths	The maximum number of next hops in an internal or external BGP route.
Always Compare MED	Whether BGP is configured to compare the MEDs for routes received from peers in different ASs.
Maximum AS Path Length	Limit on the length of AS paths that BGP accepts from its neighbors.
Fast Internal Failover	Whether BGP immediately brings down a iBGP adjacency if the routing table manager reports that the peer address is no longer reachable.
Fast External Failover	Whether BGP immediately brings down an eBGP adjacency if the link to the neighbor goes down.
Distance	The default administrative distance (or route preference) for external, internal, and locally-originated BGP routes. The table that follows lists ranges of neighbor addresses that have been configured to override the default distance with a neighbor-specific distance. If a neighbor's address falls within one of these ranges, routes from that neighbor are assigned the configured distance. If a prefix list is configured, then the distance is only assigned to prefixes from the neighbor that are permitted by the prefix list.

Parameter	Description
Redistribution	A table showing information for each source protocol (connected, static, rip, and ospf). For each of these sources the distribution list and route-map are shown, as well as the configured metric. Fields which are not configured are left blank. For ospf, an additional line shows the configured ospf match parameters.
Prefix List In	The global prefix list used to filter inbound routes from all neighbors.
Prefix List Out	The global prefix list used to filter outbound routes to all neighbors.
Networks Originated	The set of networks originated through a network command. Those networks that are actually advertised to neighbors are marked “active.”
Neighbors	A list of configured neighbors and the inbound and outbound policies configured for each.
OSPFv3 Section:	
Routing Protocol	OSPFv3.
Router ID	The router ID configured for OSPFv3.
OSPF Admin Mode	Whether OSPF is enabled or disabled globally.
Maximum Paths	The maximum number of next hops in an OSPF route.
Default Route Advertise	Whether OSPF is configured to originate a default route.
Always	Whether default advertisement depends on having a default route in the common routing table.
Metric	The metric configured to be advertised with the default route.
Metric Type	The metric type for the default route.

Example: The following shows example CLI display output for the command.

```
(Router) #show ipv6 protocols

Routing Protocol ............................... BGP
BGP Router ID .................................. 1.1.1.1
Local AS Number ................................ 1
BGP Admin Mode ................................. Enable
Maximum Paths .................................. Internal 1, External 1
Always compare MED ............................. FALSE
Maximum AS Path Length ......................... 75
Fast Internal Failover ......................... Enable
Fast External Failover ......................... Enable
Distance ....................................... Ext 20, Int 200, Local 200

Prefixes Originated:
   2005::/64 (active)
   3012::/48

Neighbors:
172.20.1.100
   Filter List In............................ 1
   Filter List Out........................... 2
   Prefix List In............................ PfxList2
   Prefix List Out........................... PfxList3
   Route Map In.............................. rmapUp
   Route Map Out............................. rmapDown


Routing Protocol ............................... OSPFv3
Router ID ...................................... 1.1.1.1
OSPF Admin Mode ................................ Enable
Maximum Paths .................................. 4
```

```
Distance ..................................... Intra 110 Inter 110 Ext 110

Default Route Advertise ...................... Disabled
Always ....................................... FALSE
Metric ....................................... Not configured
Metric Type .................................. External Type 2

Number of Active Areas ....................... 0 (0 normal, 0 stub, 0 nssa)
ABR Status ................................... Disable
ASBR Status .................................. Disable
```

8.3.0.38 show ipv6 route

This command displays the IPv6 routing table The *ipv6-address* specifies a specific IPv6 address for which the best-matching route would be displayed. The *ipv6-prefix/ipv6-prefix-length* specifies a specific IPv6 network for which the matching route would be displayed. The *interface* specifies that the routes with next-hops on the *interface* be displayed. The argument `slot/port` corresponds to a physical routing interface or VLAN routing interface. The keyword `vlan` is used to specify the VLAN ID of the routing VLAN directly instead of a *slot/port* format. The *protocol* specifies the protocol that installed the routes. The *protocol* is one of the following keywords: *connected*, *ospf*, *static*. The *all* specifies that all routes including best and non-best routes are displayed. Otherwise, only the best routes are displayed.

NOTE: If you use the *connected* keyword for *protocol*, the *all* option is not available because there are no best or non-best connected routes.

Format `show ipv6 route [{`*ipv6-address* `[`*protocol*`] | {{`*ipv6-prefix/ipv6-prefix-length* `|` *slot/port* `|` *vlan 1-4093*`} [`*protocol*`] |` *protocol* `| summary} [all] | all}]`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Route Codes	The key for the routing protocol codes that might appear in the routing table output.

The `show ipv6 route` command displays the routing tables in the following format:

```
Codes: C - connected, S - static
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2
       ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2, Truncated, K - kernel
```

The columns for the routing table display the following information:

Term	Definition
Code	The code for the routing protocol that created this routing entry.
Default Gateway	The IPv6 address of the default gateway. When the system does not have a more specific route to a packet's destination, it sends the packet to the default gateway.
IPv6-Prefix/IPv6-Prefix-Length	The IPv6-Prefix and prefix-length of the destination IPv6 network corresponding to this route.
Preference/Metric	The administrative distance (preference) and cost (metric) associated with this route. An example of this output is [1/0], where 1 is the preference and 0 is the metric.
Tag	The decimal value of the tag associated with a redistributed route, if it is not 0.
Next-Hop	The outgoing router IPv6 address to use when forwarding traffic to the next router (if any) in the path toward the destination.

Term	Definition
Route-Timestamp	The last updated time for dynamic routes. The format of Route-Timestamp will be ■ Days:Hours:Minutes if days > = 1 ■ Hours:Minutes:Seconds if days < 1
Interface	The outgoing router interface to use when forwarding traffic to the next destination. For reject routes, the next hop interface would be `Null0` interface.
T	A flag appended to an IPv6 route to indicate that it is an ECMP route, but only one of its next hops has been installed in the forwarding table. The forwarding table may limit the number of ECMP routes or the number of ECMP groups. When an ECMP route cannot be installed because such a limit is reached, the route is installed with a single next hop. Such truncated routes are identified by a **T** after the interface name.

To administratively control the traffic destined to a particular network and prevent it from being forwarded through the router, you can configure a static reject route on the router. Such traffic would be discarded and the ICMP destination unreachable message is sent back to the source. This is typically used for preventing routing loops. The reject route added in the RTO is of the type **OSPF Inter-Area**. Reject routes (routes of REJECT type installed by any protocol) are not redistributed by OSPF. Reject routes are supported in both OSPFv2 and OSPFv3.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ipv6 route

IPv6 Routing Table - 3 entries

Codes: C - connected, S - static
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2
       ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2, P - Net Prototype

S    2001::/64 [10/0] directly connected,   Null0
C    2003::/64 [0/0]
      via ::,   0/11
S    2005::/64 [1/0]
      via 2003::2,   0/11, MPLS Labels: {123 456
C 5001::/64 [0/0]
    via ::,   0/5
OE1 6001::/64 [110/1]
    via fe80::200:42ff:fe7d:2f19,   00h:00m:23s,  0/5
OI 7000::/64 [110/6]
    via fe80::200:4fff:fe35:c8bb,   00h:01m:47s,  0/11
```

Example: The following shows example CLI display output for the command to indicate a truncated route.

```
(router) #show ipv6 route

IPv6 Routing Table - 2 entries

Codes: C - connected, S - static, 6To4 - 6to4 Route
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2
       ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2, P - Net Prototype

C    2001:db9:1::/64 [0/0]
      via ::,   0/1
OI   3000::/64 [110/1]
      via fe80::200:e7ff:fe2e:ec3f,   00h:00m:11s,  0/1   T
```

Example: The following shows example CLI display output for the command to indicate kernel routes with code K.

```
(router) #show ipv6 route

IPv6 Routing Table - 4 entries
```

```
Codes: C - connected, S - static, 6To4 - 6to4 Route, B - BGP Derived
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2
       ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2, K - kernel, P - Net Prototype

C    2009:1::/64 [0/0]
      via ::,   0/11
C    2044:1::/64 [0/0]
      via ::,   0/18
K    3001:33:3::/64 [1/0]
      via 2009:1::12,   00h:00m:25s,  0/11
K    5001:55:5::/64 [1/0]
      via 2044:1::14,   00h:00m:35s,  0/18
```

Example: The following is an example of the CLI display output with a hardware failure.

```
(router) #
(router) #configure
(router) (Config)#interface 0/1
(router) (Interface 0/1)#routing
(router) (Interface 0/1)#ipv6 enable
(router) (Interface 0/1)#ipv6 address 2001::2/64
(router) (Interface 0/1)#exit
(router) (Config)#ipv6 route net-prototype 3001::/64 2001::4 1

(router) #show ipv6 route

IPv6 Routing Table - 1 entries

Codes: C - connected, S - static, 6To4 - 6to4 Route, B - BGP Derived
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2
       ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2, K - kernel
   P - Net Prototype

C    2001::/128 [0/0]
      via ::,   0/1
P    3001::/64 [0/1]
      via 2001::4,   00h:00m:04s,  0/1  hw-failure
```

8.3.0.39 show ipv6 route ecmp-groups

This command reports all current ECMP groups in the IPv6 routing table. An ECMP group is a set of two or more next hops used in one or more routes. The groups are numbered arbitrarily from 1 to n. The output indicates the number of next hops in the group and the number of routes that use the set of next hops. The output lists the IPv6 address and outgoing interface of each next hop in each group.

Format	`show ipv6 route ecmp-groups`
Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(router) #show ipv6 route ecmp-groups

ECMP Group 1 with 2 next hops (used by 1 route)
        2001:DB8:1::1 on interface 2/1
  2001:DB8:2::14 on interface 2/2

ECMP Group 2 with 3 next hops (used by 1 route)
```

```
  2001:DB8:4::15 on interface 2/32
  2001:DB8:7::12 on interface 2/33
  2001:DB8:9::45 on interface 2/34
```

8.3.0.40 show ipv6 route hw-failure

Use this command to display the routes that failed to be added to the hardware due to hash errors or a table full condition.

Format `show ipv6 route hw-failure`

Mode Privileged EXEC

Example: The following example displays the command output.

```
(Routing) #show ipv6 route connected

IPv6 Routing Table - 2 entries

Codes: C - connected, S - static, 6To4 - 6to4 Route, B - BGP Derived
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2
       ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2, K - kernel
P - Net Prototype

C    2001::/128 [0/0]
      via ::,   0/1
C    2005::/128 [0/0]
      via ::,   0/2

(Routing) #show ipv6 route hw-failure

IPv6 Routing Table - 4 entries

Codes: C - connected, S - static, 6To4 - 6to4 Route, B - BGP Derived
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2
       ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2, K - kernel
P - Net Prototype

P    3001::/64 [0/1]
      via 2001::4,   00h:00m:04s,  0/1  hw-failure
P    3001:0:0:1::/64 [0/1]
      via 2001::4,   00h:00m:04s,  0/1  hw-failure
P    3001:0:0:2::/64 [0/1]
      via 2001::4,   00h:00m:04s,  0/1  hw-failure
P    3001:0:0:3::/64 [0/1]
      via 2001::4,   00h:00m:04s,  0/1  hw-failure
```

8.3.0.41 show ipv6 route net-prototype

This command displays the net-prototype routes. The net-prototype routes are displayed with a P.

Format `show ipv6 route net-prototype`

Modes Privileged EXEC

Example:

```
(Routing) #show ipv6 route net-prototype
IPv6 Routing Table - 2 entries
```

```
Codes: C - connected, S - static, 6To4 - 6to4 Route, B - BGP Derived
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2
       ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2, K - kernel
       P - Net Prototype

P    3001::/64 [0/1]
      via 2001::4,   00h:00m:04s,  0/1
P    3001:0:0:1::/64 [0/1]
      via 2001::4,   00h:00m:04s,  0/1
```

8.3.0.42 show ipv6 route preferences

Use this command to show the preference value associated with the type of route. Lower numbers have a greater preference. A route with a preference of 255 cannot be used to forward traffic.

Format `show ipv6 route preferences`

Mode Privileged EXEC

Term	Definition
Local	Preference of directly-connected routes.
Static	Preference of static routes.
OSPF Intra	Preference of routes within the OSPF area.
OSPF Inter	Preference of routes to other OSPF routes that are outside of the area.
OSPF External	Preference of OSPF external routes.
BGP External	Preference of BGP external routes.
BGP Internal	Preference of routes to other BGP routes that are outside of the area.
BGP Local	Preference of routes within the BGP area.

Example:

```
(lb6m) #show ipv6 route preferences

Local.......................................... 0
Static......................................... 1
OSPF Intra..................................... 110
OSPF Inter..................................... 110
OSPF External.................................. 110
BGP External................................... 20
BGP Internal................................... 200
BGP Local...................................... 200
```

8.3.0.43 show ipv6 route static bfd

This command displays information about the IPv6 static BFD configured parameters configured with the `ipv6 route static bfd` command.

Format `show ipv6 route static bfd`

Modes Privileged EXEC

Example:

```
(localhost) (Config)#show ipv6 route static bfd

S          1001::2     via    0/28            Up
S          3001::2     via     4/1            Up
```

8.3.0.44 show ipv6 route summary

This command displays a summary of the state of the routing table. When the optional `all` keyword is given, some statistics, such as the number of routes from each source, include counts for alternate routes. An alternate route is a route that is not the most preferred route to its destination and therefore is not installed in the forwarding table. To include only the number of best routes, do not use the optional keyword.

Format `show ipv6 route summary [all]`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Connected Routes	Total number of connected routes in the routing table.
Static Routes	Total number of static routes in the routing table.
BGP Routes	Total number of routes installed by the BGP protocol.
External	The number of external BGP routes.
Internal	The number of internal BGP routes.
Local	The number of local BGP routes.
OSPF Routes	Total number of routes installed by OSPFv3 protocol.
Reject Routes	Total number of reject routes installed by all protocols.
Net Prototype Routes	The total number of net-prototype routes.
Number of Prefixes	Summarizes the number of routes with prefixes of different lengths.
Total Routes	The total number of routes in the routing table.
Best Routes	The number of best routes currently in the routing table. This number only counts the best route to each destination.
Alternate Routes	The number of alternate routes currently in the routing table. An alternate route is a route that was not selected as the best route to its destination.
Route Adds	The number of routes that have been added to the routing table.
Route Modifies	The number of routes that have been changed after they were initially added to the routing table.
Route Deletes	The number of routes that have been deleted from the routing table.
Unresolved Route Adds	The number of route adds that failed because none of the route's next hops were on a local subnet. Note that static routes can fail to be added to the routing table at startup because the routing interfaces are not yet up. This counter gets incremented in this case. The static routes are added to the routing table when the routing interfaces come up.
Invalid Route Adds	The number of routes that failed to be added to the routing table because the route was invalid. A log message is written for each of these failures.
Failed Route Adds	The number of routes that failed to be added to the routing table because of a resource limitation in the routing table.
Hardware Failed Route Adds	The number of routes that failed to be inserted into the hardware due to a hash error or a table full condition.
Reserved Locals	The number of routing table entries reserved for a local subnet on a routing interface that is down. Space for local routes is always reserved so that local routes can be installed when a routing interface bounces.

Term	Definition
Unique Next Hops	The number of distinct next hops used among all routes currently in the routing table. These include local interfaces for local routes and neighbors for indirect routes.
Unique Next Hops High Water	The highest count of unique next hops since counters were last cleared.
Next Hop Groups	The current number of next hop groups in use by one or more routes. Each next hop group includes one or more next hops.
Next Hop Groups High Water	The highest count of next hop groups since counters were last cleared.
ECMP Groups	The number of next hop groups with multiple next hops.
ECMP Routes	The number of routes with multiple next hops currently in the routing table.
Truncated ECMP Routes	The number of ECMP routes that are currently installed in the forwarding table with just one next hop. The forwarding table may limit the number of ECMP routes or the number of ECMP groups. When an ECMP route cannot be installed because such a limit is reached, the route is installed with a single next hop.
ECMP Retries	The number of ECMP routes that have been installed in the forwarding table after initially being installed with a single next hop.
Routes with n Next Hops	The current number of routes with each number of next hops.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ipv6 route summary

Connected Routes.............................. 4
Static Routes................................. 0
6To4 Routes................................... 0
BGP Routes.................................... 10
  External.................................... 0
  Internal.................................... 10
  Local....................................... 0
OSPF Routes................................... 13
  Intra Area Routes........................... 0
  Inter Area Routes........................... 13
  External Type-1 Routes...................... 0
  External Type-2 Routes...................... 0
Reject Routes................................. 0
Net Prototype Routes.......................... 10004
Total routes.................................. 17

Best Routes (High)............................ 17 (17)
Alternate Routes.............................. 0
Route Adds.................................... 44
Route Deletes................................. 27
Unresolved Route Adds......................... 0
Invalid Route Adds............................ 0
Failed Route Adds............................. 0
Hardware Failed Route Adds.................... 4
Reserved Locals............................... 0

Unique Next Hops (High)....................... 8 (8)
Next Hop Groups (High)........................ 8 (8)
ECMP Groups (High)............................ 3 (3)
ECMP Routes................................... 12
Truncated ECMP Routes......................... 0
ECMP Retries.................................. 0
Routes with 1 Next Hop........................ 5
Routes with 2 Next Hops....................... 1
```

```
Routes with 3 Next Hops..................... 1
Routes with 4 Next Hops..................... 10
Number of Prefixes:
    /64: 17
```

8.3.0.45 clear ipv6 route counters

The command resets to zero the IPv6 routing table counters reported in the command Section 8.3.0.44, show ipv6 route summary. The command only resets event counters. Counters that report the current state of the routing table, such as the number of routes of each type, are not reset.

Format `clear ipv6 route counters`

Mode Privileged EXEC

8.3.0.46 show ipv6 snooping counters

This command displays the counters associated with IPv6 RA GUARD feature. The number of router advertisement and router redirect packets dropped by the switch globally due to RA GUARD feature are displayed in the command output.

Format `show ipv6 snooping counters`

Modes
- Privileged EXEC
- Global Config

Example:

```
(Switching) #  show ipv6 snooping counters

IPv6 Dropped Messages

RA(Router Advertisement - ICMP type 134)

REDIR(Router Redirect - ICMP type 137)

RA             Redir
-------        -------
0               0
```

8.3.0.47 show ipv6 vlan

This command displays IPv6 VLAN routing interface addresses.

Format `show ipv6 vlan`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
MAC Address used by Routing VLANs	Shows the MAC address.

The rest of the output for this command is displayed in a table with the following column headings:

Column Headings	Definition
VLAN ID	The VLAN ID of a configured VLAN.
Logical Interface	The interface in *slot/port* format that is associated with the VLAN ID.
IPv6 Address/Prefix Length	The IPv6 prefix and prefix length associated with the VLAN ID.

8.3.0.48 show ipv6 traffic

Use this command to show traffic and statistics for IPv6 and ICMPv6. Specify a logical, loopback, or tunnel interface to view information about traffic on a specific interface. The argument `slot/port` corresponds to a physical routing interface or VLAN routing interface. The keyword `vlan` is used to specify the VLAN ID of the routing VLAN directly instead of a *slot/port* format. If you do not specify an interface, the command displays information about traffic on all interfaces.

Format `show ipv6 traffic [{slot/port|vlan 1-4093| loopback loopback-id | tunnel tunnel-id}]`

Mode Privileged EXEC

Term	Definition
Total Datagrams Received	Total number of input datagrams received by the interface, including those received in error.
Received Datagrams Locally Delivered	Total number of datagrams successfully delivered to IPv6 user-protocols (including ICMP). This counter increments at the interface to which these datagrams were addressed, which might not necessarily be the input interface for some of the datagrams.
Received Datagrams Discarded Due To Header Errors	Number of input datagrams discarded due to errors in their IPv6 headers, including version number mismatch, other format errors, hop count exceeded, errors discovered in processing their IPv6 options, etc.
Received Datagrams Discarded Due To MTU	Number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.
Received Datagrams Discarded Due To No Route	Number of input datagrams discarded because no route could be found to transmit them to their destination.
Received Datagrams With Unknown Protocol	Number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. This counter increments at the interface to which these datagrams were addressed, which might not be necessarily the input interface for some of the datagrams.
Received Datagrams Discarded Due To Invalid Address	Number of input datagrams discarded because the IPv6 address in their IPv6 header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, `::0`) and unsupported addresses (for example, addresses with unallocated prefixes). Forentities which are not IPv6 routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
Received Datagrams Discarded Due To Truncated Data	Number of input datagrams discarded because datagram frame didn't carry enough data.
Received Datagrams Discarded Other	Number of input IPv6 datagrams for which no problems were encountered to prevent their continue processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include datagrams discarded while awaiting reassembly.
Received Datagrams Reassembly Required	Number of IPv6 fragments received which needed to be reassembled at this interface. Note that this counter increments at the interface to which these fragments were addressed, which might not be necessarily the input interface for some of the fragments.
Datagrams Successfully Reassembled	Number of IPv6 datagrams successfully reassembled. Note that this counter increments at the interface to which these datagrams were addressed, which might not be necessarily the input interface for some of the fragments.

Term	Definition
Datagrams Failed To Reassemble	Number of failures detected by the IPv6 reassembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IPv6 fragments since some algorithms (notably the algorithm in by combining them as they are received. This counter increments at the interface to which these fragments were addressed, which might not be necessarily the input interface for some of the fragments.
Datagrams Forwarded	Number of output datagrams which this entity received and forwarded to their final destinations. In entities which do not act as IPv6 routers, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route processing was successful. Note that for a successfully forwarded datagram the counter of the outgoing interface increments.
Datagrams Locally Transmitted	Total number of IPv6 datagrams which local IPv6 user-protocols (including ICMP) supplied to IPv6 in requests for transmission. Note that this counter does not include any datagrams counted in ipv6IfStatsOutForwDatagrams.
Datagrams Transmit Failed	Number of output IPv6 datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipv6IfStatsOutForwDatagrams if any such packets met this (discretionary) discard criterion.
Fragments Created	Number of output datagram fragments that have been generated as a result of fragmentation at this output interface.
Datagrams Successfully Fragmented	Number of IPv6 datagrams that have been successfully fragmented at this output interface.
Datagrams Failed To Fragment	Number of IPv6 datagrams that have been discarded because they needed to be fragmented at this output interface but could not be.
Multicast Datagrams Received	Number of multicast packets received by the interface.
Multicast Datagrams Transmitted	Number of multicast packets transmitted by the interface.
Total ICMPv6 messages received	Total number of ICMP messages received by the interface which includes all those counted by ipv6IfIcmpInErrors. Note that this interface is the interface to which the ICMP messages were addressed which may not be necessarily the input interface for the messages.
ICMPv6 Messages with errors	Number of ICMP messages which the interface received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
ICMPv6 Destination Unreachable Messages	Number of ICMP Destination Unreachable messages received by the interface.
ICMPv6 Messages Prohibited Administratively	Number of ICMP destination unreachable/communication administratively prohibited messages received by the interface.
ICMPv6 Time Exceeded Messages	Number of ICMP Time Exceeded messages received by the interface.
ICMPv6 Parameter Problem Messages	Number of ICMP Parameter Problem messages received by the interface.
ICMPv6 messages with too big packets	Number of ICMP Packet Too Big messages received by the interface.
ICMPv6 Echo Request Messages Received	Number of ICMP Echo (request) messages received by the interface.
ICMPv6 Echo Reply Messages Received	Number of ICMP Echo Reply messages received by the interface.
ICMPv6 Router Solicit Messages Received	Number of ICMP Router Solicit messages received by the interface.
ICMPv6 Router Advertisement Messages Received	Number of ICMP Router Advertisement messages received by the interface.
ICMPv6 Neighbor Solicit Messages Received	Number of ICMP Neighbor Solicit messages received by the interface.
ICMPv6 Neighbor Advertisement Messages Received	Number of ICMP Neighbor Advertisement messages received by the interface.
ICMPv6 Redirect Messages Received	Number of Redirect messages received by the interface.

Term	Definition
Transmitted	Number of ICMPv6 Group Membership Query messages received by the interface.
Total ICMPv6 Messages Transmitted	Total number of ICMP messages which this interface attempted to send. Note that this counter includes all those counted by icmpOutErrors.
ICMPv6 Messages Not Transmitted Due To Error	Number of ICMP messages which this interface did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IPv6 to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.
ICMPv6 Destination Unreachable Messages Transmitted	Number of ICMP Destination Unreachable messages sent by the interface.
ICMPv6 Messages Prohibited Administratively Transmitted	Number of ICMP destination unreachable/communication administratively prohibited messages sent.
ICMPv6 Time Exceeded Messages Transmitted	Number of ICMP Time Exceeded messages sent by the interface.
ICMPv6 Parameter Problem Messages Transmitted	Number of ICMP Parameter Problem messages sent by the interface.
ICMPv6 Packet Too Big Messages Transmitted	Number of ICMP Packet Too Big messages sent by the interface.
ICMPv6 Echo Request Messages Transmitted	Number of ICMP Echo (request) messages sent by the interface.ICMP echo messages sent.
ICMPv6 Echo Reply Messages Transmitted	Number of ICMP Echo Reply messages sent by the interface.
ICMPv6 Router Solicit Messages Transmitted	Number of ICMP Router Solicitation messages sent by the interface.
ICMPv6 Router Advertisement Messages Transmitted	Number of ICMP Router Advertisement messages sent by the interface.
ICMPv6 Neighbor Solicit Messages Transmitted	Number of ICMP Neighbor Solicitation messages sent by the interface.
ICMPv6 Neighbor Advertisement Messages Transmitted	Number of ICMP Neighbor Advertisement messages sent by the interface.
ICMPv6 Redirect Messages Received	Number of Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
ICMPv6 Group Membership Query Messages Received	Number of ICMPv6 Group Membership Query messages sent.
ICMPv6 Group Membership Response Messages Received	Number of ICMPv6 Group Membership Response messages sent.
ICMPv6 Group Membership Reduction Messages Received	Number of ICMPv6 Group Membership Reduction messages sent.
ICMPv6 Duplicate Address Detects	Number of duplicate addresses detected by the interface.

8.3.0.49 clear ipv6 snooping counters

This command clears the counters associated with IPv6 RA GUARD feature.

Format `clear ipv6 snooping counters`

Mode
- Privileged EXEC
- Global Config

8.3.0.50 clear ipv6 statistics

Use this command to clear IPv6 statistics for all interfaces or for a specific interface, including loopback, tunnel, and VLAN interfaces. IPv6 statistics display in the output of the `show ipv6 traffic` command. If you do not specify an interface, the counters for all IPv6 traffic statistics reset to zero.

Format `clear ipv6 statistics [{`*`slot/port`* `| loopback` *`loopback-id`* `| tunnel` *`tunnel-id`* `| vlan` *`id`*`}]`

Mode Privileged EXEC

8.4 OSPFv3 Commands

This section describes the commands you use to configure OSPFv3, which is a link-state routing protocol that you use to route traffic within a network.

8.4.1 Global OSPFv3 Commands

8.4.1.1 ipv6 router ospf

Use this command to enter Router OSPFv3 Config mode.

Format `router ospf`
Mode Global Config

8.4.1.2 area default-cost (OSPFv3)

This command configures the monetary default cost for the stub area. The operator must specify the area id and an integer value between 1–16777215.

Format `area` ***`areaid`*** `default-cost` ***`1-16777215`***
Mode Router OSPFv3 Config

8.4.1.3 area nssa (OSPFv3)

This command configures the specified areaid to function as an NSSA.

Format `area` ***`areaid`*** `nssa`
Mode Router OSPFv3 Config

8.4.1.3.1 no area nssa

This command disables nssa from the specified area id.

Format `no area` ***`areaid`*** `nssa`
Mode Router OSPFv3 Config

8.4.1.4 area nssa default-info-originate (OSPFv3)

This command configures the metric value and type for the default route advertised into the NSSA. The optional metric parameter specifies the metric of the default route and is to be in a range of 1-16777214. If no metric is specified, the default value is 10. The metric type can be comparable (nssa-external 1) or non-comparable (nssa-external 2).

Format `area` ***`areaid`*** `nssa default-info-originate [`***`metric`***`] [{comparable | non-comparable}]`
Mode Router OSPFv3 Config

8.4.1.4.1 no area nssa default-info-originate (OSPFv3)

This command disables the default route advertised into the NSSA.

Format `no area areaid nssa default-info-originate [metric] [{comparable | non-comparable}]`
Mode Router OSPFv3 Config

8.4.1.5 area nssa no-redistribute (OSPFv3)

This command configures the NSSA ABR so that learned external routes will not be redistributed to the NSSA.

Format `area areaid nssa no-redistribute`
Mode Router OSPFv3 Config

8.4.1.5.1 no area nssa no-redistribute (OSPFv3)

This command disables the NSSA ABR so that learned external routes are redistributed to the NSSA.

Format `no area areaid nssa no-redistribute`
Mode Router OSPFv3 Config

8.4.1.6 area nssa no-summary (OSPFv3)

This command configures the NSSA so that summary LSAs are not advertised into the NSSA.

Format `area areaid nssa no-summary`
Mode Router OSPFv3 Config

8.4.1.6.1 no area nssa no-summary (OSPFv3)

This command disables nssa from the summary LSAs.

Format `no area areaid nssa no-summary`
Mode Router OSPFv3 Config

8.4.1.7 area nssa translator-role (OSPFv3)

This command configures the translator role of the NSSA. A value of *always* causes the router to assume the role of the translator the instant it becomes a border router and a value of *candidate* causes the router to participate in the translator election process when it attains border router status.

Format `area areaid nssa translator-role {always | candidate}`
Mode Router OSPFv3 Config

8.4.1.7.1 no area nssa translator-role (OSPFv3)

This command disables the nssa translator role from the specified area id.

Format `no area areaid nssa translator-role {always | candidate}`
Mode Router OSPFv3 Config

8.4.1.8 area nssa translator-stab-intv (OSPFv3)

This command configures the translator *stabilityinterval* of the NSSA. The *stabilityinterval* is the period of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router.

Format `area areaid nssa translator-stab-intv stabilityinterval`

Mode Router OSPFv3 Config

8.4.1.8.1 no area nssa translator-stab-intv (OSPFv3)

This command disables the nssa translator's *stabilityinterval* from the specified area id.

Format `no area areaid nssa translator-stab-intv stabilityinterval`

Mode Router OSPFv3 Config

8.4.1.9 area range (OSPFv3)

Use this command to configure a summary prefix that an area border router advertises for a specific area.

Default `No area ranges are configured by default. No cost is configured by default.`

Format `area area-id range prefix netmask {summarylink | nssaexternallink} [advertise | not-advertise] [cost cost]`

Mode Router OSPFv3 Config

Parameter	Description
area-id	The area identifier for the area whose networks are to be summarized.
prefix netmask	The summary prefix to be advertised when the ABR computes a route to one or more networks within this prefix in this area.
summarylink	When this keyword is given, the area range is used when summarizing prefixes advertised in type 3 summary LSAs.
nssaexternallink	When this keyword is given, the area range is used when translating type 7 LSAs to type 5 LSAs.
advertise	[Optional] When this keyword is given, the summary prefix is advertised when the area range is active. This is the default.
not-advertise	[Optional] When this keyword is given, neither the summary prefix nor the contained prefixes are advertised when the area range is active. When the not-advertise option is given, any static cost previously configured is removed from the system configuration.
cost	[Optional] If an optional cost is given, OSPF sets the metric field in the inter-area -prefix LSA to the configured value rather than setting the metric to the largest cost among the networks covered by the area range.

8.4.1.9.1 no area range

The **no** form of this command to delete a summary prefix or remove a static cost.

Format `no area areaid range prefix netmask {summarylink | nssaexternallink} cost`

Mode Router OSPFv3 Config

8.4.1.10 area stub (OSPFv3)

This command creates a stub area for the specified area ID. A stub area is characterized by the fact that AS External LSAs are not propagated into the area. Removing AS External LSAs and Summary LSAs can significantly reduce the link state database of routers within the stub area.

Format `area areaid stub`
Mode Router OSPFv3 Config

8.4.1.10.1 no area stub

This command deletes a stub area for the specified area ID.

Format `no area areaid stub`
Mode Router OSPFv3 Config

8.4.1.11 area stub no-summary (OSPFv3)

This command disables the import of Summary LSAs for the stub area identified by *areaid*.

Default enabled
Format `area areaid stub no-summary`
Mode Router OSPFv3 Config

8.4.1.11.1 no area stub no-summary

This command sets the Summary LSA import mode to the default for the stub area identified by *areaid*.

Format `no area areaid stub summarylsa`
Mode Router OSPFv3 Config

8.4.1.12 area virtual-link (OSPFv3)

This command creates the OSPF virtual interface for the specified *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

Format `area areaid virtual-link neighbor`
Mode Router OSPFv3 Config

8.4.1.12.1 no area virtual-link

This command deletes the OSPF virtual interface from the given interface, identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

Format `no area areaid virtual-link neighbor`
Mode Router OSPFv3 Config

8.4.1.13 area virtual-link dead-interval (OSPFv3)

This command configures the dead interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor. The range for *seconds* is 1 to 65535.

Default 40
Format `area` *areaid* `virtual-link` *neighbor* `dead-interval` *seconds*
Mode Router OSPFv3 Config

8.4.1.13.1 no area virtual-link dead-interval

This command configures the default dead interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

Format `no area` *areaid* `virtual-link` *neighbor* `dead-interval`
Mode Router OSPFv3 Config

8.4.1.14 area virtual-link hello-interval (OSPFv3)

This command configures the hello interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor. The range for *seconds* is 1 to 65535.

Default 10
Format `area` *areaid* `virtual-link` *neighbor* `hello-interval` *seconds*
Mode Router OSPFv3 Config

8.4.1.14.1 no area virtual-link hello-interval

This command configures the default hello interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

Format `no area` *areaid* `virtual-link` *neighbor* `hello-interval`
Mode Router OSPFv3 Config

8.4.1.15 area virtual-link retransmit-interval (OSPFv3)

This command configures the retransmit interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor. The range for *seconds* is 0 to 3600.

Default 5
Format `area` *areaid* `virtual-link` *neighbor* `retransmit-interval` *seconds*
Mode Router OSPFv3 Config

8.4.1.15.1 no area virtual-link retransmit-interval

This command configures the default retransmit interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

Format `no area areaid virtual-link neighbor retransmit-interval`
Mode Router OSPFv3 Config

8.4.1.16 area virtual-link transmit-delay (OSPFv3)

This command configures the transmit delay for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor. The range for *seconds* is 0 to 3600 (1 hour).

Default 1
Format `area areaid virtual-link neighbor transmit-delay seconds`
Mode Router OSPFv3 Config

8.4.1.16.1 no area virtual-link transmit-delay

This command configures the default transmit delay for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

Format `no area areaid virtual-link neighbor transmit-delay`
Mode Router OSPFv3 Config

8.4.1.17 auto-cost (OSPFv3)

By default, OSPF computes the link cost of each interface from the interface bandwidth. Faster links have lower metrics, making them more attractive in route selection. The configuration parameters in the `auto-cost reference bandwidth` and `bandwidth` commands give you control over the default link cost. You can configure for OSPF an interface bandwidth that is independent of the actual link speed. A second configuration parameter allows you to control the ratio of interface bandwidth to link cost. The link cost is computed as the ratio of a reference bandwidth to the interface bandwidth (ref_bw / interface bandwidth), where interface bandwidth is defined by the `bandwidth` command. Because the default reference bandwidth is 100 Mbps, OSPF uses the same default link cost for all interfaces whose bandwidth is 100 Mbps or greater. Use the `auto-cost` command to change the reference bandwidth, specifying the reference bandwidth in megabits per second (Mbps). The reference bandwidth range is 1–4294967 Mbps.

Default 100Mbps
Format `auto-cost reference-bandwidth 1-4294967`
Mode Router OSPFv3 Config

8.4.1.17.1 no auto-cost reference-bandwidth (OSPFv3)

Use this command to set the reference bandwidth to the default value.

Format `no auto-cost reference-bandwidth`
Mode Router OSPFv3 Config

8.4.1.18 clear ipv6 ospf

Use this command to disable and reenable OSPF.

Format `clear ipv6 ospf`
Mode Privileged EXEC

8.4.1.19 clear ipv6 ospf configuration

Use this command to reset the OSPF configuration to factory defaults.

Format `clear ipv6 ospf configuration`
Mode Privileged EXEC

8.4.1.20 clear ipv6 ospf counters

Use this command to reset global and interface statistics.

Format `clear ipv6 ospf counters`
Mode Privileged EXEC

8.4.1.21 clear ipv6 ospf neighbor

Use this command to drop the adjacency with all OSPF neighbors. On each neighbor's interface, send a one-way hello. Adjacencies may then be reestablished. To drop all adjacencies with a specific router ID, specify the neighbor's Router ID using the optional parameter *[neighbor-id]*.

Format `clear ipv6 ospf neighbor` *`[neighbor-id]`*
Mode Privileged EXEC

8.4.1.22 clear ipv6 ospf neighbor interface

To drop adjacency with all neighbors on a specific interface, use the optional parameter `[slot/port]`. The argument `slot/port` corresponds to a physical routing interface or VLAN routing interface. The keyword `vlan` is used to specify the VLAN ID of the routing VLAN directly instead of a *slot/port* format. To drop adjacency with a specific router ID on a specific interface, use the optional parameter *[neighbor-id]*.

Format `clear ipv6 ospf neighbor interface` *`[slot/port|vlan 1-4093] [neighbor-id]`*
Mode Privileged EXEC

8.4.1.23 clear ipv6 ospf redistribution

Use this command to flush all self-originated external LSAs. Reapply the redistribution configuration and reoriginate prefixes as necessary.

Format `clear ipv6 ospf redistribution`
Mode Privileged EXEC

8.4.1.24 default-information originate (OSPFv3)

This command is used to control the advertisement of default routes.

Default
- metric—unspecified
- type—2

Format `default-information originate [always] [metric 0-16777214] [metric-type {1 | 2}]`

Mode Router OSPFv3 Config

8.4.1.24.1 no default-information originate (OSPFv3)

This command is used to control the advertisement of default routes.

Format `no default-information originate [metric] [metric-type]`

Mode Router OSPFv3 Config

8.4.1.25 default-metric (OSPFv3)

This command is used to set a default for the metric of distributed routes.

Format `default-metric 1-16777214`

Mode Router OSPFv3 Config

8.4.1.25.1 no default-metric (OSPFv3)

This command is used to set a default for the metric of distributed routes.

Format `no default-metric`

Mode Router OSPFv3 Config

8.4.1.26 distance ospf (OSPFv3)

This command sets the route preference value of OSPF route types in the router. Lower route preference values are preferred when determining the best route. The type of OSPF route can be intra, inter, or external. All the external type routes are given the same preference value. The range of *preference* value is 1 to 255.

Default 110

Format `distance ospf {intra-area 1-255 | inter-area 1-255 | external 1-255}`

Mode Router OSPFv3 Config

8.4.1.26.1 no distance ospf

This command sets the default route preference value of OSPF routes in the router. The type of OSPF route can be intra, inter, or external. All the external type routes are given the same preference value.

Format `no distance ospf {intra-area | inter-area | external}`

Mode Router OSPFv3 Config

8.4.1.27 enable (OSPFv3)

This command resets the default administrative mode of OSPF in the router (active).

Default	enabled
Format	`enable`
Mode	Router OSPFv3 Config

8.4.1.27.1 no enable (OSPFv3)

This command sets the administrative mode of OSPF in the router to inactive.

Format	`no enable`
Mode	Router OSPFv3 Config

8.4.1.28 exit-overflow-interval (OSPFv3)

This command configures the exit overflow interval for OSPF. It describes the number of seconds after entering Overflow state that a router will wait before attempting to leave the overflow state. This allows the router to again originate non-default AS-external-LSAs. When set to 0, the router will not leave overflow state until restarted. The range for *`seconds`* is 0 to 2147483647 seconds.

Default	0
Format	`exit-overflow-interval` *`seconds`*
Mode	Router OSPFv3 Config

8.4.1.28.1 no exit-overflow-interval

This command configures the default exit overflow interval for OSPF.

Format	`no exit-overflow-interval`
Mode	Router OSPFv3 Config

8.4.1.29 external-lsdb-limit (OSPFv3)

This command configures the external LSDB limit for OSPF. If the value is –1, then there is no limit. When the number of non-default AS-external-LSAs in a router's link-state database reaches the external LSDB limit, the router enters overflow state. The router never holds more than the external LSDB limit non-default AS-external-LSAs in it database. The external LSDB limit MUST be set identically in all routers attached to the OSPF backbone and/or any regular OSPF area. The range for *`Limit`* is –1 to 2147483647.

Default	-1
Format	`external-lsdb-limit` *`limit`*
Mode	Router OSPFv3 Config

8.4.1.29.1 no external-lsdb-limit

This command configures the default external LSDB limit for OSPF.

Format	`no external-lsdb-limit`
Mode	Router OSPFv3 Config

8.4.1.30 maximum-paths (OSPFv3)

This command sets the number of paths that OSPF can report for a given destination where *maxpaths* is platform dependent.

Default	4
Format	`maximum-paths` *maxpaths*
Mode	Router OSPFv3 Config

8.4.1.30.1 no maximum-paths

This command resets the number of paths that OSPF can report for a given destination back to its default value.

Format	`no maximum-paths`
Mode	Router OSPFv3 Config

8.4.1.31 passive-interface default (OSPFv3)

Use this command to enable global passive mode by default for all interfaces. It overrides any interface level passive mode. OSPF shall not form adjacencies over a passive interface.

Default	disabled
Format	`passive-interface default`
Mode	Router OSPFv3 Config

8.4.1.31.1 no passive-interface default

Use this command to disable the global passive mode by default for all interfaces. Any interface previously configured to be passive reverts to non-passive mode.

Format	`no passive-interface default`
Mode	Router OSPFv3 Config

8.4.1.32 passive-interface (OSPFv3)

Use this command to set the interface or tunnel as passive. The argument `slot/port` corresponds to a physical routing interface or VLAN routing interface. The keyword `vlan` is used to specify the VLAN ID of the routing VLAN directly instead of a *slot/port* format. It overrides the global passive mode that is currently effective on the interface or tunnel.

Default	disabled
Format	`passive-interface {`*slot/port*`|`*vlan 1-4093*`|tunnel` *tunnel-id*`}`
Mode	Router OSPFv3 Config

8.4.1.32.1 no passive-interface

Use this command to set the interface or tunnel as non-passive. It overrides the global passive mode that is currently effective on the interface or tunnel.

Format	`no passive-interface {`*slot/port*`|`*vlan 1-4093*`|tunnel` *tunnel-id*`}`

Mode Router OSPFv3 Config

8.4.1.33 redistribute (OSPFv3)

This command configures the OSPFv3 protocol to allow redistribution of routes from the specified source protocol/routers. If you use the `bgp` keyword to redistribute BGP routes into OSPFv3, only the external BGP routes are redistributed.

Default
- metric—unspecified
- type—2
- tag—0

Format `redistribute {static | connected | bgp} [metric` *`0-16777214`*`] [metric-type {1 | 2}] [tag` *`0-4294967295`*`]`

Mode Router OSPFv3 Config

8.4.1.33.1 no redistribute

This command configures OSPF protocol to prohibit redistribution of routes from the specified source protocol/routers.

Format `no redistribute {static | connected | bgp}` *`[metric] [metric-type] [tag]`*

Mode Router OSPFv3 Config

8.4.1.34 router-id (OSPFv3)

This command sets a 4-digit dotted-decimal number uniquely identifying the router ospf id. The *`ipaddress`* is a configured value.

Format `router-id` *`ipaddress`*

Mode Router OSPFv3 Config

8.4.1.35 timers pacing lsa-group

Use this command to adjust how OSPFv3 groups LSAs for periodic refresh. OSPFv3 refreshes self-originated LSAs approximately once every 30 minutes. When OSPFv3 refreshes LSAs, it considers all self-originated LSAs whose age is from 1800 to 1800 plus the pacing group size. Grouping LSAs for refresh allows OSPFv3 to combine refreshed LSAs into a minimal number of LS Update packets. Minimizing the number of Update packets makes LSA distribution more efficient.

When OSPFv3 originates a new or changed LSA, it selects a random refresh delay for the LSA. When the refresh delay expires, OSPFv3 refreshes the LSA. By selecting a random refresh delay, OSPFv3 avoids refreshing a large number of LSAs at one time, even if a large number of LSAs are originated at one time.

seconds is the width of the window in which LSAs are refreshed. The range for the pacing group window is from 10 to 1800 seconds.

Default 60 seconds

Format `timers pacing lsa-group` *`seconds`*

Mode Privileged EXEC

8.4.1.35.1 no timers pacing lsa-group

This command returns the LSA Group Pacing parameter to the factory default value of 60 seconds.

Format `no timers pacing lsa-group`
Mode Privileged EXEC

8.4.1.36 timers throttle spf

The initial “wait interval” is set to an amount of delay specified by the spf-hold value. If an SPF calculation is not scheduled during the current “wait interval”, the next SPF calculation is scheduled at a delay of *spf-start*. If there has been an SPF calculation scheduled during the current “wait interval”, the “wait interval” is set to two times the current “wait interval” until the “wait interval” reaches the maximum time in milliseconds as specified in *spf-maximum*. Subsequent wait times remain at the maximum until the values are reset or an LSA is received between SPF calculations.

Default *spf-start* = 2000 ms
spf-hold = 5000 ms
spf-maximum = 5000 ms
Format `timers throttle spf` *`spf-start spf-hold spf-maximum`*
Mode Privileged EXEC

Parameter	Description
spf-start	Indicates the SPF schedule delay in milliseconds when no SPF calculation has been scheduled during the current “wait interval”. Value range is 1 to 600000 milliseconds.
spf-hold	Indicates the initial SPF “wait interval” in milliseconds. Value range is 1 to 600000 milliseconds.
spf-maximum	Indicates the maximum SPF “wait interval” in milliseconds. Value range is 1 to 600000 milliseconds.

8.4.1.36.1 no timers throttle spf

This command returns the SPF throttling parameters to the factory default values.

Format `no timers throttle spf`
Mode Privileged EXEC

8.4.1.37 trapflags (OSPFv3)

Use this command to enable individual OSPF traps, enable a group of trap flags at a time, or enable all the trap flags at a time. The different groups of trapflags, and each group’s specific trapflags to enable or disable, are listed in Table 15.

Table 15: Trapflag Groups (OSPFv3)

Group	Flags
errors	■ authentication-failure ■ bad-packet ■ config-error ■ virt-authentication-failure ■ virt-bad-packet ■ virt-config-error

Table 15: Trapflag Groups (OSPFv3) (Continued)

Group	Flags
lsa	■ lsa-maxage ■ lsa-originate
overflow	■ lsdb-overflow ■ lsdb-approaching-overflow
retransmit	■ packets ■ virt-packets
state-change	■ if-state-change ■ neighbor-state-change ■ virtif-state-change ■ virtneighbor-state-change

- To enable the individual flag, enter the `group name` followed by that particular flag.
- To enable all the flags in that group, give the group name followed by `all`.
- To enable all the flags, give the command as `trapflags all`.

Default disabled

Format
```
trapflags {
all |
errors {all | authentication-failure | bad-packet | config-error | virt-authentication-
failure | virt-bad-packet | virt-config-error} |
lsa {all | lsa-maxage | lsa-originate} |
overflow {all | lsdb-overflow | lsdb-approaching-overflow} |
retransmit {all | packets | virt-packets} |
state-change {all | if-state-change | neighbor-state-change | virtif-state-change |
virtneighbor-state-change}
}
```

Mode Router OSPFv3 Config

8.4.1.37.1 no trapflags

Use this command to revert to the default reference bandwidth.

- To disable the individual flag, enter the `group name` followed by that particular flag.
- To disable all the flags in that group, give the group name followed by `all`.
- To disable all the flags, give the command as `trapflags all`.

Format
```
no trapflags {
all |
errors {all | authentication-failure | bad-packet | config-error | virt-
authentication-failure | virt-bad-packet | virt-config-error} |
lsa {all | lsa-maxage | lsa-originate} |
overflow {all | lsdb-overflow | lsdb-approaching-overflow} |
retransmit {all | packets | virt-packets} |
state-change {all | if-state-change | neighbor-state-change | virtif-state-
change | virtneighbor-state-change}
}
```

Mode Router OSPFv3 Config

8.4.2 OSPFv3 Interface Commands

8.4.2.1 ipv6 ospf area

This command sets the OSPF area to which the specified router interface or range of interfaces belongs. It also enables OSPF on the specified router interface or range of interfaces. The *area* is a 32-bit integer, formatted as a 4-digit dotted-decimal number or a decimal value in the range of 0-4294967295. The *area* uniquely identifies the area to which the interface connects. Assigning an area ID for an area that does not yet exist, causes the area to be created with default values.

Format `ipv6 ospf area` *0-4294967295*
Mode Interface Config

8.4.2.2 ipv6 ospf cost

This command configures the cost on an OSPF interface or range of interfaces. The *cost* parameter has a range of 1 to 65535.

Default 10
Format `ipv6 ospf cost` *1-65535*
Mode Interface Config

8.4.2.2.1 no ipv6 ospf cost

This command configures the default cost on an OSPF interface.

Format `no ipv6 ospf cost`
Mode Interface Config

8.4.2.3 ipv6 ospf dead-interval

This command sets the OSPF dead interval for the specified interface or range of interfaces. The value for *seconds* is a valid positive integer, which represents the length of time in seconds that a router's Hello packets have not been seen before its neighbor routers declare that the router is down. The value for the length of time must be the same for all routers attached to a common network. This value should be some multiple of the Hello Interval (i.e., 4). Valid values range for *seconds* is from 1 to 2147483647.

Default 40
Format `ipv6 ospf dead-interval` *1-2147483647*
Mode Interface Config

8.4.2.3.1 no ipv6 ospf dead-interval

This command sets the default OSPF dead interval for the specified interface or range of interfaces.

Format `no ipv6 ospf dead-interval`
Mode Interface Config

8.4.2.4 ipv6 ospf hello-interval

This command sets the OSPF hello interval for the specified interface. The value for *seconds* is a valid positive integer, which represents the length of time in seconds. The value for the length of time must be the same for all routers attached to a network. Valid values for *seconds* range from 1 to 65535.

Default 10
Format `ipv6 ospf hello-interval` *seconds*
Mode Interface Config

8.4.2.4.1 no ipv6 ospf hello-interval

This command sets the default OSPF hello interval for the specified interface.

Format `no ipv6 ospf hello-interval`
Mode Interface Config

8.4.2.5 ipv6 ospf link-lsa-suppression

Use this command to enable Link LSA Suppression on an interface. When Link LSA Suppression is enabled on a point-to-point (P2P) interface, no Link LSA protocol packets are originated (transmitted) on the interface. This configuration does not apply to non-P2P interfaces.

Default False
Format `ipv6 ospf link-lsa-suppression`
Mode Privileged EXEC

8.4.2.5.1 no ipv6 ospf link-lsa-suppression

This command returns Link LSA Suppression for the interface to disabled. When Link LSA Suppression is disabled, Link LSA protocol packets are originated (transmitted) on the P2P interface.

Format `no ipv6 ospf link-lsa-suppression`
Mode Privileged EXEC

8.4.2.6 ipv6 ospf mtu-ignore

This command disables OSPF maximum transmission unit (MTU) mismatch detection on an interface or range of interfaces. OSPF Database Description packets specify the size of the largest IP packet that can be sent without fragmentation on the interface. When a router receives a Database Description packet, it examines the MTU advertised by the neighbor. By default, if the MTU is larger than the router can accept, the Database Description packet is rejected and the OSPF adjacency is not established.

Default enabled
Format `ipv6 ospf mtu-ignore`
Mode Interface Config

8.4.2.6.1 no ipv6 ospf mtu-ignore

This command enables the OSPF MTU mismatch detection.

Format	`no ipv6 ospf mtu-ignore`
Mode	Interface Config

8.4.2.7 ipv6 ospf network

This command changes the default OSPF network type for the interface or range of interfaces. Normally, the network type is determined from the physical IP network type. By default all Ethernet networks are OSPF type broadcast. Similarly, tunnel interfaces default to point-to-point. When an Ethernet port is used as a single large bandwidth IP network between two routers, the network type can be point-to-point since there are only two routers. Using point-to-point as the network type eliminates the overhead of the OSPF designated router election. It is normally not useful to set a tunnel to OSPF network type broadcast.

Default	broadcast
Format	`ipv6 ospf network {broadcast | point-to-point}`
Mode	Interface Config

8.4.2.7.1 no ipv6 ospf network

This command sets the interface type to the default value.

Format	`no ipv6 ospf network {broadcast | point-to-point}`
Mode	Interface Config

8.4.2.8 ipv6 ospf prefix-suppression

This command suppresses the advertisement of the IPv6 prefixes that are associated with an interface, except for those associated with secondary IPv6 addresses. This command takes precedence over the global configuration. If this configuration is not specified, the global prefix-suppression configuration applies.

prefix-suppression can be disabled at the interface level by using the disable option. The disable option is useful for excluding specific interfaces from performing prefix-suppression when the feature is enabled globally.

Note that the disable option disable is not equivalent to not configuring the interface specific prefix-suppression. If prefix-suppression is not configured at the interface level, the global prefix-suppression configuration is applicable for the IPv6 prefixes associated with the interface.

Default	prefix-suppression is not configured.
Format	`ipv6 ospf prefix-suppression [disable]`
Mode	Interface Config

8.4.2.8.1 no ipv6 ospf prefix-suppression

This command removes prefix-suppression configurations at the interface level. When the `no ipv6 ospf prefix-suppression` command is used, global prefix-suppression applies to the interface. Not configuring the command is not equal to disabling interface level prefix-suppression.

Format `no ipv6 ospf prefix-suppression`
Mode Interface Config

8.4.2.9 ipv6 ospf priority

This command sets the OSPF priority for the specified router interface or range of interfaces. The priority of the interface is a priority integer from 0 to 255. A value of 0 indicates that the router is not eligible to become the designated router on this network.

Default 1, which is the highest router priority
Format `ipv6 ospf priority` *`0-255`*
Mode Interface Config

8.4.2.9.1 no ipv6 ospf priority

This command sets the default OSPF priority for the specified router interface.

Format `no ipv6 ospf priority`
Mode Interface Config

8.4.2.10 ipv6 ospf retransmit-interval

This command sets the OSPF retransmit Interval for the specified interface or range of interfaces. The retransmit interval is specified in seconds. The value for *`seconds`* is the number of seconds between link-state advertisement retransmissions for adjacencies belonging to this router interface. This value is also used when retransmitting database description and link-state request packets. Valid values range from 0 to 3600 (1 hour).

Default 5
Format `ipv6 ospf retransmit-interval` *`seconds`*
Mode Interface Config

8.4.2.10.1 no ipv6 ospf retransmit-interval

This command sets the default OSPF retransmit Interval for the specified interface.

Format `no ipv6 ospf retransmit-interval`
Mode Interface Config

8.4.2.11 ipv6 ospf transmit-delay

This command sets the OSPF Transit Delay for the specified interface or range of interfaces. The transmit delay is specified in seconds. In addition, it sets the estimated number of seconds it takes to transmit a link state update packet over this interface. Valid values for *`seconds`* range from 1 to 3600 (1 hour).

Default 1
Format `ipv6 ospf transmit-delay` *`seconds`*
Mode Interface Config

8.4.2.11.1 no ipv6 ospf transmit-delay

This command sets the default OSPF Transit Delay for the specified interface.

Format `no ipv6 ospf transmit-delay`

Mode Interface Config

8.4.3 OSPFv3 Graceful Restart Commands

The OSPFv3 protocol can be configured to participate in the checkpointing service, so that these protocols can execute a “graceful restart” when the management unit fails. In a graceful restart, the hardware to continues forwarding IPv6 packets using OSPFv3 routes while a backup switch takes over management unit responsibility

Graceful restart uses the concept of “helpful neighbors”. A fully adjacent router enters helper mode when it receives a link state announcement (LSA) from the restarting management unit indicating its intention of performing a graceful restart. In helper mode, a switch continues to advertise to the rest of the network that they have full adjacencies with the restarting router, thereby avoiding announcement of a topology change and the potential for flooding of LSAs and shortest-path-first (SPF) runs (which determine OSPF routes). Helpful neighbors continue to forward packets through the restarting router. The restarting router relearns the network topology from its helpful neighbors.

Graceful restart can be enabled for either planned or unplanned restarts, or both. A planned restart is initiated by the operator through the management command `initiate failover`. The operator may initiate a failover in order to take the management unit out of service (for example, to address a partial hardware failure), to correct faulty system behavior which cannot be corrected through less severe management actions, or other reasons. An unplanned restart is an unexpected failover caused by a fatal hardware failure of the management unit or a software hang or crash on the management unit.

8.4.3.1 nsf (OSPFv3)

Use this command to enable the OSPF graceful restart functionality on an interface. To disable graceful restart, use the no form of the command.

Default Disabled

Format `nsf [ietf] [planned-only]`

Modes Router OSPFv3 Config

Parameter	Description
ietf	This keyword is accepted but not required.
planned-only	This optional keyword indicates that OSPF should only perform a graceful restart when the restart is planned (i.e., when the restart is a result of the initiate failover command).

8.4.3.1.1 no nsf (OSPFv3)

Use this command to disable graceful restart for all restarts.

8.4.3.2 nsf restart-interval (OSPFv3)

Use this command to configure the number of seconds that the restarting router asks its neighbors to wait before exiting helper mode. This is referred to as the grace period. The restarting router includes the grace period in its grace LSAs. For planned restarts (using the `initiate failover` command), the grace LSAs are sent prior to restarting the management unit, whereas for unplanned restarts, they are sent after reboot begins.

The grace period must be set long enough to allow the restarting router to reestablish all of its adjacencies and complete a full database exchange with each of those neighbors.

Default 120 seconds

Format `nsf [ietf] restart-interval` ***1-1800***

Modes Router OSPFv3 Config

Parameter	Description
ietf	This keyword is accepted but not required.
seconds	The number of seconds that the restarting router asks its neighbors to wait before exiting helper mode. The range is from 1 to 1800 seconds.

8.4.3.2.1 no nsfrestart-interval (OSPFv3)

Use this command to revert the grace period to its default value.

Format `no [ietf] nsf restart-interval`
Modes Router OSPFv3 Config

8.4.3.3 nsf helper (OSPFv3)

Use this command to enable helpful neighbor functionality for the OSPF protocol. You can enable this functionality for planned or unplanned restarts, or both.

Default OSPF may act as a helpful neighbor for both planned and unplanned restarts
Format `nsf helper [planned-only]`
Modes Router OSPFv3 Config

Parameter	Description
planned-only	This optional keyword indicates that OSPF should only help a restarting router performing a planned restart.

8.4.3.3.1 no nsf helper (OSPFv3)

Use this command to disable helpful neighbor functionality for OSPF.

Format `no nsf helper`
Modes Router OSPFv3 Config

8.4.3.4 nsf ietf helper disable (OSPFv3)

Use this command to disable helpful neighbor functionality for OSPF.

NOTE: The commands `no nsf helper` and `nsf ietf helper disable` are functionally equivalent. The command `nsf ietf helper disable` is supported solely for compatibility with other network software CLI.

Format `nsf ietf helper disable`
Modes Router OSPFv3 Config

8.4.3.5 nsf helper strict-lsa-checking (OSPFv3)

The restarting router is unable to react to topology changes. In particular, the restarting router will not immediately update its forwarding table; therefore, a topology change may introduce forwarding loops or black holes that persist until the graceful restart completes. By exiting the graceful restart on a topology change, a router tries to eliminate the loops or black holes as quickly as possible by routing around the restarting router. A helpful neighbor considers a link down with the restarting router to be a topology change, regardless of the strict LSA checking configuration.

Use this command to require that an OSPF helpful neighbor exit helper mode whenever a topology change occurs.

Default Enabled.
Format `nsf [ietf] helper strict-lsa-checking`
Modes Router OSPFv3 Config

Parameter	Description
ietf	This keyword is accepted but not required.

8.4.3.5.1 no nsf [ietf] helper strict-lsa-checking (OSPFv3)

Use this command to allow OSPF to continue as a helpful neighbor in spite of topology changes.

Default Enabled.
Format `nsf [ietf] helper strict-lsa-checking`
Modes Router OSPFv3 Config

8.4.4 OSPFv3 Stub Router Commands

8.4.4.1 max-metric router-lsa

To configure OSPFv3 to enter stub router mode, use this command in Router OSPFv3 Global Configuration mode. When OSPFv3 is in stub router mode, OSPFv3 sets the metric in the nonstub links in its router LSA to MaxLinkMetric. Other routers therefore compute very long paths through the stub router, and prefer any alternate path. Doing so eliminates all transit traffic through the stub router, when alternate routes are available. Stub router mode is useful when adding or removing a router from a network or to avoid transient routes when a router reloads.

You can administratively force OSPFv3 into stub router mode. OSPFv3 remains in stub router mode until you take OSPFv3 out of stub router mode. Alternatively, you can configure OSPF to start in stub router mode for a configurable period of time after the router boots up.

If you set the summary LSA metric to 16,777,215, other routers will skip the summary LSA when they compute routes.

If you have configured the router to enter stub router mode on startup (max-metric router-lsa on-startup), and then enter max-metric router lsa, there is no change. If OSPFv3 is administratively in stub router mode (the max-metric router-lsa command has been given), and you configure OSPFv3 to enter stub router mode on startup (max-metric router-lsa on-startup), OSPFv3 exits stub router mode (assuming the startup period has expired) and the configuration is updated. Without any parameters, stub router mode only sends maximum metric values for router LSAs.

Default `OSPF is not in stub router mode by default`

Format `max-metric router-lsa [external-lsa` *`1-16777215`*`] [inter-area-lsas` *`1-16777215`*`] [on-startup` *`5-86400`*`] [summary-lsa` *`1-16777215`*`]`

Mode OSPFv3 Router Configuration

Parameter	Description
external-lsa	(Optional) Sends the maximum metric values for external LSAs. *max-metric-value* is the maximum metric value to use for LSAs. The range is 1 to 16777215 (0xFFFFFF). The default value is 16711680 (0xFF0000).
inter-area-lsas	(Optional) Sends the maximum metric values for Inter-Area-Router LSAs
on-startup	(Optional) Starts OSPF in stub router mode. *seconds* is the number of seconds that OSPF remains in stub router mode after a reboot. The range is 5 to 86,400 seconds. There is no default value.
summary-lsa	(Optional) Sends the maximum metric values for Summary LSAs

8.4.4.1.1 no max-metric router-lsa

Use this command in OSPFv3 Router Configuration mode to disable stub router mode. The command clears either type of stub router mode (always or on-startup) and resets all LSA options. If OSPF is configured to enter global configuration mode on startup, and during normal operation you want to immediately place OSPF in stub router mode, issue the command **no max-metric router-lsa on-startup**. The command **no max-metric** with the external-lsa, inter-area-lsas, or summary-lsa option **router-lsa summary-lsa** causes OSPF to send summary LSAs with metrics computed using normal procedures.

Format `no max-metric router-lsa [external-lsa] [inter-area-lsas] [on-startup] [summary-lsa]`

Mode OSPFv3 Router Configuration

8.4.4.2 clear ipv6 ospf stub-router

Use this command to force OSPF to exit stub router mode when it has automatically entered stub router mode because of a resource limitation. OSPF only exits stub router mode if it entered stub router mode because of a resource limitation or it if is in stub router mode at startup. This command has no effect if OSPF is configured to be in stub router mode permanently.

Format `clear ipv6 ospf stub-router`

Mode Privileged EXEC

8.4.5 OSPFv3 Show Commands

8.4.5.1 show ipv6 ospf

This command displays information relevant to the OSPF router.

Format `show ipv6 ospf`

Mode
- Privileged EXEC
- User EXEC

NOTE: Some of the information below displays only if you enable OSPF and configure certain features.

Term	Definition
Router ID	A 32-bit integer in dotted decimal format identifying the router, about which information is displayed. This is a configured value.
OSPF Admin Mode	Shows whether the administrative mode of OSPF in the router is enabled or disabled. This is a configured value.
External LSDB Limit	The maximum number of non-default AS-external-LSAs entries that can be stored in the link-state database.
Exit Overflow Interval	The number of seconds that, after entering overflow state, a router will attempt to leave overflow state.
SPF Start Time	The number of milliseconds the SPF calculation is delayed if no SPF calculation has been scheduled during the current “wait interval”.
SPF Hold Time	The number of milliseconds of the initial “wait interval”.
SPF Maximum Hold Time	The maximum number of milliseconds of the “wait interval”.
LSA Refresh Group Pacing Time	The size of the LSA refresh group window, in seconds.
AutoCost Ref BW	Shows the value of the auto-cost reference bandwidth configured on the router.
Default Passive Setting	Shows whether the interfaces are passive by default.
Maximum Paths	The maximum number of paths that OSPF can report for a given destination.
Default Metric	Default value for redistributed routes.
Default Route Advertise	Indicates whether the default routes received from other source protocols are advertised or not.
Always	Shows whether default routes are always advertised.
Metric	The metric for the advertised default routes. If the metric is not configured, this field is blank.
Metric Type	Shows whether the routes are External Type 1 or External Type 2.
Number of Active Areas	The number of active OSPF areas. An “active” OSPF area is an area with at least one interface up.
ABR Status	Shows whether the router is an OSPF Area Border Router.
ASBR Status	Shows if the ASBR mode is enabled or disabled. Enable implies that the router is an autonomous system border router. Router automatically becomes an ASBR when it is configured to redistribute routes learnt from other protocol. The possible values for the ASBR status is enabled (if the router is configured to re-distribute routes learned by other protocols) or disabled (if the router is not configured for the same).
Stub Router Status	The status of the stub router: Active or Inactive.
Stub Router Reason	This is displayed only if the stub router is active. Shows the reason for the stub router: Configured, Startup, or Resource Limitation
Stub Router Startup Time Remaining	This is displayed only if the stub router is in startup stub router mode. The remaining time (in seconds) until OSPF exits stub router mode.

Term	Definition
Stub Router Duration	This row is only listed if the stub router is active and the router entered stub mode because of a resource limitation. The time elapsed since the router last entered the stub router mode. The duration is displayed in DD:HH:MM:SS format.
External LSDB Overflow	When the number of non-default external LSAs exceeds the configured limit, External LSDB Limit, OSPF goes into LSDB overflow state. In this state, OSPF withdraws all of its self-originated non-default external LSAs. After the Exit Overflow Interval, OSPF leaves the overflow state, if the number of external LSAs has been reduced.
External LSA Count	The number of external (LS type 5) link-state advertisements in the link-state database.
External LSA Checksum	The sum of the LS checksums of external link-state advertisements contained in the link-state database.
New LSAs Originated	The number of new link-state advertisements that have been originated.
LSAs Received	The number of link-state advertisements received determined to be new instantiations.
LSA Count	The total number of link state advertisements currently in the link state database.
Maximum Number of LSAs	The maximum number of LSAs that OSPF can store.
LSA High Water Mark	The maximum size of the link state database since the system started.
Retransmit List Entries	The total number of LSAs waiting to be acknowledged by all neighbors. An LSA may be pending acknowledgment from more than one neighbor.
Maximum Number of Retransmit Entries	The maximum number of LSAs that can be waiting for acknowledgment at any given time.
Retransmit Entries High Water Mark	The highest number of LSAs that have been waiting for acknowledgment.
Redistributing	This field is a heading and appears only if you configure the system to take routes learned from a non-OSPF source and advertise them to its peers.
Source	Shows source protocol/routes that are being redistributed. Possible values are static, connected, BGP, or RIP.
Metric	The metric of the routes being redistributed.
Metric Type	Shows whether the routes are External Type 1 or External Type 2.
Tag	The decimal value attached to each external route.
Subnets	For redistributing routes into OSPF, the scope of redistribution for the specified protocol.
Distribute-List	The access list used to filter redistributed routes.
Prefix-suppression	Displays whether prefix-suppression is enabled or disabled on the given interface.
NSF Support	Indicates whether nonstop forwarding (NSF) is enabled for the OSPF protocol for planned restarts, unplanned restarts or both (Always).
NSF Restart Interval	The user-configurable grace period during which a neighboring router will be in the helper state after receiving notice that the management unit is performing a graceful restart.
NSF Restart Status	The current graceful restart status of the router.
NSF Restart Age	Number of seconds until the graceful restart grace period expires.
NSF Restart Exit Reason	Indicates why the router last exited the last restart: ■ None—Graceful restart has not been attempted. ■ In Progress—Restart is in progress. ■ Completed—The previous graceful restart completed successfully. ■ Timed Out—The previous graceful restart timed out. ■ Topology Changed—The previous graceful restart terminated prematurely because of a topology change.
NSF Help Support	Indicates whether helpful neighbor functionality has been enabled for OSPF for planned restarts, unplanned restarts, or both (Always).

Term	Definition
NSF help Strict LSA checking	Indicates whether strict LSA checking has been enabled. If enabled, then an OSPF helpful neighbor will exit helper mode whenever a topology change occurs. If disabled, an OSPF neighbor will continue as a helpful neighbor in spite of topology changes.

8.4.5.2 show ipv6 ospf abr

This command displays the internal OSPFv3 routes to reach Area Border Routers (ABR). This command takes no options.

Format `show ipv6 ospf abr`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Type	The type of the route to the destination. It can be either: ■ intra — Intra-area route ■ inter — Inter-area route
Router ID	Router ID of the destination.
Cost	Cost of using this route.
Area ID	The area ID of the area from which this route is learned.
Next Hop	Next hop toward the destination.
Next Hop Intf	The outgoing router interface to use when forwarding traffic to the next hop.

8.4.5.3 show ipv6 ospf area

This command displays information about the area. The *areaid* identifies the OSPF area that is being displayed.

Format `show ipv6 ospf area` *areaid*

Modes
- Privileged EXEC
- User EXEC

Term	Definition
AreaID	The area id of the requested OSPF area.
External Routing	A number representing the external routing capabilities for this area.
Spf Runs	The number of times that the intra-area route table has been calculated using this area's link-state database.
Area Border Router Count	The total number of area border routers reachable within this area.
Area LSA Count	Total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.
Area LSA Checksum	A number representing the Area LSA Checksum for the specified AreaID excluding the external (LS type 5) link-state advertisements.
Stub Mode	Represents whether the specified Area is a stub area or not. The possible values are enabled and disabled. This is a configured value.
Import Summary LSAs	Shows whether to import summary LSAs (enabled).
OSPF Stub Metric Value	The metric value of the stub area. This field displays only if the area is a configured as a stub area.

The following OSPF NSSA specific information displays only if the area is configured as an NSSA.

Term	Definition
Import Summary LSAs	Shows whether to import summary LSAs into the NSSA.
Redistribute into NSSA	Shows whether to redistribute information into the NSSA.
Default Information Originate	Shows whether to advertise a default route into the NSSA.
Default Metric	The metric value for the default route advertised into the NSSA.
Default Metric Type	The metric type for the default route advertised into the NSSA.
Translator Role	The NSSA translator role of the ABR, which is always or candidate.
Translator Stability Interval	The amount of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router.
Translator State	Shows whether the ABR translator state is disabled, always, or elected.

8.4.5.4 show ipv6 ospf asbr

This command displays the internal OSPFv3 routes to reach Autonomous System Boundary Routers (ASBR). This command takes no options.

Format `show ipv6 ospf asbr`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Type	The type of the route to the destination. It can be either: ■ intra — Intra-area route ■ inter — Inter-area route
Router ID	Router ID of the destination.
Cost	Cost of using this route.
Area ID	The area ID of the area from which this route is learned.
Next Hop	Next hop toward the destination.
Next Hop Intf	The outgoing router interface to use when forwarding traffic to the next hop.

8.4.5.5 show ipv6 ospf database

This command displays information about the link state database when OSPFv3 is enabled. If you do not enter any parameters, the command displays the LSA headers for all areas. Use the optional *areaid* parameter to display database information about a specific area. Use the other optional parameters to specify the type of link state advertisements to display. Use *external* to display the external LSAs. Use *inter-area* to display the inter-area LSAs. Use *link* to display the link LSAs. Use *network* to display the network LSAs. Use nssa-external to display NSSA external LSAs. Use *prefix* to display intra-area Prefix LSAs. Use *router* to display router LSAs. Use *unknown area*, *unknown as*, or *unknown link* to display unknown area, AS or link-scope LSAs, respectively. Use *lsid* to specify the link state ID (LSID). Use *adv-router* to show the LSAs that are restricted by the advertising router. Use *self-originate* to display the LSAs in that are self originated. The information below is only displayed if OSPF is enabled.

Format `show ipv6 ospf [areaid] database [{external | inter-area {prefix | router} | link | network | nssa-external | prefix | router | unknown {area | as | link}}] [lsid] [{adv-router [rtrid] | self-originate}]`

Modes
- Privileged EXEC
- User EXEC

For each link-type and area, the following information is displayed.

Term	Definition
Link Id	A number that uniquely identifies an LSA that a router originates from all other self originated LSAs of the same LS type.
Adv Router	The Advertising Router. Is a 32-bit dotted decimal number representing the LSDB interface.
Age	A number representing the age of the link state advertisement in seconds.
Sequence	A number that represents which LSA is more recent.
Checksum	The total number LSA checksum.
Prefix	The IPv6 prefix.
Interface	The interface for the link.
Rtr Count	The number of routers attached to the network.

8.4.5.6 show ipv6 ospf database database-summary

Use this command to display the number of each type of LSA in the database and the total number of LSAs in the database.

Format `show ipv6 ospf database database-summary`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Router	Total number of router LSAs in the OSPFv3 link state database.
Network	Total number of network LSAs in the OSPFv3 link state database.
Inter-area Prefix	Total number of inter-area prefix LSAs in the OSPFv3 link state database.
Inter-area Router	Total number of inter-area router LSAs in the OSPFv3 link state database.
Type-7 Ext	Total number of NSSA external LSAs in the OSPFv3 link state database.
Link	Total number of link LSAs in the OSPFv3 link state database.
Intra-area Prefix	Total number of intra-area prefix LSAs in the OSPFv3 link state database.
Link Unknown	Total number of link-source unknown LSAs in the OSPFv3 link state database.
Area Unknown	Total number of area unknown LSAs in the OSPFv3 link state database.
AS Unknown	Total number of as unknown LSAs in the OSPFv3 link state database.
Type-5 Ext	Total number of AS external LSAs in the OSPFv3 link state database.
Self-Originated Type-5	Total number of self originated AS external LSAs in the OSPFv3 link state database.
Total	Total number of router LSAs in the OSPFv3 link state database.

8.4.5.7 show ipv6 ospf interface

This command displays the information for the IFO object or virtual interface tables. The argument `slot/port` corresponds to a physical routing interface or VLAN routing interface. The keyword **vlan** is used to specify the VLAN ID of the routing VLAN directly instead of a *slot/port* format.

Format `show ipv6 ospf interface {`*`slot/port`*`|`*`vlan 1-4093`*`|loopback `*`loopback-id`*` | tunnel `*`tunnel-id`*`}`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
IP Address	The IPv6 address of the interface.
ifIndex	The interface index number associated with the interface.
OSPF Admin Mode	Shows whether the admin mode is enabled or disabled.
OSPF Area ID	The area ID associated with this interface.
Router Priority	The router priority. The router priority determines which router is the designated router.
Retransmit Interval	The frequency, in seconds, at which the interface sends LSA.
Hello Interval	The frequency, in seconds, at which the interface sends Hello packets.
Dead Interval	The amount of time, in seconds, the interface waits before assuming a neighbor is down.
LSA Ack Interval	The amount of time, in seconds, the interface waits before sending an LSA acknowledgement after receiving an LSA.
Interface Transmit Delay	The number of seconds the interface adds to the age of LSA packets before transmission.
Authentication Type	The type of authentication the interface performs on LSAs it receives.
Metric Cost	The priority of the path. Low costs have a higher priority than high costs.
Prefix-suppression	Displays whether prefix-suppression is enabled, disabled, or unconfigured on the given interface.
Passive Status	Shows whether the interface is passive or not.
OSPF MTU-ignore	Shows whether to ignore MTU mismatches in database descriptor packets sent from neighboring routers.
Link LSA Suppression	The configured state of Link LSA Suppression for the interface.

The following information only displays if OSPF is initialized on the interface:

Term	Definition
OSPF Interface Type	Broadcast LANs, such as Ethernet and IEEE 802.5, take the value *`broadcast`*. The OSPF Interface Type will be 'broadcast'.
State	The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router.
Designated Router	The router ID representing the designated router.
Backup Designated Router	The router ID representing the backup designated router.
Number of Link Events	The number of link events.
Metric Cost	The cost of the OSPF interface.

8.4.5.8 show ipv6 ospf interface brief

This command displays brief information for the IFO object or virtual interface tables.

Format `show ipv6 ospf interface brief`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Interface	*The routing interface associated with the rest of the data in the row.*
OSPF Admin Mode	States whether OSPF is enabled or disabled on a router interface.
OSPF Area ID	The OSPF Area ID for the specified interface.
Router Priority	The router priority. The router priority determines which router is the designated router.
Metric Cost	The priority of the path. Low costs have a higher priority than high costs.
Hello Interval	The frequency, in seconds, at which the interface sends Hello packets.
Dead Interval	The amount of time, in seconds, the interface waits before assuming a neighbor is down.
Retransmit Interval	The frequency, in seconds, at which the interface sends LSA.
Retransmit Delay Interval	The number of seconds the interface adds to the age of LSA packets before transmission.
LSA Ack Interval	The amount of time, in seconds, the interface waits before sending an LSA acknowledgement after receiving an LSA.

8.4.5.9 show ipv6 ospf interface stats

This command displays the statistics for a specific interface. The command displays information only if OSPF is enabled.

Format `show ipv6 ospf interface stats {`*`slot/port`* `| vlan` *`id`*`}`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
OSPFv3 Area ID	The area id of this OSPF interface.
IP Address	The IP address associated with this OSPF interface.
OSPFv3 Interface Events	The number of times the specified OSPF interface has changed its state, or an error has occurred.
Virtual Events	The number of state changes or errors that occurred on this virtual link.
Neighbor Events	The number of times this neighbor relationship has changed state, or an error has occurred.
Packets Received	The number of OSPFv3 packets received on the interface.
Packets Transmitted	The number of OSPFv3 packets sent on the interface.
LSAs Sent	The total number of LSAs flooded on the interface.
LSA Acks Received	The total number of LSA acknowledged from this interface.
LSA Acks Sent	The total number of LSAs acknowledged to this interface.
Sent Packets	The number of OSPF packets transmitted on the interface.
Received Packets	The number of valid OSPF packets received on the interface.
Discards	The number of received OSPF packets discarded because of an error in the packet or an error in processing the packet.
Bad Version	The number of received OSPF packets whose version field in the OSPF header does not match the version of the OSPF process handling the packet.

Term	Definition
Virtual Link Not Found	The number of received OSPF packets discarded where the ingress interface is in a non-backbone area and the OSPF header identifies the packet as belonging to the backbone, but OSPF does not have a virtual link to the packet's sender.
Area Mismatch	The number of OSPF packets discarded because the area ID in the OSPF header is not the area ID configured on the ingress interface.
Invalid Destination Address	The number of OSPF packets discarded because the packet's destination IP address is not the address of the ingress interface and is not the AllDrRouters or AllSpfRouters multicast addresses.
No Neighbor at Source Address	The number of OSPF packets dropped because the sender is not an existing neighbor or the sender's IP address does not match the previously recorded IP address for that neighbor. NOTE: Does not apply to Hellos.
Invalid OSPF Packet Type	The number of OSPF packets discarded because the packet type field in the OSPF header is not a known type.
Hellos Ignored	The number of received Hello packets that were ignored by this router from the new neighbors after the limit has been reached for the number of neighbors on an interface or on the system as a whole.

Table 12, Trapflags Groups lists the number of OSPF packets of each type sent and received on the interface.

8.4.5.10 show ipv6 ospf lsa-group

This command displays the number of self-originated LSAs within each LSA group.

Format `show ipv6 ospf lsa-group`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Total self-originated LSAs	The number of LSAs the router is currently originating.
Average LSAs per group	The number of self-originated LSAs divided by the number of LSA groups. The number of LSA groups is the refresh interval (1800 seconds) divided by the pacing interval (configured with `timers pacing lsa-group`) plus two.
Pacing group limit	The maximum number of self-originated LSAs in one LSA group. If the number of LSAs in a group exceeds this limit, OSPF redistributes LSAs throughout the refresh interval to achieve better balance.
Groups	For each LSA pacing group, the output shows the range of LSA ages in the group and the number of LSAs in the group.

Example: The following shows an example of the command.

```
(R1) #show ipv6 ospf lsa-group

Total self-originated LSAs:  3019
Average LSAs per group:  100
Pacing group limit:  400
Number of self-originated LSAs within each LSA group...


Group Start Age   Group End Age    Count
              0              59       96
             60             119       88
            120             179      102
```

```
 180             239       95
 240             299       95
 300             359       92
 360             419       48
 420             479       58
 480             539      103
 540             599       99
 600             659      119
 660             719      110
 720             779      106
 780             839      122
 840             899      110
 900             959       99
 960            1019      135
1020            1079      101
1080            1139       94
1140            1199      115
1200            1259      110
1260            1319      111
1320            1379      111
1380            1439       99
1440            1499      102
1500            1559       96
1560            1619      106
1620            1679      111
1680            1739      106
1740            1799       80
1800            1859        0
1860            1919        0
```

8.4.5.11 show ipv6 ospf max-metric

This command displays the configured maximum metrics for stub-router mode.

Format `show ipv6 ospf max-metric`

Modes
- Privileged EXEC
- User EXEC

Example: The following shows an example of the command.

```
(config)#show ipv6 ospf max-metric
OSPFv3 Router with ID (3.3.3.3)
 Start time: 00:00:00, Time elapsed: 00:01:05
 Originating router-LSAs with maximum metric
    Condition: on startup for 1000 seconds, State: inactive
    Advertise external-LSAs with metric 16711680
```

8.4.5.12 show ipv6 ospf neighbor

This command displays information about OSPF neighbors. If you do not specify a neighbor IP address, the output displays summary information in a table. If you specify an interface or tunnel, only the information for that interface or tunnel displays. The argument `slot/port` corresponds to a physical routing interface or VLAN routing interface. The keyword `vlan` is used to specify the VLAN ID of the routing VLAN directly instead of a *slot/port* format. The *`ip-address`* is the IP address of the neighbor, and when you specify this, detailed information about the neighbor displays. The information below only displays if OSPF is enabled and the interface has a neighbor.

Format `show ipv6 ospf neighbor [interface {slot/port|vlan 1-4093|tunnel tunnel_id}][ip-address]`

Modes
- Privileged EXEC
- User EXEC

If you do not specify an IP address, a table with the following columns displays for all neighbors or the neighbor associated with the interface that you specify:

Term	Definition
Router ID	The 4-digit dotted-decimal number of the neighbor router.
Priority	The OSPF priority for the specified interface. The priority of an interface is a priority integer from 0 to 255. A value of '0' indicates that the router is not eligible to become the designated router on this network.
Intf ID	The interface ID of the neighbor.
Interface	The interface of the local router.
State	The state of the neighboring routers. Possible values are: ■ Down- initial state of the neighbor conversation - no recent information has been received from the neighbor. ■ Attempt - no recent information has been received from the neighbor but a more concerted effort should be made to contact the neighbor. ■ Init - an Hello packet has recently been seen from the neighbor, but bidirectional communication has not yet been established. ■ 2 way - communication between the two routers is bidirectional. ■ Exchange start - the first step in creating an adjacency between the two neighboring routers, the goal is to decide which router is the master and to decide upon the initial DD sequence number. ■ Exchange - the router is describing its entire link state database by sending Database Description packets to the neighbor. ■ Full - the neighboring routers are fully adjacent and they will now appear in router-LSAs and network-LSAs.
Dead Time	The amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.
Restart Helper Status	Indicates the status of this router as a helper during a graceful restart of the router specified in the command line: ■ Helping—This router is acting as a helpful neighbor to the specified router. ■ Not Helping—This router is not a helpful neighbor at this time.
Restart Reason	When this router is in helpful neighbor mode, this indicates the reason for the restart as provided by the restarting router.
Remaining Grace Time	The number of seconds remaining the in current graceful restart interval. This is displayed only when this router is currently acting as a helpful neighbor for the router specified in the command.
Restart Helper Exit Reason	Indicates the reason that the specified router last exited a graceful restart. ■ None—Graceful restart has not been attempted ■ In Progress—Restart is in progress ■ Completed—The previous graceful restart completed successfully ■ Timed Out—The previous graceful restart timed out ■ Topology Changed—The previous graceful restart terminated prematurely because of a topology change

If you specify an IP address for the neighbor router, the following fields display:

Term	Definition
Interface	The interface of the local router.
Area ID	The area ID associated with the interface.
Options	An integer value that indicates the optional OSPF capabilities supported by the neighbor. These are listed in its Hello packets. This enables received Hello Packets to be rejected (i.e., neighbor relationships will not even start to form) if there is a mismatch in certain crucial OSPF capabilities.

Term	Definition
Router Priority	The router priority for the specified interface.
Dead Timer Due	The amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.
State	The state of the neighboring routers.
Events	Number of times this neighbor relationship has changed state, or an error has occurred.
Retransmission Queue Length	An integer representing the current length of the retransmission queue of the specified neighbor router Id of the specified interface.

8.4.5.13 show ipv6 ospf range

This command displays the set of OSPFv3 area ranges configured for a given area.

Format `show ipv6 ospf range` *areaid*

Modes Privileged EXEC

Term	Definition
Area ID	The area whose prefixes are summarized.
IPv6 Prefix/Prefix Length	The summary prefix and prefix length.
Type	**S** (Summary Link) or **E** (External Link)
Action	**Enabled** or **Disabled**
Cost	Metric to be advertised when the range is active.

8.4.5.14 show ipv6 ospf statistics

This command displays information about the 15 most recent Shortest Path First (SPF) calculations. SPF is the OSPF routing table calculation.

Format `show ipv6 ospf statistics`

Modes
- Privileged EXEC
- User EXEC

The command displays the following information with the most recent statistics displayed at the end of the table.

Term	Definition
Delta T	The time since the routing table was computed. The time is in the format hours, minutes, and seconds (hh:mm:ss).
Intra	The time taken to compute intra-area routes, in milliseconds.
Summ	The time taken to compute inter-area routes, in milliseconds.
Ext	The time taken to compute external routes, in milliseconds.
SPF Total	The total time taken to compute routes, in milliseconds. The total may exceed the sum of Intra, Summ, and Ext times.
RIB Update	The time from the completion of the routing table calculation until all changes have been made in the common routing table [the Routing Information Base (RIB)], in milliseconds

Term	Definition
Reason	The event or events that triggered the SPF. The reason codes are as follows: ■ R: New router LSA ■ N: New network LSA ■ SN: New network (inter-area prefix) summary LSA ■ SA: New ASBR (inter-area router) summary LSA ■ X: New external LSA ■ IP: New intra-area prefix LSA ■ L: New Link LSA

Example: The following shows example CLI display output for the command.

```
(Routing) #show ipv6 ospf statistics

 Area 0.0.0.0: SPF algorithm executed 10 times

Delta T         Intra       Summ        Ext    SPF Total   RIB Update  Reason

23:32:46            0          0          0            0            0   R, IP
23:32:09            0          0          0            0            0   R, N, IP
23:32:04            0          0          0            0            0   R
23:31:44            0          0          0            0            0   R, N, IP
23:31:39            0          0          0            0            1   R
23:29:57            0          3          7           10          131   R
23:29:52            0         14         29           43          568   SN
04:07:23            0          9         23           33          117   SN
04:07:23            0          9         23           33          117   SN
04:07:18            0          0          0            1          485   SN
04:07:14            0          1          0            1            3    X
```

8.4.5.15 show ipv6 ospf stub table

This command displays the OSPF stub table. The information below will only be displayed if OSPF is initialized on the switch.

Format `show ipv6 ospf stub table`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Area ID	A 32-bit identifier for the created stub area.
Type of Service	Type of service associated with the stub metric. For this release, Normal TOS is the only supported type.
Metric Val	The metric value is applied based on the TOS. It defaults to the least metric of the type of service among the interfaces to other areas. The OSPF cost for a route is a function of the metric value.
Import Summary LSA	Controls the import of summary LSAs into stub areas.

8.4.5.16 show ipv6 ospf virtual-link

This command displays the OSPF Virtual Interface information for a specific area and neighbor. The *areaid* parameter identifies the area and the *neighbor* parameter identifies the neighbor's Router ID.

Format `show ipv6 ospf virtual-link` *areaid neighbor*

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Area ID	The area id of the requested OSPF area.
Neighbor Router ID	The input neighbor Router ID.
Hello Interval	The configured hello interval for the OSPF virtual interface.
Dead Interval	The configured dead interval for the OSPF virtual interface.
Interface Transmit Delay	The configured transmit delay for the OSPF virtual interface.
Retransmit Interval	The configured retransmit interval for the OSPF virtual interface.
Authentication Type	The type of authentication the interface performs on LSAs it receives.
State	The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router. This is the state of the OSPF interface.
Neighbor State	The neighbor state.

8.4.5.17 show ipv6 ospf virtual-link brief

This command displays the OSPFV3 Virtual Interface information for all areas in the system.

Format `show ipv6 ospf virtual-link brief`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Area ID	The area id of the requested OSPFV3 area.
Neighbor	The neighbor interface of the OSPFV3 virtual interface.
Hello Interval	The configured hello interval for the OSPFV3 virtual interface.
Dead Interval	The configured dead interval for the OSPFV3 virtual interface.
Retransmit Interval	The configured retransmit interval for the OSPFV3 virtual interface.
Transmit Delay	The configured transmit delay for the OSPFV3 virtual interface.

8.5 DHCPv6 Commands

This section describes the commands you use to configure the DHCPv6 server on the system and to view DHCPv6 information.

8.5.0.1 ipv6 dhcp client pd

Use this command to enable the Dynamic Host Configuration Protocol (DHCP) for IPv6 client process (if the process is not currently running) and to enable requests for prefix delegation through a specified interface. When prefix delegation is enabled and a prefix is successfully acquired, the prefix is stored in the IPv6 general prefix pool with an internal name defined by the automatic argument.

NOTE: The Prefix Delegation client is supported on only one IP interface.

rapid-commit enables the use of a two-message exchange method for prefix delegation and other configuration. If enabled, the client includes the rapid commit option in a solicit message.

The DHCP for IPv6 client, server, and relay functions are mutually exclusive on an interface. If one of these functions is already enabled and a user tries to configure a different function on the same interface, a message is displayed.

Default	Prefix delegation is disabled on an interface.
Format	`ipv6 dhcp client pd [rapid-commit]`
Mode	Interface Config

Example: The following examples enable prefix delegation on interface 0/1:

```
(Switch) #configure
(Switch) (Config)#interface 0/1
(Switch) (Interface 0/1)# ipv6 dhcp client pd

(Switch) #configure
(Switch) (Config)#interface 0/1
(Switch) (Interface 0/1)# ipv6 dhcp client pd rapid-commit
```

8.5.0.1.1 no ipv6 dhcp client pd

This command disables requests for prefix delegation.

Format	`no ipv6 dhcp client pd`
Mode	Interface Config

8.5.0.2 ipv6 dhcp conflict logging

This command enables/disables the logging of the bindings reported to be conflicting by the DHCPv6 Clients via DECLINE messages.

Default	Enabled
Format	`ipv6 dhcp conflict logging`
Mode	Global Config

Example:

```
(switch) #configure
(switch) (Config)# ipv6 dhcp conflict logging
```

8.5.0.3 ipv6 dhcp server

Use this command to configure DHCPv6 server functionality on an interface or range of interfaces. The *pool-name* is the DHCPv6 pool containing stateless and/or prefix delegation parameters, *automatic* enables the server to automatically determine which pool to use when allocating addresses for a client, *rapid-commit* is an option that allows for an abbreviated exchange between the client and server, and *pref-value* is a value used by clients to determine preference between multiple DHCPv6 servers. For a particular interface, DHCPv6 server and DHCPv6 relay functions are mutually exclusive.

Format `ipv6 dhcp server {`*pool-name* `| automatic}[rapid-commit] [preference` *pref-value*`]`

Mode Interface Config

8.5.0.4 ipv6 dhcp relay destination

Use this command to configure an interface for DHCPv6 relay functionality on an interface or range of interfaces. Use the *destination* keyword to set the relay server IPv6 address. The *relay-address* parameter is an IPv6 address of a DHCPv6 relay server. Use the *interface* keyword to set the relay server interface. The *relay-interface* parameter is an interface (*slot/port*) to reach a relay server. Multiple relay addresses can be configured on an interface.The optional *remote-id* is the Relay Agent Information Option “remote ID” suboption to be added to relayed messages.This can either be the special keyword *duid-ifid*, which causes the “remote ID” to be derived from the DHCPv6 server DUID and the relay interface number, or it can be specified as a user-defined string.

NOTE: If *relay-address* is an IPv6 global address, then *relay-interface* is not required. If *relay-address* is a link-local or multicast address, then *relay-interface* is required. Finally, if you do not specify a value for *relay-address*, then you must specify a value for *relay-interface* and the DHCPV6-ALL-AGENTS multicast address (i.e. `FF02::1:2`) is used to relay DHCPv6 messages to the relay server.

Format `ipv6 dhcp relay {destination [`*relay-address*`] interface [`*relay-interface*`]| interface [`*relay-interface*`]} [remote-id (`*duid-ifid* `| user-defined-string)]`

Mode Interface Config

8.5.0.5 ipv6 dhcp relay remote-id

This command configures the relay agent information option *remote ID* sub-option to be added to the DHCPv6 relayed messages. This can either be the special keyword `duid-ifid`, which causes the remote ID to be derived from the DHCPv6 Server DUID and the relay interface number, or it can be specified as a user-defined string.

Default None configured

Format `ipv6 dhcp relay remote-id {`*duid-ifid* `| user-defined-string)]`

Mode Interface Config

8.5.0.5.1 no ipv6 dhcp relay remote-id

This command resets the relay agent information option *remote ID* sub-option to be added to the DHCPv6 relayed messages to the default value.

\

Default None configured

Format `no ipv6 dhcp relay remote-id {duid-ifid | user-defined-string)]`
Mode Interface Config

8.5.0.6 ipv6 dhcp pool

Use this command from Global Config mode to enter IPv6 DHCP Pool Config mode. Use the `exit` command to return to Global Config mode. To return to the User EXEC mode, enter CTRL+Z. The *pool-name* should be less than 31 alpha-numeric characters. DHCPv6 pools are used to specify information for DHCPv6 server to distribute to DHCPv6 clients. These pools are shared between multiple interfaces over which DHCPv6 server capabilities are configured.

Once the DHCP for IPv6 configuration information pool has been created, use the `ipv6 dhcp server` command to associate the pool with a server on an interface. If you do not configure an information pool, use the `ipv6 dhcp server interface` configuration command to enable the DHCPv6 server function on an interface.

When you associate a DHCPv6 pool with an interface, only that pool services requests on the associated interface. The pool also services other interfaces. If you do not associate a DHCPv6 pool with an interface, it can service requests on any interface. Not using any IPv6 address prefix means that the pool returns only configured options.

Format `ipv6 dhcp pool pool-name`
Mode Global Config

8.5.0.6.1 no ipv6 dhcp pool

This command removes the specified DHCPv6 pool.

Format `no ipv6 dhcp pool pool-name`
Mode Global Config

8.5.0.7 address prefix (IPv6)

Use this command to sets an address prefix for address assignment. This address must be in hexadecimal, using 16-bit values between colons.

If `lifetime` values are not configured, the default lifetime values for *valid-lifetime* and *preferred-lifetime* are considered to be infinite.

Format `address prefix ipv6-prefix [lifetime {valid-lifetime preferred-lifetime | infinite}]`
Mode IPv6 DHCP Pool Config

Term	Definition
lifetime	(Optional) Sets a length of time for the hosts to remember router advertisements. If configured, both valid and preferred lifetimes must be configured.
valid-lifetime	The amount of time, in seconds, the prefix remains valid for the requesting router to use. The range is from 60 through 4294967294. The *preferred-lifetime* value cannot exceed the *valid-lifetime* value.
preferred-lifetime	The amount of time, in seconds, that the prefix remains preferred for the requesting router to use. The range is from 60 through 4294967294. The *preferred-lifetime* value cannot exceed the *valid-lifetime* value.
infinite	An unlimited lifetime.

Example: The following example shows how to configure an IPv6 address prefix for the IPv6 configuration pool *pool1*:

```
(Switch) #configure
(Switch) (Config)# ipv6 dhcp pool pool1
(Switch) (Config-dhcp6s-pool)# address prefix 2001::/64
(Switch) (Config-dhcp6s-pool)# exit
```

8.5.0.8 domain-name (IPv6)

This command sets the DNS domain name which is provided to DHCPv6 client by DHCPv6 server. DNS domain name is configured for stateless server support. Domain name consist of no more than 31 alpha-numeric characters. DHCPv6 pool can have multiple number of domain names with maximum of 8.

Format `domain-name` *`domain`*

Mode IPv6 DHCP Pool Config

8.5.0.8.1 no domain-name

This command will remove dhcpv6 domain name from dhcpv6 pool.

Format `no domain-name` *`dns-domain-name`*

Mode IPv6 DHCP Pool Config

8.5.0.9 dns-server (IPv6)

This command sets the ipv6 DNS server address which is provided to dhcpv6 client by dhcpv6 server. DNS server address is configured for stateless server support. DHCPv6 pool can have multiple number of domain names with a maximum of 8.

Format `dns-server` *`ipv6-address`*

Mode IPv6 DHCP Pool Config

8.5.0.9.1 no dns-server

This command will remove DHCPv6 server address from DHCPv6 server.

Format `no dns-server` *`dns-server-address`*

Mode IPv6 DHCP Pool Config

8.5.0.10 prefix-delegation (IPv6)

Multiple IPv6 prefixes can be defined within a pool for distributing to specific DHCPv6 Prefix delegation clients. Prefix is the delegated IPv6 prefix. DUID is the client's unique DUID value (Example: 00:01:00:09:f8:79:4e:00:04:76:73:43:76'). Name is 31 characters textual client’s name which is useful for logging or tracing only. Valid lifetime is the valid lifetime for the delegated prefix in seconds and preferred lifetime is the preferred lifetime for the delegated prefix in seconds.

Default
- valid-lifetime—2592000
- preferred-lifetime—604800

Format `prefix-delegation` *`prefix/prefixlength`* `client-`*`DUID`* `[name` *`client-name`*`][prefer-lifetime` *`0-4294967295`*`|infinite][valid-lifetime` *`0-4294967295`*`|infinite]`

Mode IPv6 DHCP Pool Config

8.5.0.10.1 no prefix-delegation

This command deletes a specific prefix-delegation client.

Format `no prefix-delegation` *`prefix/prefix-delegation DUID`*
Mode IPv6 DHCP Pool Config

8.5.0.11 show ipv6 dhcp

This command displays the DHCPv6 server name, status, and conflict logging status.

Format `show ipv6 dhcp`
Mode Privileged EXEC

Term	Definition
DHCPv6 is Enabled (Disabled)	The status of the DHCPv6 server.
DHCPv6 Conflict Logging Mode	Indicates whether DHCPv6 Conflict Logging is enabled or disabled.
Server DUID	If configured, shows the DHCPv6 unique identifier.

Example:

```
(switch) #show ipv6 dhcp

DHCPv6 is enabled
DHCPv6 Conflict Logging Mode is enabled
Server DUID: 00:01:00:06:a5:e6:dc:bb:f8:b1:56:29:fc:2c
```

8.5.0.12 show ipv6 dhcp statistics

This command displays the IPv6 DHCP statistics for all interfaces.

Format `show ipv6 dhcp statistics`
Mode Privileged EXEC

Term	Definition
DHCPv6 Solicit Packets Received	Number of solicit received statistics.
DHCPv6 Request Packets Received	Number of request received statistics.
DHCPv6 Confirm Packets Received	Number of confirm received statistics.
DHCPv6 Renew Packets Received	Number of renew received statistics.
DHCPv6 Rebind Packets Received	Number of rebind received statistics.
DHCPv6 Release Packets Received	Number of release received statistics.
DHCPv6 Decline Packets Received	Number of decline received statistics.
DHCPv6 Inform Packets Received	Number of inform received statistics.
DHCPv6 Relay-forward Packets Received	Number of relay forward received statistics.
DHCPv6 Relay-reply Packets Received	Number of relay-reply received statistics.
DHCPv6 Malformed Packets Received	Number of malformed packets statistics.
Received DHCPv6 Packets Discarded	Number of DHCP discarded statistics.

Term	Definition
Total DHCPv6 Packets Received	Total number of DHCPv6 received statistics
DHCPv6 Advertisement Packets Transmitted	Number of advertise sent statistics.
DHCPv6 Reply Packets Transmitted	Number of reply sent statistics.
DHCPv6 Reconfig Packets Transmitted	Number of reconfigure sent statistics.
DHCPv6 Relay-reply Packets Transmitted	Number of relay-reply sent statistics.
DHCPv6 Relay-forward Packets Transmitted	Number of relay-forward sent statistics.
Total DHCPv6 Packets Transmitted	Total number of DHCPv6 sent statistics.

8.5.0.13 show ipv6 dhcp interface

This command displays DHCPv6 information for all relevant interfaces or the specified interface. The argument `slot/port` corresponds to a physical routing interface or VLAN routing interface. The keyword **vlan** is used to specify the VLAN ID of the routing VLAN directly instead of a *slot/port* format. If you specify an interface, you can use the optional `statistics` parameter to view statistics for the specified interface.

Format `show ipv6 dhcp interface {slot/port|vlan 1-4093} [statistics]`

Mode Privileged EXEC

Term	Definition
IPv6 Interface	The interface name in *slot/port* format.
Mode	Shows whether the interface is a IPv6 DHCP relay or server.

If the interface mode is server, the following information displays.

Term	Definition
Pool Name	The pool name specifying information for DHCPv6 server distribution to DHCPv6 clients.
Server Preference	The preference of the server.
Option Flags	Shows whether rapid commit is enabled.

If the interface mode is relay, the following information displays.

Term	Definition
Relay Address	The IPv6 address of the relay server.
Relay Interface Number	The relay server interface in *slot/port* format.
Relay Remote ID	If configured, shows the name of the relay remote.
Option Flags	Shows whether rapid commit is configured.

If you use the statistics parameter, the command displays the IPv6 DHCP statistics for the specified interface. See Section 8.5.0.12, show ipv6 dhcp statistics for information about the output.

8.5.0.14 show ipv6 dhcp binding

This command displays configured DHCP pool.

Format `show ipv6 dhcp binding` *`[ipv6-address]`*

Mode Privileged EXEC

Term	Definition
DHCP Client Address	Address of DHCP Client.
DUID	String that represents the Client DUID.
IAID	Identity Association ID.
Prefix/Prefix Length	IPv6 address and mask length for delegated prefix.
Prefix Type	IPV6 Prefix type (IAPD, IANA, or IATA).
Client Address	Address of DHCP Client.
Client Interface	IPv6 Address of DHCP Client.
Expiration	Address of DNS server address.
Valid Lifetime	Valid lifetime in seconds for delegated prefix.
Preferred Lifetime	Preferred lifetime in seconds for delegated prefix.

8.5.0.15 show ipv6 dhcp conflict

This command displays the conflict bindings in the DHCPv6 server that are created when the leased bindings are declined by DHCPv6 clients. Passing an optional ipv6-address argument displays the details about the specific conflict binding corresponding to that IPv6 address.

Format `show ipv6 dhcp conflict [`*`ipv6-address`*`]`

Mode Privileged EXEC

Example:

```
(switch) #show ipv6 dhcp conflict


Pool Name..................................... STATEFUL
Prefix........................................ 2001::/64
Conflict Bindings............................. 2001::2
.......... ................................... 2001::3
```

8.5.0.16 show ipv6 dhcp pool

This command displays configured DHCP pool.

Format `show ipv6 dhcp pool` *`pool-name`*

Mode Privileged EXEC

Term	Definition
DHCP Pool Name	Unique pool name configuration.
Client DUID	Client's DHCP unique identifier. DUID is generated using the combination of the local system burned-in MAC address and a timestamp value.
Host	Name of the client.

Term	Definition
Prefix/Prefix Length	IPv6 address and mask length for delegated prefix.
Preferred Lifetime	Preferred lifetime in seconds for delegated prefix.
Valid Lifetime	Valid lifetime in seconds for delegated prefix.
DNS Server Address	Address of DNS server address.
Domain Name	DNS domain name.

8.5.0.17 show network ipv6 dhcp statistics

This command displays the statistics of the DHCPv6 client running on the network management interface.

Format `show network ipv6 dhcp statistics`

Mode
- Privileged EXEC
- User EXEC

Field	Description
DHCPv6 Advertisement Packets Received	The number of DHCPv6 Advertisement packets received on the network interface.
DHCPv6 Reply Packets Received	The number of DHCPv6 Reply packets received on the network interface.
Received DHCPv6 Advertisement Packets Discarded	The number of DHCPv6 Advertisement packets discarded on the network interface.
Received DHCPv6 Reply Packets Discarded	The number of DHCPv6 Reply packets discarded on the network interface.
DHCPv6 Malformed Packets Received	The number of DHCPv6 packets that are received malformed on the network interface.
Total DHCPv6 Packets Received	The total number of DHCPv6 packets received on the network interface.
DHCPv6 Solicit Packets Transmitted	The number of DHCPv6 Solicit packets transmitted on the network interface.
DHCPv6 Request Packets Transmitted	The number of DHCPv6 Request packets transmitted on the network interface.
DHCPv6 Renew Packets Transmitted	The number of DHCPv6 Renew packets transmitted on the network interface.
DHCPv6 Rebind Packets Transmitted	The number of DHCPv6 Rebind packets transmitted on the network interface.
DHCPv6 Release Packets Transmitted	The number of DHCPv6 Release packets transmitted on the network interface.
Total DHCPv6 Packets Transmitted	The total number of DHCPv6 packets transmitted on the network interface.

Example: The following shows example CLI display output for the command.

```
(Switching)#show network ipv6 dhcp statistics
DHCPv6 Client Statistics
------------------------

DHCPv6 Advertisement Packets Received.............. 0
```

```
DHCPv6 Reply Packets Received..................... 0
Received DHCPv6 Advertisement Packets Discarded..... 0
Received DHCPv6 Reply Packets Discarded............. 0
DHCPv6 Malformed Packets Received................... 0
Total DHCPv6 Packets Received....................... 0

DHCPv6 Solicit Packets Transmitted.................. 0
DHCPv6 Request Packets Transmitted.................. 0
DHCPv6 Renew Packets Transmitted.................... 0
DHCPv6 Rebind Packets Transmitted................... 0
DHCPv6 Release Packets Transmitted.................. 0
Total DHCPv6 Packets Transmitted.................... 0
```

8.5.0.18 show serviceport ipv6 dhcp statistics

This command displays the statistics of the DHCPv6 client running on the serviceport management interface.

Format `show serviceport ipv6 dhcp statistics`

Mode
- Privileged EXEC
- User EXEC

Field	Description
DHCPv6 Advertisement Packets Received	The number of DHCPv6 Advertisement packets received on the service port interface.
DHCPv6 Reply Packets Received	The number of DHCPv6 Reply packets received on the service port interface.
Received DHCPv6 Advertisement Packets Discarded	The number of DHCPv6 Advertisement packets discarded on the service port interface.
Received DHCPv6 Reply Packets Discarded	The number of DHCPv6 Reply packets discarded on the service port interface.
DHCPv6 Malformed Packets Received	The number of DHCPv6 packets that are received malformed on the service port interface.
Total DHCPv6 Packets Received	The total number of DHCPv6 packets received on the service port interface.
DHCPv6 Solicit Packets Transmitted	The number of DHCPv6 Solicit packets transmitted on the service port interface.
DHCPv6 Request Packets Transmitted	The number of DHCPv6 Request packets transmitted on the service port interface.
DHCPv6 Renew Packets Transmitted	The number of DHCPv6 Renew packets transmitted on the service port interface.
DHCPv6 Rebind Packets Transmitted	The number of DHCPv6 Rebind packets transmitted on the service port interface.
DHCPv6 Release Packets Transmitted	The number of DHCPv6 Release packets transmitted on the service port interface.
Total DHCPv6 Packets Transmitted	The total number of DHCPv6 packets transmitted on the service port interface.

Example: The following shows example CLI display output for the command.

```
(Switching)#show serviceport ipv6 dhcp statistics
DHCPv6 Client Statistics
------------------------
DHCPv6 Advertisement Packets Received.............. 0
DHCPv6 Reply Packets Received...................... 0
Received DHCPv6 Advertisement Packets Discarded..... 0
Received DHCPv6 Reply Packets Discarded............. 0
DHCPv6 Malformed Packets Received................... 0
Total DHCPv6 Packets Received....................... 0

DHCPv6 Solicit Packets Transmitted.................. 0
DHCPv6 Request Packets Transmitted.................. 0
```

```
DHCPv6 Renew Packets Transmitted..................... 0
DHCPv6 Rebind Packets Transmitted.................... 0
DHCPv6 Release Packets Transmitted................... 0
Total DHCPv6 Packets Transmitted..................... 0
```

8.5.0.19 clear ipv6 dhcp

Use this command to clear DHCPv6 statistics for all interfaces or for a specific interface. Use the *slot/port* parameter to specify an interface and the vlan parameter to specify a VLAN.

Format `clear ipv6 dhcp {statistics | interface {slot/port | vlan id} }`

Mode Privileged EXEC

8.5.0.20 clear ipv6 dhcp binding

This command deletes an automatic address binding from the DHCP server database. *address* is a valid IPv6 address.

A binding table entry on the DHCP for IPv6 server is automatically:

- Created whenever a prefix is delegated to a client from the configuration pool.
- Updated when the client renews, rebinds, or confirms the prefix delegation.
- Deleted when the client releases all the prefixes in the binding voluntarily, all prefixes' valid lifetimes have expired, or an administrator runs the **clear ipv6 dhcp binding** command.

If the `clear ipv6 dhcp binding` command is used with the optional *ipv6-address* argument specified, only the binding for the specified client is deleted. If the `clear ipv6 dhcp binding` command is used without the *ipv6-address* argument, all automatic client bindings are deleted from the DHCP for IPv6 binding table.

Format `clear ipv6 dhcp binding [ipv6-address]`

Mode Privileged EXEC

8.5.0.21 clear ipv6 dhcp conflict

This command deletes the DHCPv6 Client conflict binding(s) that represent the address (es) declined by DHCPv6 Clients.

Format `clear ipv6 dhcp conflict { ipv6-address | * }`

Mode Privileged EXEC

Syntax	Description
ipv6-address	The conflicting address declined by a DHCPv6 Client.
*	Indicates all conflicting addresses in the database.

Usage Guidelines

The `clear ipv6 dhcp` conflict command is used as a server function.

A conflict binding entry is created by the DHCPv6 server whenever an advertised lease binding is declined by a DHCPv6 client.

If the `clear ipv6 dhcp` conflict command is used with the optional `ipv6-address` argument specified, only that specific conflict binding is deleted. If the `clear ipv6 dhcp conflict *` command is used without the `ipv6-address` argument, then all conflict client bindings are deleted.

Example:

```
(switch) # clear ipv6 dhcp conflict 2003:1::2
(switch) # clear ipv6 dhcp conflict *
```

8.5.0.22 clear network ipv6 dhcp statistics

Use this command to clear the DHCPv6 statistics *on the network management* interface.

Format `clear network ipv6 dhcp statistics`

Mode
- Privileged EXEC

8.5.0.23 clear serviceport ipv6 dhcp statistics

Use this command to clear the DHCPv6 client statistics *on the service port* interface.

Format `clear serviceport ipv6 dhcp statistics`

Mode
- Privileged EXEC

8.6 DHCPv6 Snooping Configuration Commands

This section describes commands you use to configure IPv6 DHCP Snooping.

8.6.0.1 ipv6 dhcp snooping

Use this command to globally enable IPv6 DHCP Snooping.

Default	disabled
Format	`ipv6 dhcp snooping`
Mode	Global Config

8.6.0.1.1 no ipv6 dhcp snooping

Use this command to globally disable IPv6 DHCP Snooping.

Format	`no ipv6 dhcp snooping`
Mode	Global Config

8.6.0.2 ipv6 dhcp snooping vlan

Use this command to enable DHCP Snooping on a list of comma-separated VLAN ranges.

Default	disabled
Format	`ipv6 dhcp snooping vlan` *`vlan-list`*
Mode	Global Config

8.6.0.2.1 no ipv6 dhcp snooping vlan

Use this command to disable DHCP Snooping on VLANs.

Format	`no ipv6 dhcp snooping vlan` *`vlan-list`*
Mode	Global Config

8.6.0.3 ipv6 dhcp snooping verify mac-address

Use this command to enable verification of the source MAC address with the client hardware address in the received DCHP message.

Default	enabled
Format	`ipv6 dhcp snooping verify mac-address`
Mode	Global Config

8.6.0.3.1 no ipv6 dhcp snooping verify mac-address

Use this command to disable verification of the source MAC address with the client hardware address.

Format	`no ipv6 dhcp snooping verify mac-address`

Mode Global Config

8.6.0.4 ipv6 dhcp snooping database

Use this command to configure the persistent location of the DHCP Snooping database. This can be local or a remote file on a given IP machine.

Default local

Format `ipv6 dhcp snooping database {local|tftp://hostIP/filename}`

Mode Global Config

8.6.0.5 ipv6 dhcp snooping database write-delay

Use this command to configure the interval in seconds at which the DHCP Snooping database is persisted. The interval value ranges from 15 to 86400 seconds.

Default 300 seconds

Format `ipv6 dhcp snooping database write-delay` *`interval`*

Mode Global Config

8.6.0.5.1 no ip dhcp snooping database write-delay

Use this command to set the write delay value to the default value.

Format `no ip dhcp snooping database write-delay`

Mode Global Config

8.6.0.6 ipv6 dhcp snooping binding

Use this command to configure static DHCP Snooping binding.

Format `ipv6 dhcp snooping binding` *`macaddr`* `vlan` *`1-4093 ip address`* `interface` *`interface id`*

Mode Global Config

8.6.0.6.1 no ipv6 dhcp snooping binding

Use this command to remove the DHCP static entry from the DHCP Snooping database.

Format `no ipv6 dhcp snooping binding` *`mac-address`*

Mode Global Config

8.6.0.7 ipv6 dhcp snooping trust

Use this command to configure an interface or range of interfaces as trusted.

Default disabled

Format `ipv6 dhcp snooping trust`

Mode Interface Config

8.6.0.7.1 no ipv6 dhcp snooping trust

Use this command to configure the port as untrusted.

Format `no ipv6 dhcp snooping trust`
Mode Interface Config

8.6.0.8 ipv6 dhcp snooping log-invalid

Use this command to control the logging DHCP messages filtration by the DHCP Snooping application. This command can be used to configure a single interface or a range of interfaces.

Default disabled
Format `ipv6 dhcp snooping log-invalid`
Mode Interface Config

8.6.0.8.1 no ipv6 dhcp snooping log-invalid

Use this command to disable the logging DHCP messages filtration by the DHCP Snooping application.

Format `no ipv6 dhcp snooping log-invalid`
Mode Interface Config

8.6.0.9 ipv6 dhcp snooping limit

Use this command to control the rate at which the DHCP Snooping messages come on an interface or range of interfaces. By default, rate limiting is disabled. When enabled, the rate can range from 0 to 300 packets per second. The burst level range is 1 to 15 seconds. Rate limiting is configured on a physical port and may be applied to trusted and untrusted ports.

Default disabled (no limit)
Format `ipv6 dhcp snooping limit {rate` *`0-300`* `[`*`burst interval seconds`*`]}`
Mode Interface Config

8.6.0.9.1 no ipv6 dhcp snooping limit

Use this command to set the rate at which the DHCP Snooping messages come, and the burst level, to the defaults.

Format `no ipv6 dhcp snooping limit`
Mode Interface Config

8.6.0.10 ipv6 verify source

Use this command to configure the IPv6SG source ID attribute to filter the data traffic in the hardware. Source ID is the combination of IP address and MAC address. Normal command allows data traffic filtration based on the IP address. With the “port-security” option, the data traffic is filtered based on the IP and MAC addresses.

This command can be used to configure a single interface or a range of interfaces.

Default `the source ID is the IP address`
Format `ipv6 verify source {port-security}`
Mode Interface Config

8.6.0.10.1 no ipv6 verify source

Use this command to disable the IPv6SG configuration in the hardware. You cannot disable port-security alone if it is configured.

Format `no ipv6 verify source`
Mode Interface Config

8.6.0.11 ipv6 verify binding

Use this command to configure static IPv6 source guard (IPv6SG) entries.

Format `ipv6 verify binding` *`mac-address`* `vlan` *`vlan id ipv6 address`* `interface` *`interface id`*
Mode Global Config

8.6.0.11.1 no ipv6 verify binding

Use this command to remove the IPv6SG static entry from the IPv6SG database.

Format `no ipv6 verify binding` *`mac-address`* `vlan` *`vlan id ipv6 address`* `interface` *`interface id`*
Mode Global Config

8.6.0.12 show ipv6 dhcp snooping

Use this command to display the DHCP Snooping global configurations and per port configurations.

Format `show ipv6 dhcp snooping`
Mode
- Privileged EXEC
- User EXEC

Term	Definition
Interface	The interface for which data is displayed.
Trusted	If it is enabled, DHCP snooping considers the port as trusted. The factory default is disabled.
Log Invalid Pkts	If it is enabled, DHCP snooping application logs invalid packets on the specified interface.

Example: The following shows example CLI display output for the command.

```
(switch) #show ipv6 dhcp snooping

DHCP snooping is Disabled
DHCP snooping source MAC verification is enabled
DHCP snooping is enabled on the following VLANs:
```

```
11 - 30, 40

Interface   Trusted    Log Invalid Pkts
---------   --------   ----------------
0/1          Yes             No
0/2          No             Yes
0/3          No             Yes
0/4          No              No
0/6          No              No
```

8.6.0.13 show ipv6 dhcp snooping binding

Use this command to display the DHCP Snooping binding entries. To restrict the output, use the following options:

- Dynamic: Restrict the output based on DCHP snooping.
- Interface: Restrict the output based on a specific interface.
- Static: Restrict the output based on static entries.
- VLAN: Restrict the output based on VLAN.

Format `show ipv6 dhcp snooping binding [{static/dynamic}] [interface` ***slot/port*** `] [vlan` ***1-4093*** `]`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
MAC Address	Displays the MAC address for the binding that was added. The MAC address is the key to the binding database.
IPv6 Address	Displays the valid IPv6 address for the binding rule.
VLAN	The VLAN for the binding rule.
Interface	The interface to add a binding into the DHCP snooping interface.
Type	Binding type; statically configured from the CLI or dynamically learned.
Lease (sec)	The remaining lease time for the entry.

Example: The following shows example CLI display output for the command.

```
(switch) #show ipv6 dhcp snooping binding

Total number of bindings: 2

MAC Address          IPv6 Address  VLAN  Interface  Type  Lease time (Secs)
-----------------  -------------- ----  ---------  ---- ------------------
00:02:B3:06:60:80   2000::1/64     10    0/1             86400
00:0F:FE:00:13:04   3000::1/64     10    0/1             86400
```

8.6.0.14 show ipv6 dhcp snooping database

Use this command to display the DHCP Snooping configuration related to the database persistency.

Format `show ipv6 dhcp snooping database`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Agent URL	Bindings database agent URL.
Write Delay	The maximum write time to write the database into local or remote.

Example: The following shows example CLI display output for the command.

```
(switch) #show ipv6 dhcp snooping database

agent url:  /10.131.13.79:/sai1.txt

write-delay:  5000
```

8.6.0.15 show ipv6 dhcp snooping interfaces

Use this command to show the DHCP Snooping status of all interfaces or a specified interface.

Format `show ipv6 dhcp snooping interfaces [interface` *`slot/port`*`]`

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(switch) #show ipv6 dhcp snooping interfaces

 Interface    Trust State  Rate Limit    Burst Interval
                              (pps)       (seconds)
-----------   ----------   ----------   --------------
   1/g1            No           15              1
   1/g2            No           15              1
   1/g3            No           15              1

(switch) #show ip dhcp snooping interfaces ethernet 0/1

 Interface    Trust State  Rate Limit    Burst Interval
                              (pps)       (seconds)
-----------   ----------   ----------   --------------
   0/1             Yes          15              1
```

8.6.0.16 show ipv6 dhcp snooping statistics

Use this command to list statistics for IPv6 DHCP Snooping security violations on untrusted ports.

Format `show ipv6 dhcp snooping statistics`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Interface	The IPv6 address of the interface in *`slot/port`* format.
MAC Verify Failures	Represents the number of DHCP messages that were filtered on an untrusted interface because of source MAC address and client hardware address mismatch.
Client Ifc Mismatch	Represents the number of DHCP release and Deny messages received on the different ports than learned previously.

Term	Definition
DHCP Server Msgs Rec'd	Represents the number of DHCP server messages received on Untrusted ports.

Example: The following shows example CLI display output for the command.

```
(switch) #show ipv6 dhcp snooping statistics

 Interface    MAC Verify   Client Ifc   DHCP Server
               Failures     Mismatch    Msgs Rec'd
-----------   ----------   ----------   -----------
0/2                  0            0             0
0/3                  0            0             0
0/4                  0            0             0
0/5                  0            0             0
0/6                  0            0             0
0/7                  0            0             0
0/8                  0            0             0
0/9                  0            0             0
0/10                 0            0             0
0/11                 0            0             0
0/12                 0            0             0
0/13                 0            0             0
0/14                 0            0             0
0/15                 0            0             0
0/16                 0            0             0
0/17                 0            0             0
0/18                 0            0             0
0/19                 0            0             0
0/20                 0            0             0
```

8.6.0.17 clear ipv6 dhcp snooping binding

Use this command to clear all DHCPv6 Snooping bindings on all interfaces or on a specific interface.

Format `clear ipv6 dhcp snooping binding [interface` *`slot/port`*`]`

Mode
- Privileged EXEC
- User EXEC

8.6.0.18 clear ipv6 dhcp snooping statistics

Use this command to clear all DHCPv6 Snooping statistics.

Format `clear ipv6 dhcp snooping statistics`

Mode
- Privileged EXEC
- User EXEC

8.6.0.19 show ipv6 verify

Use this command to display the IPv6 configuration on a specified slot/port.

Format `show ipv6 verify` *`interface`*

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Interface	Interface address in slot/port format.
Filter Type	Is one of two values: ■ ip-v6mac: User has configured MAC address filtering on this interface. ■ ipv6: Only IPv6 address filtering on this interface.
IPv6 Address	IPv6 address of the interface
MAC Address	If MAC address filtering is not configured on the interface, the MAC Address field is empty. If port security is disabled on the interface, then the MAC Address field displays “permit-all.”
VLAN	The VLAN for the binding rule.

Example: The following shows example CLI display output for the command.

```
(switch) #show ipv6 verify 0/1

Interface  Filter Type    IP Address       MAC Address      Vlan
---------  -----------  ---------------  -----------------  -----
    0/1     ipv6-mac       2000::1/64      00:02:B3:06:60:80     10
    0/1     ipv6-mac       3000::1/64      00:0F:FE:00:13:04     10
```

8.6.0.20 show ipv6 verify source

Use this command to display the IPv6SG configurations on all ports. If the interface option is specified, the output is restricted to the specified slot/port.

Format `show ipv6 verify source {`*`interface`*`}`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Interface	Interface address in slot/port format.
Filter Type	Is one of two values: ■ ip-v6mac: User has configured MAC address filtering on this interface. ■ ipv6: Only IPv6 address filtering on this interface.
IPv6 Address	IPv6 address of the interface
MAC Address	If MAC address filtering is not configured on the interface, the MAC Address field is empty. If port security is disabled on the interface, then the MAC Address field displays “permit-all.”
VLAN	The VLAN for the binding rule.

Example: The following shows example CLI display output for the command.

```
(switch) #show ipv6 verify source

Interface  Filter Type    IP Address       MAC Address      Vlan
---------  -----------  ---------------  -----------------  -----
    0/1     ipv6-mac       2000::1/64      00:02:B3:06:60:80     10
    0/1     ipv6-mac       3000::1/64      00:0F:FE:00:13:04     10
```

8.6.0.21 show ipv6 source binding

Use this command to display the IPv6SG bindings.

Format `show ipv6 source binding [{dhcp-snooping|static}] [interface slot/port] [vlan id]`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
MAC Address	The MAC address for the entry that is added.
IP Address	The IP address of the entry that is added.
Type	Entry type; statically configured from CLI or dynamically learned from DHCP Snooping.
VLAN	VLAN for the entry.
Interface	IP address of the interface in *slot/port* format.

Example: The following shows example CLI display output for the command.

```
(switch) #show ipv6 source binding

MAC Address            IP Address       Type          Vlan     Interface
-----------------  ---------------  -------------  -----  -------------
00:00:00:00:00:08          2000::1  dhcp-snooping     2         0/1
00:00:00:00:00:09          3000::1  dhcp-snooping     3         0/1
00:00:00:00:00:0A          4000::1  dhcp-snooping     4         0/1
```

8.7 IPv6 Policy-Based Routing Commands

The following commands in the Section 7.5, Policy-Based Routing Commands section for IPv4 traffic can also be used with IPv6 traffic:

- Section 7.5.0.4, match length
- Section 7.5.0.5, match mac-list
- Section 7.5.0.6, set interface

For information about routing policy commands for BGP, see Section 11.2, BGP Routing Policy Commands.

8.7.0.1 ipv6 policy

Use this command to identify a route map to use for policy-based IPv6 routing on an interface.

Format `ipv6 policy route-map` *`route-map-name`*

Mode Interface Config

Parameter	Description
route-map-name	The name of the route map to use for policy routing. It must match a map tag specified by a route-map command. If user tries to apply a route-map name that is not configured/ created yet, an error is shown to user.

Usage Guidelines:

A route-map statement should contain eligible match/set conditions for policy-based routing in order to be applied to hardware.

- Valid match conditions: `match ipv6 address acl, match mac-list, match length`
- Valid set conditions: `set ipv6 next-hop, set ipv6 default next-hop, set ipv6 precedence`

A route-map statement should contain at least one match condition and one set condition as specified above for it to be eligible to be applied to hardware. If not, the route-map is not applied to hardware.

NOTE: Route-map and DiffServ cannot work on the same interface.

When a route-map is applied on a VLAN interface and a DiffServ policy is applied on a member port of the same VLAN interface, the port policy has priority over the VLAN policy.

The same route-map cannot be applied using both `ip policy` and `ipv6 policy` commands on an interface.

Example:

```
(Routing) (Interface vlan 40)#show ip policy

Interface            Route-Map
------------  ----------------------------------------
3/4              rm6
(Routing) (Interface vlan 40)#ipv6 policy route-map rm6

Route-map  is already in use for IPv6 based policy routing
```

When a route-map has both IPv4 and IPv6 statements provisioned and the user applies the route-map using the `ipv6 policy` command, then the IPv4 statements in the route-map will not take effect. A message will be displayed to the user to indicate this.

Example:

```
(Routing) (Interface vlan 40)#ipv6 policy route-map rm4
```

IPv4 statements in this route-map will not be applied using IPv6 Policy Based Routing

8.7.0.1.1 no ipv6 policy

Use this command to disable policy based routing from an interface.

Format `no ipv6 policy route-map` *`route-map-name`*

Mode Interface Config

8.7.0.2 match ipv6 address

Use this command to configure a route map to match based on the match criteria configured in an IPv6 access-list.

If you specify a non-configured IPv6 ACL name/number to match, the CLI displays an error message. Make sure the IPv6 ACL is configured before it is linked to a route-map. Actions present in IPv6 ACL configuration are applied with other actions involved in the route-map. When an IPv6 ACL referenced by a route-map is removed or rules are added or deleted from that ACL, configuration is rejected. Adding ACLs to or removing ACLs from a route-map that is attached to an interface is allowed.

When a list of IPv6 access-lists is specified in this command, if packet matches at least one of these access-list match criteria, then the corresponding set actions in route-map are applied to packet.

If there are duplicate IPv6 access-list numbers/names in this command, the duplicate configuration is ignored.

Default No match criteria are defined by default.

Format `match ipv6 address {`*`access-list-number`* `|` *`access-list-name`*`} [...`*`access-list-number`* `|` *`access-list-name`*`]`

Mode Route Map Configuration

Parameter	Description
access-list-number	The IPv6 access-list number that identifies an access-list configured through access-list CLI configuration commands. This number is 1 to 99 for standard access list number. This number is 100 to 199 for extended access list number.
access-list-name	The IPv6 access-list name that identifies the named IPv6 ACL. The `access-list-name` can be up to 31 characters in length. A maximum of four ACLs can be specified in this match clause.

Example: Following sequence shows how to create a route-map with a match clause on an ACL number and apply that route-map on an interface.

```
(Routing) (Config)#ipv6 access-list acl2
(Routing) (Config-ipv6-acl)#permit ipv6 1001::1 any
(Routing) (Config-ipv6-acl)#exit
(Routing) (Config)#route-map rm1 permit 40
(Routing) (route-map)#match ipv6 address acl2
```

```
(Routing) (config-route-map)#set ipv6 default next-hop 2001::2
(Routing) (config)#interface 0/1
(Routing) (Interface 0/1)#ip address 10.1.1.1 255.255.255.0
(Routing) (Interface 0/1)#ipv6  policy route-map rm1
```

The `ipv6 policy route-map rm1` command is applied to interface 0/1. All packets ingressing on 0/1 are policy-routed if a match is made as per the IPv6 access-list.

Sequence number 40 in route map rm1 is used to match all packets sourced from host 1001::1 If there is a match, and if the router has no explicit route for the packet's destination, it is sent to next-hop address 2001::2

The rest of the packets are forwarded as per normal L3 destination-based routing.

8.7.0.2.1 no match ipv6 address

Use this command to delete a match statement from a route map.

Format `no match ipv6 address [...a`*`ccess-list-number | access-list-name`*`]`

Mode Route Map Configuration

8.7.0.3 set ipv6 next-hop

Use this command to specify the adjacent next-hop router in the path toward the destination to which the packets should be forwarded. If more than one IPv6 address is specified, the first IPv6 address associated with a currently up connected interface is used to route the packets.

Format `set ipv6 next-hop [interface` *`slot/port | vlan link-local address`* `] ipv6-address [...ipv6-address]`

Mode Route Map Configuration

Parameter	Description
ipv6-address	The global IPv6 address of the next hop to which packets are output. It must be the address of an adjacent router
interface	Use the `interface` keyword to specify an IPv6 next hop using the link local address. You can then specify the link-local address along with the interface. A maximum of four next-hop global IPv6 addresses and a link-local address can be specified in this `set` clause. The link-local next hop is prioritized over the global next-hops.

Usage Guidelines

The `set ipv6 next-hop` command affects all incoming packet types and is always used if configured.. A check is made in the NDP table to see if the next hop is resolved, if so packets are forwarded to the next-hop.

In a route-map statement, `set ipv6 next-hop` and `set ipv6 default next-hop` terms are mutually exclusive. However, a `set ipv6 default next-hop` can be configured in a separate route-map statement.

Example:

```
(Routing) (route-map)#set ipv6 next-hop 3333::2
```

8.7.0.3.1 no set ipv6 next-hop

Use this command to remove a set command from a route map.

Format no set ipv6 next-hop [interface *slot/port* | *vlan link-local address*] ipv6-address [...ipv6-address]

Mode Route Map Configuration

8.7.0.4 set ipv6 default next-hop

Use this command to set a list of default next-hop IPv6 addresses. If more than one IPv6 address is specified, the first next hop specified that appears to be adjacent to the router is used. The other specified IPv6 addresses are tried in turn.

Format `set ipv6 default next-hop [interface slot/port | vlan link-local address] ipv6-address [...ipv6-address]`

Mode Route Map Configuration

Parameter	Description
ipv6-address	The Global IPv6 address of the next hop to which packets are output. It must be the address of an adjacent router.
Interface	When the user wants to specify an IPv6 next hop using the link local address - then the interface key word needs to be used. The user can then specify the link-local address along with the interface. A maximum of 4 next-hop global IPv6 addresses and a link-local address can be specified in this 'set' clause. The link-local next hop is prioritized over the global next-hops.

Usage Guidelines

A packet is routed to the next hop specified by the `set ipv6 default next-hop` command only if there is no explicit route for the packet's destination address in the routing table. A default route in the routing table is not considered an explicit route for an unknown destination address.

In a route-map statement, `set ipv6 next-hop` and `set ipv6 default next-hop` terms are mutually exclusive.However, a `set ipv6 next-hop` can be configured in a separate route-map statement

When a `set ipv6 default next-hop` is configured in a route-map and applied on an interface, if a default route is present in the system, it is expected that packets matching route-map rules are still policy route. This is because a default route is not considered explicit route to destination.

Example:

```
(Routing)(config-route-map)# set ipv6 default next-hop 2002::2
```

8.7.0.4.1 no set ipv6 default next-hop

Use this command to remove a set command from a route map.

Format `no set ipv6 default next-hop ip-address [...ip-address]`

Mode Route Map Configuration

8.7.0.5 set ipv6 precedence

Similar to IPv4, use this command to set the precedence in the IPv6 packet header. With 3 bits, there are 8 possible values for the IP precedence; values 0 through 7 are defined. This gives the administrator the ability to enable differentiated classes of service.

Format `set ipv6 precedence` *`0-7`*
Mode Route Map Configuration

Parameter	Description
0	Sets the routine precedence
1	Sets the priority precedence
2	Sets the immediate precedence
3	Sets the Flash precedence
4	Sets the Flash override precedence
5	Sets the critical precedence
6	Sets the internetwork control precedence
7	Sets the network control precedence

8.7.0.5.1 no set ipv6 precedence

Use this command to reset the three IPv6 precedence bits in the IP packet header to the default.

Format `no set ipv6 precedence`
Mode Route Map Configuration

8.7.0.6 show ipv6 policy

Use this command to display the route maps used for policy routing on the router's interfaces

Format `show ipv6 policy`
Mode Privileged EXEC

Example:

```
(Routing) #show ipv6 policy

Interface            Route-Map

-- -- -- -- -- --   -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -

0/24                 rmapv6
```

Chapter 9: IP Multicast Commands

This chapter describes the IP Multicast commands available in the EFOS CLI.

9.1 Multicast Commands

This section describes the commands you use to configure IP Multicast and to view IP Multicast settings and statistics.

9.1.0.1 ip mcast boundary

This command adds an administrative scope multicast boundary specified by *groupipaddr* and *mask* for which this multicast administrative boundary is applicable. *groupipaddr* is a group IP address and *mask* is a group IP mask. This command can be used to configure a single interface or a range of interfaces.

Format ip mcast boundary *groupipaddr mask*
Mode Interface Config

9.1.0.1.1 no ip mcast boundary

This command deletes an administrative scope multicast boundary specified by *groupipaddr* and *mask* for which this multicast administrative boundary is applicable. *groupipaddr* is a group IP address and *mask* is a group IP mask.

Format no ip mcast boundary *groupipaddr mask*
Mode Interface Config

9.1.0.2 ip mroute

This command configures an IPv4 Multicast Static Route for a source.

Default No MRoute is configured on the system.
Format ip mroute *src-ip-addr src-mask rpf-addr preference*
Mode Global Config

Parameter	Description
src-ip-addr	The IP address of the multicast source network.
src-mask	The IP mask of the multicast data source.
rpf-ip-addr	The IP address of the RPF next-hop router toward the source.
preference	The administrative distance for this Static MRoute, that is, the preference value. The range is 1 to 255.

9.1.0.2.1 no ip mroute

This command removes the configured IPv4 Multicast Static Route.

Format no ip mroute *src-ip-addr*
Mode Global Config

9.1.0.3 ip multicast

This command sets the administrative mode of the IP multicast forwarder in the router to active. This command also enables the administrative mode of IPv6 multicast routing.

Default disabled
Format ip multicast
Mode Global Config

9.1.0.3.1 no ip multicast

This command sets the administrative mode of the IP multicast forwarder in the router to inactive.

Format `no ip multicast`
Mode Global Config

9.1.0.4 ip multicast ttl-threshold

This command is specific to IPv4. Use this command to apply the given Time-to-Live threshold value to a routing interface or range of interfaces. The `ttl-threshold` is the TTL threshold which is to be applied to the multicast Data packets which are to be forwarded from the interface. This command sets the Time-to-Live threshold value such that any data packets forwarded over the interface having TTL value above the configured value are dropped. The value for `ttl-threshold` ranges from 0 to 255.

Default 1
Format `ip multicast ttl-threshold` *`ttlvalue`*
Mode Interface Config

9.1.0.4.1 no ip multicast ttl-threshold

This command applies the default `ttl-threshold` to a routing interface. The `ttl-threshold` is the TTL threshold which is to be applied to the multicast Data packets which are to be forwarded from the interface.

Format `no ip multicast ttl-threshold`
Mode Interface Config

9.1.0.5 show ip mcast

This command displays the system-wide multicast information.

Format `show ip mcast`
Modes
- Privileged EXEC
- User EXEC

Term	Definition
Admin Mode	The administrative status of multicast. Possible values are enabled or disabled.
Protocol State	The current state of the multicast protocol. Possible values are Operational or Non-Operational.

Term	Definition
Table Max Size	The maximum number of entries allowed in the multicast table.
Protocol	The multicast protocol running on the router. Possible values are PIMDM, PIMSM, or DVMRP.
Multicast Forwarding Cache Entry Count	The number of entries in the multicast forwarding cache.

9.1.0.6 show ip mcast boundary

This command displays all the configured administrative scoped multicast boundaries. The argument *slot/port* corresponds to a physical routing interface or VLAN routing interface. The keyword **vlan** is used to specify the VLAN ID of the routing VLAN directly instead of in a *slot/port* format.

Format `show ip mcast boundary {`*`slot/port`*`|vlan `*`1-4093`*`|all}`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Interface	*slot/port*
Group Ip	The group IP address.
Mask	The group IP mask.

9.1.0.7 show ip mcast interface

This command displays the multicast information for the specified interface. The argument *slot/port* corresponds to a physical routing interface or VLAN routing interface. The keyword **vlan** is used to specify the VLAN ID of the routing VLAN directly instead of in a *slot/port* format.

Format `show ip mcast interface {`*`slot/port`*`|vlan `*`1-4093`*`}`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Interface	*slot/port*
TTL	The time-to-live value for this interface.

9.1.0.8 show ip mroute

This command displays a summary or all the details of the multicast table.

NOTE: This command replaces the `show ip mcast mroute` command.

Format `show ip mroute {detail | summary | group `*`group-address`*` | source `*`source-address`*`}`

Modes
- Privileged EXEC
- User EXEC

If you use the `detail, group`, or `source` parameters in PIM Sparse mode, the command displays the following fields:

Parameter	Description
Flags	■ F: Register flag. Indicates that the source connected router is sending registers to RP. This flag can be seen only on Designated Router connected to source. ■ T: SPT-bit set. Indicates that packets have been received on the shortest path source tree. ■ R: RP-bit set. Indicates that the (S, G) entry is pointing toward the RP. This flag typically indicates a prune state along the shared tree for a particular source.
Outgoing interface flags	■ C: Connected. A member of the multicast group is directly connected to the interface. ■ J: Received PIM (*,G) Join on this interface.
Timers:Uptime/Expires	■ Uptime: Indicates per interface how long (in hours, minutes, and seconds) the entry has been in the IP multicast routing table. ■ Expires: Indicates per interface how long (in seconds) until the entry will be removed from the IP multicast routing table
Counters	■ Joins: Indicates the number of (*,G) or (S,G) joins received for the given entry. ■ Prunes: Indicates the number of (*,G) or (S,G) prunes received for the given entry. ■ Registers: Indicates the number of register messages received for the given (S,G) entry. ■ Register Stops: Indicates the number of register stop messages received for the given (S,G) entry.
RPF Address	IP address of the upstream router to the source.
Outgoing interface list	List of outgoing Interfaces.
Protocol	The current operating multicast routing protocol.
RP	Address of the RP router.
Incoming interface	Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.

If you use the `detail` parameter in any mode other than PIM sparse mode, the command displays the following fields:

Term	Definition
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Expiry Time	The time of expiry of this entry in seconds.
Up Time	The time elapsed since the entry was created in seconds.
RPF Neighbor	The IP address of the RPF neighbor.
Flags	The flags associated with this entry.

If you use the `summary` parameter in PIM Sparse mode, the command displays the following fields:

Parameter	Description
Source IP	Source address of the multicast route entry.
Group IP	Group address of the multicast route entry.
Protocol	The current operating multicast routing protocol.
Incoming Interface	Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.
Outgoing Interface List	List of outgoing Interfaces.

If you use the `summary` parameter, the command displays the following fields:

Term	Definition
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Protocol	The multicast routing protocol by which the entry was created.
Incoming Interface	The interface on which the packet for the source/group arrives.
Outgoing Interface List	The list of outgoing interfaces on which the packet is forwarded.

Example: This example shows the output for the summary parameter in PIM Sparse mode.

```
(Routing) #show  ip mroute summary

                  Multicast route table summary
                                              Incoming  Outgoing
Source IP       Group IP        Protocol    Interface Interface List
--------------- --------------- ---------- --------- ---------------
192.168.10.1    225.1.1.1        PIMSM      Vl10     Vl20, Vl30
```

Example: This example shows the output for the detail parameter in PIM Sparse mode.

```
IP Multicast Routing Table
Flags: C - Connected, J - Received Pim (*,G) Join,
R - RP-bit set, F - Register flag, T - SPT-bit set
Timers: Uptime/Expires    Protocol: PIMSM

( *,225.6.6.6)
00:00:41/000    RP: 1.1.1.1
Joins/Prunes: 0/0
Incoming interface:            RPF nbr: 0.0.0.0
Outgoing interface list:
4/1        00:00:41/218    Joins:          0    Flags:   C

( *,225.7.7.7)
00:00:36/000    RP: 1.1.1.1
Joins/Prunes: 0/0
Incoming interface:            RPF nbr: 0.0.0.0
Outgoing interface list:
4/1        00:00:36/224    Joins:          0    Flags:   C

(3.3.3.11,225.6.6.6)
00:00:51/158    Flags:   T
Joins/Prunes: 0/0    Reg/Reg-stop: 0/0
Incoming interface: 4/2        RPF nbr: 3.3.3.11
Outgoing interface list:
4/1        00:00:41/000    Joins:          0

(3.3.3.11,225.7.7.7)
00:17:42/201    Flags:   T
Joins/Prunes: 0/0    Reg/Reg-stop: 0/0
Incoming interface: 4/2        RPF nbr: 3.3.3.11
Outgoing interface list:
4/1        00:00:36/000    Joins:          0
```

Example: This example shows the output for the detail parameter in PIM Dense mode when a multicast routing protocol other than PIMSM is enabled.

```
(Routing) (Config)#show ip mroute detail

IP Multicast Routing Table
                                Expiry Time   Up Time
Source IP       Group IP        (hh:mm:ss)    (hh:mm:ss)    RPF Neighbor    Flags
--------------- --------------- ------------- ------------- --------------- -----
192.168.10.1    225.1.1.1       00:02:45      05:37:09      192.168.20.5    SPT
```

Example: This example shows IPv6 output for the detail parameter in PIM Sparse mode.

```
#show ipv6 mroute detail

IP Multicast Routing Table
Flags: C - Connected, J - Received Pim (*,G) Join,
R - RP-bit set, F - Register flag, T - SPT-bit set
Timers: Uptime/Expires    Protocol: PIMSM

( *,ff43::3)
00:00:41/000    RP: 2001::1
Joins/Prunes: 0/0
Incoming interface:            RPF nbr: ::
Outgoing interface list:
4/1        00:00:41/219    Joins:          0    Flags:   C

( *,ff24::6)
00:00:22/000    RP: 2001::1
Joins/Prunes: 0/0
Incoming interface:            RPF nbr: ::
Outgoing interface list:
4/1        00:00:41/219    Joins:          0    Flags:   C

(3001::10,ff43::3)
00:00:07/203    Flags:   T
Joins/Prunes: 0/0    Reg/Reg-stop: 0/0
Incoming interface: 4/2        RPF nbr: 3001::10
Outgoing interface list:
4/1        00:00:07/000    Joins:          0

(4001::33,ff22::3)
00:00:55/108    Flags:   T
Joins/Prunes: 0/0    Reg/Reg-stop: 0/0
Incoming interface: 4/1        RPF nbr: 3001::10
Outgoing interface list:
4/2        00:00:66/000    Joins:          0

(3001::10,ff43::3)
00:00:07/203    Flags:   T
Joins/Prunes: 0/0    Reg/Reg-stop: 0/0
Incoming interface: 4/1        RPF nbr: 3001::10
Outgoing interface list:
4/2        00:00:77/000    Joins:          0
```

Example: This example shows output for the group parameter in PIM Sparse mode.

```
(U16)# show ip mroute group 229.10.0.1
IP Multicast Routing Table
```

```
Flags: C - Connected,J - Received PIM (*,G) Join,
       R - RP-bit set, F - Register flag, T - SPT-bit set
Timers: Uptime(HH:MM:SS)/Expiry(SSS)
Protocol: PIMSM

(*, 229.10.0.1), 00:04:35/179, RP: 192.0.2.20
Joins/Prunes: 20/1
Incoming interface: Null, RPF Address: 0.0.0.0
Outgoing interface list:
    VLAN 6    00:00:30/150  Joins:15  Flags: C
    VLAN 5    00:04:35/150  Joins:10  Flags: C
    VLAN 2    00:01:28/0    Joins:20  Flags: J

(192.0.2.20, 229.10.0.1), 00:04:35/177, Flags: T
Joins/Prunes:20/1 , Reg/Reg-Stop:100/0
Incoming interface: VLAN 2, RPF Address: 0.0.0.0
Outgoing interface list:
    VLAN 5    00:03:25/0    Joins:20
    VLAN 6    00:00:10/0    Joins:5
```

Example: The following example shows output for the source parameter in PIM Sparse mode.

```
(U16)# show ip mroute source 192.0.2.20
IP Multicast Routing Table

Flags: C - Connected,J - Received PIM (*,G) Join,
       R - RP-bit set, F - Register flag, T - SPT-bit set
Timers: Uptime(HH:MM:SS)/Expiry(SSS)
Protocol: PIMSM

(192.0.2.20, 229.10.0.1), 00:04:35/177, Flags: T
Joins/Prunes:20/1 , Reg/Reg-Stop:100/0
Incoming interface: VLAN 2, RPF Address: 0.0.0.0
Outgoing interface list:
    VLAN 5    00:03:25/0    Joins:20
    VLAN 6    00:00:10/0    Joins:5
```

9.1.0.9 show ip mcast mroute group

This command displays the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the given *groupipaddr*.

Format `show ip mcast mroute group` ***groupipaddr*** `{detail | summary}`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Protocol	The multicast routing protocol by which this entry was created.
Incoming Interface	The interface on which the packet for this group arrives.
Outgoing Interface List	The list of outgoing interfaces on which this packet is forwarded.

9.1.0.10 show ip mcast mroute source

This command displays the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the given source IP address or source IP address and group IP address pair.

Format `show ip mcast mroute source` *`sourceipaddr`* `{summary | groupipaddr}`

Modes
- Privileged EXEC
- User EXEC

If you use the *`groupipaddr`* parameter, the command displays the following column headings in the output table:

Term	Definition
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Expiry Time	The time of expiry of this entry in seconds.
Up Time	The time elapsed since the entry was created in seconds.
RPF Neighbor	The IP address of the RPF neighbor.
Flags	The flags associated with this entry.

If you use the `summary` parameter, the command displays the following column headings in the output table:

Term	Definition
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Protocol	The multicast routing protocol by which this entry was created.
Incoming Interface	The interface on which the packet for this source arrives.
Outgoing Interface List	The list of outgoing interfaces on which this packet is forwarded.

9.1.0.11 show ip mcast mroute static

Use the `show ip mcast mroute static` command in Privileged EXEC or User EXEC mode to display all the static routes configured in the static mcast table, if it is specified, or display the static route associated with the particular *sourceipaddr*.

Format `show ip mcast mroute static [`*`sourceipaddr`*`]`

Modes
- Privileged EXEC
- User EXEC

Parameter	Description
Source IP	IP address of the multicast source network.
Source Mask	The subnetwork mask pertaining to the sourceIP.
RPF Address	The IP address of the RPF next-hop router toward the source.
Preference	The administrative distance for this Static MRoute.

Example: The following shows example CLI display output for the command.

```
(Routing)#show ip mcast mroute static

                     MULTICAST STATIC ROUTES
Source IP        Source Mask   RPF Address     Preference
---------------- ------------- --------------- ----------
1.1.1.1          255.255.255.0   2.2.2.2         23
```

9.1.0.12 clear ip mroute

This command deletes all or the specified IP multicast route entries.

NOTE: This command only clears dynamic mroute entries. It does not clear static mroutes.

Format `clear ip mroute {*|group-address[source-address]}`

Modes Privileged EXEC

Parameter	Description
*****	Deletes all IPv4 entries from the IP multicast routing table.
group-address	IP address of the multicast group.
source-address	The IP address of a multicast source that is sending multicast traffic to the group.

Example: The following deletes all entries from the IP multicast routing table:

```
(Routing) # clear ip mroute *
```

Example: The following deletes all entries from the IP multicast routing table that match the given multicast group address (224.1.2.1), irrespective of which source is sending for this group:

```
(Routing) # clear ip mroute 224.1.2.1
```

Example: The following deletes all entries from the IP multicast routing table that match the given multicast group address (224.1.2.1) and the multicast source address (192.168.10.10):

```
(Routing) # clear ip mroute 224.1.2.1 192.168.10.10
```

9.2 DVMRP Commands

This section describes the Distance Vector Multicast Routing Protocol (DVMRP) commands.

9.2.0.1 ip dvmrp

This command sets administrative mode of DVMRP in the router to active.

Default disabled
Format `ip dvmrp`
Mode Global Config

9.2.0.1.1 no ip dvmrp

This command sets administrative mode of DVMRP in the router to inactive.

Format `no ip dvmrp`
Mode Global Config

9.2.0.2 ip dvmrp metric

This command configures the metric for an interface or range of interfaces. This value is used in the DVMRP messages as the cost to reach this network. This field has a range of 1 to 31.

Default 1
Format `ip dvmrp metric` *`metric`*
Mode Interface Config

9.2.0.2.1 no ip dvmrp metric

This command resets the metric for an interface to the default value. This value is used in the DVMRP messages as the cost to reach this network.

Format `no ip dvmrp metric`
Mode Interface Config

9.2.0.3 ip dvmrp trapflags

This command enables the DVMRP trap mode.

Default disabled
Format `ip dvmrp trapflags`
Mode Global Config

9.2.0.3.1 no ip dvmrp trapflags

This command disables the DVMRP trap mode.

Format `no ip dvmrp trapflags`
Mode Global Config

9.2.0.4 ip dvmrp

This command sets the administrative mode of DVMRP on an interface or range of interfaces to active.

Default disabled
Format `ip dvmrp`
Mode Interface Config

9.2.0.4.1 no ip dvmrp

This command sets the administrative mode of DVMRP on an interface to inactive.

Format `no ip dvmrp`
Mode Interface Config

9.2.0.5 show ip dvmrp

This command displays the system-wide information for DVMRP.

Format `show ip dvmrp`
Modes
- Privileged EXEC
- User EXEC

Term	Definition
Admin Mode	Indicates whether DVMRP is enabled or disabled.
Version String	The version of DVMRP being used.
Number of Routes	The number of routes in the DVMRP routing table.
Reachable Routes	The number of entries in the routing table with non-infinite metrics.

The following fields are displayed for each interface.

Term	Definition
Interface	*slot/port*
Interface Mode	The mode of this interface. Possible values are Enabled and Disabled.
State	The current state of DVMRP on this interface. Possible values are Operational or Non-Operational.

9.2.0.6 show ip dvmrp interface

This command displays the interface information for DVMRP on the specified interface. The argument *slot/port* corresponds to a physical routing interface or VLAN routing interface. The keyword **vlan** is used to specify the VLAN ID of the routing VLAN directly instead of in a *slot/port* format.

Format `show ip dvmrp interface {slot/port|vlan 1-4093}`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Interface Mode	Indicates whether DVMRP is enabled or disabled on the specified interface.
Metric	The metric of this interface. This is a configured value.
Local Address	The IP address of the interface.

The following field is displayed only when DVMRP is operational on the interface.

Term	Definition
Generation ID	The Generation ID value for the interface. This is used by the neighboring routers to detect that the DVMRP table should be resent.

The following fields are displayed only if DVMRP is enabled on this interface.

Term	Definition
Received Bad Packets	The number of invalid packets received.
Received Bad Routes	The number of invalid routes received.
Sent Routes	The number of routes that have been sent on this interface.

9.2.0.7 show ip dvmrp neighbor

This command displays the neighbor information for DVMRP.

Format `show ip dvmrp neighbor`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
IfIndex	The value of the interface used to reach the neighbor.
Nbr IP Addr	The IP address of the DVMRP neighbor for which this entry contains information.
State	The state of the neighboring router. The possible value for this field are ACTIVE or DOWN.
Up Time	The time since this neighboring router was learned.
Expiry Time	The time remaining for the neighbor to age out. This field is not applicable if the State is DOWN.
Generation ID	The Generation ID value for the neighbor.
Major Version	The major version of DVMRP protocol of neighbor.
Minor Version	The minor version of DVMRP protocol of neighbor.
Capabilities	The capabilities of neighbor.
Received Routes	The number of routes received from the neighbor.
Rcvd Bad Pkts	The number of invalid packets received from this neighbor.

Term	Definition
Rcvd Bad Routes	The number of correct packets received with invalid routes.

9.2.0.8 show ip dvmrp nexthop

This command displays the next hop information on outgoing interfaces for routing multicast datagrams.

Format `show ip dvmrp nexthop`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Source IP	The sources for which this entry specifies a next hop on an outgoing interface.
Source Mask	The IP Mask for the sources for which this entry specifies a next hop on an outgoing interface.
Next Hop Interface	The interface in *slot/port* format for the outgoing interface for this next hop.
Type	The network is a LEAF or a BRANCH.

9.2.0.9 show ip dvmrp prune

This command displays the table listing the router's upstream prune information.

Format `show ip dvmrp prune`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Group IP	The multicast Address that is pruned.
Source IP	The IP address of the source that has pruned.
Source Mask	The network Mask for the prune source. It should be all 1s or both the prune source and prune mask must match.
Expiry Time (secs)	The expiry time in seconds. This is the time remaining for this prune to age out.

9.2.0.10 show ip dvmrp route

This command displays the multicast routing information for DVMRP.

Format `show ip dvmrp route`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Source Address	The multicast address of the source group.
Source Mask	The IP Mask for the source group.
Upstream Neighbor	The IP address of the neighbor which is the source for the packets for a specified multicast address.

Term	Definition
Interface	The interface used to receive the packets sent by the sources.
Metric	The distance in hops to the source subnet. This field has a different meaning than the Interface Metric field.
Expiry Time (secs)	The expiry time in seconds, which is the time left for this route to age out.
Up Time (secs)	The time when a specified route was learnt, in seconds.

9.3 PIM Commands

This section describes the commands you use to configure Protocol Independent Multicast -Dense Mode (PIM-DM) and Protocol Independent Multicast - Sparse Mode (PIM-SM). PIM-DM and PIM-SM are multicast routing protocols that provides scalable inter-domain multicast routing across the Internet, independent of the mechanisms provided by any particular unicast routing protocol. Only one PIM mode can be operational at a time.

9.3.0.1 ip pim dense

This command administratively enables the PIM Dense mode across the router.

Default disabled
Format `ip pim dense`
Mode Global Config

Example: The following shows an example of the command.

```
(Routing) (Config) #ip pim dense
```

9.3.0.1.1 no ip pim dense

This command administratively disables the PIM Dense mode across the router.

Format `no ip pim dense`
Mode Global Config

9.3.0.2 ip pim sparse

This command administratively enables the PIM Sparse mode across the router.

Default disabled
Format `ip pim sparse`
Mode Global Config

Example: The following shows an example of the command.

```
(Routing) (Config) #ip pim sparse
```

9.3.0.2.1 no ip pim sparse

This command administratively disables the PIM Sparse mode across the router.

Format `no ip pim sparse`
Mode Global Config

9.3.0.3 ip pim

Use this command to administratively enable PIM on the specified interface.

Default disabled

Format `ip pim`
Mode Interface Config

Example: The following shows example CLI display output for the command.

```
(Routing) (Interface 0/1) #ip pim
```

9.3.0.3.1 no ip pim

Use this command to disable PIM on the specified interface.

Format `no ip pim`
Mode Interface Config

9.3.0.4 ip pim hello-interval

This command configures the transmission frequency of PIM hello messages the specified interface. This field has a range of 0 to 18000 seconds.

Default 30
Format `ip pim hello-interval` *seconds*
Mode Interface Config

Example: The following shows an example of the command.

```
(Routing) (Interface 0/1) #ip pim hello-interval 50
```

9.3.0.4.1 no ip pim hello-interval

This command resets the transmission frequency of hello messages between PIM enabled neighbors to the default value.

Format `no ip pim hello-interval`
Mode Interface Config

9.3.0.5 ip pim bsr-border

Use this command to prevent bootstrap router (BSR) messages from being sent or received on the specified interface.

NOTE: This command takes effect only when Sparse mode in enabled in the Global mode.

Default disabled
Format `ip pim bsr-border`
Mode Interface Config

Example: The following shows an example of the command.

```
(Routing) (Interface 0/1) #ip pim bsr-border
```

9.3.0.5.1 no ip pim bsr-border

Use this command to disable the specified interface from being the BSR border.

Format `no ip pim bsr-border`

Mode Interface Config

9.3.0.6 ip pim bsr-candidate

This command is used to configure the router to announce its candidacy as a bootstrap router (BSR). The argument *slot/port* corresponds to a physical routing interface or VLAN routing interface. The keyword **vlan** is used to specify the VLAN ID of the routing VLAN directly instead of in a *slot/port* format.

NOTE: This command takes effect only when PIM-SM is configured as the PIM mode.

Default Disabled

Format `ip pim bsr-candidate interface {slot/port|vlan 1-4093} hash-mask-length [bsr-priority] [interval interval]`

Mode Global Config

Parameters	Description
slot/port	Interface number on this router from which the BSR address is derived, to make it a candidate. This interface must be enabled with PIM.
hash-mask-length	Length of a mask (32 bits maximum) that is to be ANDed with the group address before the hash function is called. All groups with the same seed hash correspond to the same RP. For example, if this value is 24, only the first 24 bits of the group addresses matter. This allows you to get one RP for multiple groups.
bsr-priority	Priority of the candidate BSR. The range is an integer from 0 to 255. The BSR with the larger priority is preferred. If the priority values are the same, the router with the larger IP address is the BSR. The default value is 0.
interval	[Optional] Indicates the BSR candidate advertisement interval. The range is from 1 to 16383 seconds. The default value is 60 seconds.

Example: The following shows examples of the command.

```
(Routing) (Config) #ip pim bsr-candidate interface 0/1 32 5
(Routing) (Config) #ip pim bsr-candidate interface 0/1 32 5 interval 100
```

9.3.0.6.1 no ip pim bsr-candidate

Use this command to remove the configured PIM Candidate BSR router.

Format `no ip pim bsr-candidate interface {slot/port|vlan 1-4093}`

Mode Global Config

9.3.0.7 ip pim dr-priority

Use this command to set the priority value for which a router is elected as the designated router (DR).

NOTE: This command takes effect only when Sparse mode is enabled in the Global mode.

Default 1

Format `ip pim dr-priority 0-2147483647`

Mode Interface Config

Example: The following shows example CLI display output for the command.

```
(Routing) (Interface 0/1) #ip pim dr-priority 10
```

9.3.0.7.1 no ip pim dr-priority

Use this command to return the DR Priority on the specified interface to its default value.

Format `no ip pim dr-priority`
Mode Interface Config

9.3.0.8 ip pim join-prune-interval

Use this command to configure the frequency of PIM Join/Prune messages on a specified interface. The join/prune interval is specified in seconds. This parameter can be configured to a value from 0 to 18000.

NOTE: This command takes effect only when is configured as the PIM mode.

Default 60
Format `ip pim join-prune-interval` *`0-18000`*
Mode Interface Config

Example: The following shows examples of the command.

```
(Routing) (Interface 0/1) #ip pim join-prune-interval 90
```

9.3.0.8.1 no ip pim join-prune-interval

Use this command to set the join/prune interval on the specified interface to the default value.

Format `no ip pim join-prune-interval`
Mode Interface Config

9.3.0.9 ip pim rp-address

This command defines the address of a PIM Rendezvous point (RP) for a specific multicast group range.

NOTE: This command takes effect only when PIM-SM is configured as the PIM mode.

Default 0
Format `ip pim rp-address` *`rp-address group-address group-mask`* `[override]`
Mode Global Config

Parameter	Description
rp-address	The IP address of the RP.
group-address	The group address supported by the RP.
group-mask	The group mask for the group address.
override	[Optional] Indicates that if there is a conflict, the RP configured with this command prevails over the RP learned by BSR.

Example: The following shows an example of the command.

```
(Routing) (Config) #ip pim rp-address 192.168.10.1
   224.1.2.0 255.255.255.0
```

9.3.0.9.1 no ip pim rp-address

Use this command to remove the address of the configured PIM Rendezvous point (RP) for the specified multicast group range.

Format `no ip pim rp-address` *`rp-address group-address group-mask`* `[override]`

Mode Global Config

9.3.0.10 ip pim rp-candidate

Use this command to configure the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR) for a specific multicast group range. The argument *slot/port* corresponds to a physical routing interface or VLAN routing interface. The keyword **vlan** is used to specify the VLAN ID of the routing VLAN directly instead of in a *slot/port* format.

NOTE: This command takes effect only when PIM-SM is configured as the PIM mode.

Default Disabled

Format `ip pim rp-candidate interface {`*`slot/port`*`|`*`vlan 1-4093`*`} group-address group-mask [interval interval]`

Mode Global Config

Parameter	Description
slot/port	The IP address associated with this interface type and number is advertised as a candidate RP address. This interface must be enabled with PIM.
group-address	The multicast group address that is advertised in association with the RP address.
group-mask	The multicast group prefix that is advertised in association with the RP address.
interval	[Optional] Indicates the RP candidate advertisement interval. The range is from 1 to 16383 seconds. The default value is 60 seconds.

Example: The following shows examples of the command.

```
(Routing) (Config) #ip pim rp-candidate interface 0/1 224.1.2.0 255.255.255.0
(Routing) (Config) #ip pim rp-candidate interface 0/1 224.1.2.0 255.255.255.0 interval 200
```

9.3.0.10.1 no ip pim rp-candidate

Use this command to remove the configured PIM candidate Rendezvous point (RP) for a specific multicast group range.

Format `no ip pim rp-candidate interface {`*`slot/port`*`|`*`vlan 1-4093`*`} group-address group-mask`

Mode Global Config

9.3.0.11 ip pim ssm

Use this command to define the Source Specific Multicast (SSM) range of IP multicast addresses on the router.

NOTE: This command takes effect only when PIM-SM is configured as the PIM mode.

Default disabled

Format `ip pim ssm {default | group-address group-mask}`

Mode Global Config

Parameter	Description
default-range	Defines the SSM range access list to 232/8.

Example: The following shows an example of the command.

```
(Routing) (Config) #ip pim ssm default
(Routing) (Config) #ip pim ssm 232.1.2.0 255.255.255.0
```

9.3.0.11.1 no ip pim ssm

Use this command to remove the Source Specific Multicast (SSM) range of IP multicast addresses on the router.

Format `no ip pim ssm {default | group-address group-mask}`

Mode Global Config

9.3.0.12 ip pim-trapflags

This command enables the PIM trap mode for both Sparse Mode (SM) and Dense Mode. (DM).

Default disabled

Format `ip pim-trapflags`

Mode Global Config

9.3.0.12.1 no ip pim-trapflags

This command sets the PIM trap mode to the default.

Format `no ip pim-trapflags`

Mode Global Config

9.3.0.13 show ip mfc

This command displays mroute entries in the multicast forwarding (MFC) database.

Format `show ip mfc`

Modes
- Privileged EXEC
- User EXEC

Terms	Parameters
MFC IPv4 Mode	Enabled when IPv4 Multicast routing is operational.
MFC IPv6 Mode	Enabled when IPv6 Multicast routing is operational.
MFC Entry Count	The number of entries present in MFC.

Terms	Parameters
Current multicast IPv4 Protocol	The current operating IPv4 multicast routing protocol.
Current multicast IPv6 Protocol	The current operating multicast IPv6 routing protocol.
Total Software Forwarded packets	Total Number of multicast packets forwarded in software.
Source Address	Source address of the multicast route entry.
Group Address	Group address of the multicast route entry.
Packets Forwarded in Software for this entry	Number of multicast packets that are forwarded in software for a specific multicast route entry,
Protocol	Multicast Routing Protocol that has added a specific entry
Expiry Time (secs)	Expiry time for a specific Multicast Route entry in seconds.
Up Time (secs)	Up Time in seconds for a specific Multicast Routing entry.
Incoming interface	Incoming interface for a specific Multicast Route entry.
Outgoing interface list	Outgoing interface list for a specific Multicast Route entry.

Example:

```
(Routing) (Config)#show ip mfc

MFC IPv4 Mode................................. Enabled
MFC IPv6 Mode................................. Disabled
MFC Entry Count .............................. 1
Current multicast IPv4 protocol............... PIMSM
Current multicast IPv6 protocol............... No protocol enabled.
Total software forwarded packets ............. 0

Source address: 192.168.10.5
Group address: 225.1.1.1
Packets forwarded in software for this entry: 0           Protocol: PIM-SM
Expiry Time (secs): 206       Up Time (secs): 4
Incoming interface: 0/10    Outgoing interface list: None
```

9.3.0.14 show ip pim

This command displays the system-wide information for PIM-DM or PIM-SM.

Format `show ip pim`

Modes
- Privileged EXEC
- User EXEC

NOTE: If the PIM mode is PIM-DM (dense), some of the fields in the following table do not display in the command output because they are applicable only to PIM-SM.

Term	Definition
PIM Mode	Indicates the configured mode of the PIM protocol as dense (PIM-DM) or sparse (PIM-SM)
Interface	*slot/port*
Interface Mode	Indicates whether PIM is enabled or disabled on this interface.
Operational Status	The current state of PIM on this interface: Operational or Non-Operational.

Example: The following shows example CLI display output for the command.

Example #1: PIM Mode - Dense

```
(Routing) #show ip pim

PIM Mode      Dense

InterfaceInterface-ModeOperational-Status
---------   --------------    ------------------
0/1       Enabled           Operational
0/3       Disabled          Non-Operational
```

Example #2: PIM Mode - Sparse

```
(Routing) #show ip pim

PIM Mode      Sparse

InterfaceInterface-ModeOperational-Status
---------   --------------    ------------------
0/1       Enabled           Operational
0/3       Disabled          Non-Operational
```

Example #3: PIM Mode - None

```
(Routing) #show ip pim

PIM Mode      None

None of the routing interfaces are enabled for PIM.
```

9.3.0.15 show ip pim ssm

This command displays the configured source specific IP multicast addresses. If no SSM Group range is configured, this command output is `No SSM address range is configured`.

Format `show ip pim ssm`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Group Address	The IP multicast address of the SSM group.
Prefix Length	The network prefix length.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip pim ssm

Group Address/Prefix Length
---------------------------
232.0.0.0/8
```

If no SSM Group range is configured, this command displays the following message:

```
No SSM address range is configured.
```

9.3.0.16 show ip pim interface

This command displays the PIM interface status parameters. The argument *slot/port* corresponds to a physical routing interface or VLAN routing interface. The keyword **vlan** is used to specify the VLAN ID of the routing VLAN directly instead of in a *slot/port* format. If no interface is specified, the command displays the status parameters of all PIM-enabled interfaces.

Format `show ip pim interface [slot/port|vlan 1-4093}]`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Interface	*slot/port The interface number.*
Mode	Indicates the active PIM mode enabled on the interface is dense or sparse.
Hello Interval	The frequency at which PIM hello messages are transmitted on this interface. By default, the value is 30 seconds.
Join Prune Interval	The join/prune interval value for the PIM router. The interval is in seconds.
DR Priority	The priority of the Designated Router configured on the interface. This field is not applicable if the interface mode is Dense.
BSR Border	Identifies whether this interface is configured as a bootstrap router border interface.
Neighbor Count	The number of PIM neighbors learned on this interface. This is a dynamic value and is shown only when a PIM interface is operational.
Designated Router	The IP address of the elected Designated Router for this interface. This is a dynamic value and will only be shown when a PIM interface is operational. This field is not applicable if the interface mode is Dense.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip pim interface

Interface.....................................0/1
  Mode........................................Sparse
  Hello Interval (secs).......................30
  Join Prune Interval (secs)..................60
  DR Priority.................................1
  BSR Border..................................Disabled
  Neighbor Count..............................1
  Designated Router...........................192.168.10.1

Interface.....................................0/2
  Mode........................................Sparse
  Hello Interval (secs).......................30
  Join Prune Interval (secs)..................60
  DR Priority.................................1
  BSR Border..................................Disabled
  Neighbor Count..............................1
  Designated Router...........................192.168.10.1
```

If none of the interfaces are enabled for PIM, the following message is displayed:

```
None of the routing interfaces are enabled for PIM.
```

9.3.0.17 show ip pim neighbor

This command displays PIM neighbors discovered by PIMv2 Hello messages. The argument *slot/port* corresponds to a physical routing interface or VLAN routing interface. The keyword **vlan** is used to specify the VLAN ID of the routing VLAN directly instead of in a *slot/port* format. If the interface number is not specified, the command displays the status parameters of all PIM-enabled interfaces.

Format `show ip pim neighbor [{slot/port|vlan 1-4093}]`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Neighbor Address	The IP address of the PIM neighbor on an interface.
Interface	*slot/port*
Up Time	The time since this neighbor has become active on this interface.
Expiry Time	Time remaining for the neighbor to expire.
DR Priority	The DR Priority configured on this Interface (PIM-SM only). **NOTE:** DR Priority is applicable only when sparse-mode configured routers are neighbors. Otherwise, NA is displayed in this field.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip pim neighbor 0/1

Neighbor Addr   Interface Uptime      Expiry Time DR
                          (hh:mm:ss) (hh:mm:ss)   Priority
--------------- --------- ---------- ---------- --------
192.168.10.2    0/1     00:02:55     00:01:15   NA


(Routing) #show ip pim neighbor

Neighbor Addr   Interface  Uptime      Expiry Time DR
                           (hh:mm:ss) (hh:mm:ss)   Priority
--------------- ---------  ---------- ---------- --------
192.168.10.2    0/1      00:02:55     00:01:15   1
192.168.20.2    0/2      00:03:50     00:02:10   1
```

If no neighbors have been learned on any of the interfaces, the following message is displayed:

```
No neighbors exist on the router.
```

9.3.0.18 show ip pim bsr-router

This command displays the bootstrap router (BSR) information.

Format `show ip pim bsr-router {candidate | elected}`

Mode
- Privileged EXEC
- User EXEC

Parameter	Definition
BSR Address	IP address of the BSR.
BSR Priority	Priority as configured in the `ip pim bsr-candidate` command.
BSR Hash Mask Length	Length of a mask (maximum 32 bits) that is to be ANDed with the group address before the hash function is called. This value is configured in the `ip pim bsr-candidate` command.
C-BSR Advertisement Interval	Indicates the configured C-BSR Advertisement interval with which the router, acting as a C-BSR, will periodically send the C-BSR advertisement messages.
Next Bootstrap Message	Time (in hours, minutes, and seconds) in which the next bootstrap message is due from this BSR.

Example: The following shows example CLI display output for the command.

Example #1:

```
(Routing) #show ip pim bsr-router elected

BSR Address..................................... 192.168.10.1
  BSR Priority.................................. 0
  BSR Hash Mask Length.......................... 30
  Next Bootstrap message (hh:mm:ss)............. 00:00:24
```

Example #2:

```
(Routing) #show ip pim bsr-router candidate

BSR Address..................................... 192.168.10.1
  BSR Priority.................................. 0
  BSR Hash Mask Length.......................... 30
  C-BSR Advertisement Interval (secs)......... 60
  Next Bootstrap message (hh:mm:ss)............. NA
```

If no configured or elected BSRs exist on the router, the following message is displayed:

```
   No BSR's exist/learned on this router.
```

9.3.0.19 show ip pim rp-hash

This command displays the rendezvous point (RP) selected for the specified group address.

Format `show ip pim rp-hash` *`group-address`*

Modes
- Privileged EXEC
- User EXEC

Term	Definition
RP Address	The IP address of the RP for the group specified.
Type	Indicates the mechanism (BSR or static) by which the RP was selected.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip pim rp-hash 224.1.2.0

RP Address192.168.10.1
   TypeStatic
```

If no RP Group mapping exist on the router, the following message is displayed:

```
No RP-Group mappings exist/learned on this router.
```

9.3.0.20 show ip pim rp mapping

Use this command to display the mapping for the PIM group to the active Rendezvous points (RP) of which the router is a aware (either configured or learned from the bootstrap router (BSR)). Use the optional parameters to limit the display to a specific RP address or to view group-to-candidate RP or group to Static RP mapping information.

Format `show ip pim rp mapping [{`*`rp-address`*`|candidate|static}]`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
RP Address	The IP address of the RP for the group specified.
Group Address	The IP address of the multicast group.
Group Mask	The subnet mask associated with the group.
Origin	Indicates the mechanism (BSR or static) by which the RP was selected.
C-RP Advertisement Interval	Indicates the configured C-RP Advertisement interval with which the router acting as a Candidate RP will periodically send the C-RP advertisement messages to the elected BSR.

Example: The following show examples of CLI display output for the command.

Example #1:

```
(Routing) #show ip pim rp mapping 192.168.10.1

RP Address       192.168.10.1
   Group Address 224.1.2.1
   Group Mask    255.255.255.0
   Origin        Static
```

Example #2:

```
 (Routing) #show ip pim rp mapping

RP Address       192.168.10.1
   Group Address 224.1.2.1
   Group Mask    255.255.255.0
   Origin        Static

RP Address       192.168.20.1
   Group Address 229.2.0.0
   Group Mask    255.255.0.0
   Origin        Static
```

Example #3:

```
(Routing) # show ip pim rp mapping candidate

RP Address..................................... 192.168.10.1
   Group Address............................... 224.1.2.1
   Group Mask.................................. 255.255.0.0
   Origin...................................... BSR
   C-RP Advertisement Interval (secs)......... 60
```

```
   Next Candidate RP Advertisement (hh:mm:ss). 00:00:15
```

If no RP Group mapping exist on the router, the following message is displayed:

```
No RP-Group mappings exist on this router.
```

9.3.0.21 show ip pim statistics

This command displays statistics for the received PIM control packets per interface. This command displays statistics only if PIM sparse mode is enabled.

Format `show ip pim statistics`

Modes
- Privileged EXEC
- User EXEC

The following information is displayed.

Parameters	Description
Stat	RX: Packets received Tx: Packets transmitted
Interface	The PIM-enabled routing interface
Hello	The number of PIM Hello messages
Register	The number of PIM Register messages
Reg-Stop	The number of PIM Register-stop messages
Join/Pru	The number of PIM Join/Prune messages
BSR	The number of PIM Boot Strap messages
Assert	The number of PIM Assert messages
CRP	The number of PIM Candidate RP Advertisement messages.

Example:

Example 1:

```
(Routing) #show ip pim statistics
=====================================================================
Interface  Stat   Hello Register Reg-Stop Join/Pru  BSR  Assert  CRP
=====================================================================
Vl10         Rx       0        0        0        0     0     0     0
             Tx       2        0        0        0     0     0     0

     Invalid Packets Received - 0
---------------------------------------------------------------------
Vl20         Rx       0        0        0        5     0     0     0
             Tx       8        7        0        0     0     0     0

     Invalid Packets Received - 0
---------------------------------------------------------------------
0/5       Rx       0        0        6        5     0     0     0
            Tx       10       9        0        0     0     0     0

     Invalid Packets Received - 0
---------------------------------------------------------------------
```

Example 2:

```
(Routing) #show ip pim statistics vlan 10
=========================================================================
Interface  Stat   Hello Register Reg-Stop Join/Pru  BSR  Assert  CRP
=========================================================================
Vl10        Rx       0        0        0        0     0     0     0
            Tx       2        0        0        0     0     0     0

     Invalid Packets Received - 0
-------------------------------------------------------------------------
```

Example 3:

```
(Routing) #show ip pim statistics 0/5
=========================================================================
Interface  Stat   Hello Register Reg-Stop Join/Pru  BSR  Assert  CRP
=========================================================================
1/0/5       Rx       0        0        6        5     0     0     0
            Tx       10       9        0        0     0     0     0

     Invalid Packets Received - 0
```

NOTE: For ipv6 statistics use the key word ipv6.

9.4 Internet Group Message Protocol Commands

This section describes the commands you use to view and configure Internet Group Message Protocol (IGMP) settings.

9.4.0.1 ip igmp

This command sets the administrative mode of IGMP in the system to active on an interface, range of interfaces, or on all interfaces.

Default disabled

Format `ip igmp`

Modes
- Global Config
- Interface Config

9.4.0.1.1 no ip igmp

This command sets the administrative mode of IGMP in the system to inactive.

Format `no ip igmp`

Modes
- Global Config
- Interface Config

9.4.0.2 ip igmp router-alert-check

Use this command to enable router-alert validation for IGMP packets.

Default disabled

Format `ip igmp router-alert-check`

Mode Global Config

9.4.0.2.1 no ip igmp router-alert-check

This command sets the IP IGMP router-alert-check value to default.

Format `no ip igmp router-alert-check`

Mode Global Config

9.4.0.3 ip igmp version

This command configures the version of IGMP for an interface or range of interfaces. The value for *`version`* is either 1, 2 or 3.

Default 3

Format `ip igmp version` *`version`*

Modes Interface Config

9.4.0.3.1 no ip igmp version

This command resets the version of IGMP to the default value.

Format `no ip igmp version`
Modes Interface Config

9.4.0.4 ip igmp last-member-query-count

This command sets the number of Group-Specific Queries sent by the interface or range of interfaces before the router assumes that there are no local members on the interface. The range for *`count`* is 1 to 20.

Format `ip igmp last-member-query-count` *`count`*
Modes Interface Config

9.4.0.4.1 no ip igmp last-member-query-count

This command resets the number of Group-Specific Queries to the default value.

Format `no ip igmp last-member-query-count`
Modes Interface Config

9.4.0.5 ip igmp last-member-query-interval

This command configures the Maximum Response Time inserted in Group-Specific Queries which are sent in response to Leave Group messages. The range for *`seconds`* is 0 to 255 tenths of a second. This value can be configured on one interface or a range of interfaces

Default 10 tenths of a second (1 second)
Format `ip igmp last-member-query-interval` *`seconds`*
Modes Interface Config

9.4.0.5.1 no ip igmp last-member-query-interval

This command resets the Maximum Response Time to the default value.

Format `no ip igmp last-member-query-interval`
Modes Interface Config

9.4.0.6 ip igmp query-interval

This command configures the query interval for the specified interface or range of interfaces. The query interval determines how fast IGMP Host-Query packets are transmitted on this interface. The range for `query-interval` is 1 to 3600 seconds.

Default 125 seconds
Format `ip igmp query-interval` *`seconds`*
Modes Interface Config

9.4.0.6.1 no ip igmp query-interval

This command resets the query interval for the specified interface to the default value. This is the frequency at which IGMP Host-Query packets are transmitted on this interface.

Format `no ip igmp query-interval`
Modes Interface Config

9.4.0.7 ip igmp query-max-response-time

This command configures the maximum response time interval for the specified interface or range of interfaces, which is the maximum query response time advertised in IGMPv2 queries on this interface.The time interval is specified in tenths of a second. The range for `gmp query-max-response-time` is 0 to 255 tenths of a second.

Default 100
Format `ip igmp query-max-response-time` *`0-255`*
Mode Interface Config

9.4.0.7.1 no ip igmp query-max-response-time

This command resets the maximum response time interval for the specified interface, which is the maximum query response time advertised in IGMPv2 queries on this interface to the default value. The maximum response time interval is reset to the default time.

Format `no ip igmp query-max-response-time`
Mode Interface Config

9.4.0.8 ip igmp robustness

This command configures the robustness that allows tuning of the interface or range of interfaces. The robustness is the tuning for the expected packet loss on a subnet. If a subnet is expected to have a lot of loss, the Robustness variable may be increased for the interface. The range for *`robustness`* is 1 to 255.

Default 2
Format `ip igmp robustness` *`1-255`*
Mode Interface Config

9.4.0.8.1 no ip igmp robustness

This command sets the robustness value to default.

Format `no ip igmp robustness`
Mode Interface Config

9.4.0.9 ip igmp startup-query-count

This command sets the number of Queries sent out on startup, separated by the Startup Query Interval on the interface or range of interfaces. The range for *`count`* is 1 to 20.

Default 2
Format `ip igmp startup-query-count` *`1-20`*
Mode Interface Config

9.4.0.9.1 no ip igmp startup-query-count

This command resets the number of Queries sent out on startup, separated by the Startup Query Interval on the interface to the default value.

Format `no ip igmp startup-query-count`
Mode Interface Config

9.4.0.10 ip igmp startup-query-interval

This command sets the interval between General Queries sent on startup on the interface or range of interfaces. The time interval value is in seconds. The range for *`interval`* is 1 to 300 seconds.

Default 31
Format `ip igmp startup-query-interval` *`1-300`*
Mode Interface Config

9.4.0.10.1 no ip igmp startup-query-interval

This command resets the interval between General Queries sent on startup on the interface to the default value.

Format `no ip igmp startup-query-interval`
Mode Interface Config

9.4.0.11 show ip igmp

This command displays the system-wide IGMP information.

Format `show ip igmp`
Modes
- Privileged EXEC
- User EXEC

Term	Definition
IGMP Admin Mode	The administrative status of IGMP. This is a configured value.
Interface	*slot/port*
Interface Mode	Indicates whether IGMP is enabled or disabled on the interface. This is a configured value.
Protocol State	The current state of IGMP on this interface. Possible values are Operational or Non-Operational.

9.4.0.12 show ip igmp groups

This command displays the registered multicast groups on the interface. The argument *slot/port* corresponds to a physical routing interface or VLAN routing interface. The keyword **vlan** is used to specify the VLAN ID of the routing VLAN directly instead of in a *slot/port* format. If [detail] is specified this command displays the registered multicast groups on the interface in detail.

Format `show ip igmp groups {slot/port|vlan 1-4093 [detail]}`

Mode Privileged EXEC

If you do not use the `detail` keyword, the following fields appear:

Term	Definition
IP Address	The IP address of the interface participating in the multicast group.
Subnet Mask	The subnet mask of the interface participating in the multicast group.
Interface Mode	This displays whether IGMP is enabled or disabled on this interface.

The following fields are not displayed if the interface is not enabled:

Term	Definition
Querier Status	This displays whether the interface has IGMP in Querier mode or Non-Querier mode.
Groups	The list of multicast groups that are registered on this interface.

If you use the `detail` keyword, the following fields appear:

Term	Definition
Multicast IP Address	The IP address of the registered multicast group on this interface.
Last Reporter	The IP address of the source of the last membership report received for the specified multicast group address on this interface.
Up Time	The time elapsed since the entry was created for the specified multicast group address on this interface.
Expiry Time	The amount of time remaining to remove this entry before it is aged out.
Version1 Host Timer	The time remaining until the local router assumes that there are no longer any IGMP version 1 multicast members on the IP subnet attached to this interface. This could be an integer value or "-----" if there is no Version 1 host present.
Version2 Host Timer	The time remaining until the local router assumes that there are no longer any IGMP version 2 multicast members on the IP subnet attached to this interface. This could be an integer value or "-----" if there is no Version 2 host present.
Group Compatibility Mode	The group compatibility mode (v1, v2 or v3) for this group on the specified interface.

9.4.0.13 show ip igmp interface

This command displays the IGMP information for the interface. The argument *slot/port* corresponds to a physical routing interface or VLAN routing interface. The keyword **vlan** is used to specify the VLAN ID of the routing VLAN directly instead of in a *slot/port* format.

Format `show ip igmp interface {slot/port|vlan 1-4093}`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Interface	*slot/port*
IGMP Admin Mode	The administrative status of IGMP.
Interface Mode	Indicates whether IGMP is enabled or disabled on the interface.
IGMP Version	The version of IGMP running on the interface. This value can be configured to create a router capable of running either IGMP version 1 or 2.
Query Interval	The frequency at which IGMP Host-Query packets are transmitted on this interface.
Query Max Response Time	The maximum query response time advertised in IGMPv2 queries on this interface.
Robustness	The tuning for the expected packet loss on a subnet. If a subnet is expected to be have a lot of loss, the Robustness variable may be increased for that interface.
Startup Query Interval	The interval between General Queries sent by a Querier on startup.
Startup Query Count	The number of Queries sent out on startup, separated by the Startup Query Interval.
Last Member Query Interval	The Maximum Response Time inserted into Group-Specific Queries sent in response to Leave Group messages.
Last Member Query Count	The number of Group-Specific Queries sent before the router assumes that there are no local members.

9.4.0.14 show ip igmp interface membership

This command displays the list of interfaces that have registered in the multicast group.

Format `show ip igmp interface membership` ***multiipaddr*** `[detail]`

Mode Privileged EXEC

Term	Definition
Interface	Valid slot and port number separated by forward slashes.
Interface IP	The IP address of the interface participating in the multicast group.
State	The interface that has IGMP in Querier mode or Non-Querier mode.
Group Compatibility Mode	The group compatibility mode (v1, v2 or v3) for the specified group on this interface.
Source Filter Mode	The source filter mode (Include/Exclude) for the specified group on this interface. This is “-----” for IGMPv1 and IGMPv2 Membership Reports.

If you use the `detail` keyword, the following fields appear:

Term	Definition
Interface	Valid slot and port number separated by forward slashes.
Group Compatibility Mode	The group compatibility mode (v1, v2 or v3) for the specified group on this interface.
Source Filter Mode	The source filter mode (Include/Exclude) for the specified group on this interface. This is “-----” for IGMPv1 and IGMPv2 Membership Reports.

Term	Definition
Source Hosts	The list of unicast source IP addresses in the group record of the IGMPv3 Membership Report with the specified multicast group IP address. This is “-----” for IGMPv1 and IGMPv2 Membership Reports.
Expiry Time	The amount of time remaining to remove this entry before it is aged out. This is “-----” for IGMPv1 and IGMPv2 Membership Reports.

9.4.0.15 show ip igmp interface stats

This command displays the IGMP statistical information for the interface. The statistics are only displayed when the interface is enabled for IGMP. The argument *slot/port* corresponds to a physical routing interface or VLAN routing interface. The keyword **vlan** is used to specify the VLAN ID of the routing VLAN directly instead of in a *slot/port* format.

Format `show ip igmp interface stats [slot/port|vlan 1-4093]`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Querier Status	The status of the IGMP router, whether it is running in Querier mode or Non-Querier mode.
Querier IP Address	The IP address of the IGMP Querier on the IP subnet to which this interface is attached.
Querier Up Time	The time since the interface Querier was last changed.
Querier Expiry Time	The amount of time remaining before the Other Querier Present Timer expires. If the local system is the querier, the value of this object is zero.
Wrong Version Queries	The number of queries received whose IGMP version does not match the IGMP version of the interface.
Number of Joins	The number of times a group membership has been added on this interface.
Number of Groups	The current number of membership entries for this interface.

9.5 IGMP Proxy Commands

The IGMP Proxy is used by IGMP Router (IPv4 system) to enable the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP router interfaces. With IGMP Proxy enabled, the system acts as proxy to all the hosts residing on its router interfaces.

9.5.0.1 ip igmp-proxy

This command enables the IGMP Proxy on the an interface or range of interfaces. To enable the IGMP Proxy on an interface, you must enable multicast forwarding. Also, make sure that there are no multicast routing protocols enabled on the router.

Format `ip igmp-proxy`
Mode Interface Config

9.5.0.1.1 no ip igmp-proxy

This command disables the IGMP Proxy on the router.

Format `no ip igmp-proxy`
Mode Interface Config

9.5.0.2 ip igmp-proxy unsolicit-rprt-interval

This command sets the unsolicited report interval for the IGMP Proxy interface or range of interfaces. This command is valid only when you enable IGMP Proxy on the interface or range of interfaces. The value of *interval* can be 1-260 seconds.

Default 1
Format `ip igmp-proxy unsolicit-rprt-interval` *1-260*
Mode Interface Config

9.5.0.2.1 no ip igmp-proxy unsolicit-rprt-interval

This command resets the unsolicited report interval of the IGMP Proxy router to the default value.

Format `no ip igmp-proxy unsolicit-rprt-interval`
Mode Interface Config

9.5.0.3 ip igmp-proxy reset-status

This command resets the host interface status parameters of the IGMP Proxy interface (or range of interfaces). This command is valid only when you enable IGMP Proxy on the interface.

Format `ip igmp-proxy reset-status`
Mode Interface Config

9.5.0.4 show ip igmp-proxy

This command displays a summary of the host interface status parameters. It displays the following parameters only when you enable IGMP Proxy.

Format `show ip igmp-proxy`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Interface index	The interface number of the IGMP Proxy.
Admin Mode	States whether the IGMP Proxy is enabled or not. This is a configured value.
Operational Mode	States whether the IGMP Proxy is operationally enabled or not. This is a status parameter.
Version	The present IGMP host version that is operational on the proxy interface.
Number of Multicast Groups	The number of multicast groups that are associated with the IGMP Proxy interface.
Unsolicited Report Interval	The time interval at which the IGMP Proxy interface sends unsolicited group membership report.
Querier IP Address on Proxy Interface	The IP address of the Querier, if any, in the network attached to the upstream interface (IGMP-Proxy interface).
Older Version 1 Querier Timeout	The interval used to timeout the older version 1 queriers.
Older Version 2 Querier Timeout	The interval used to timeout the older version 2 queriers.
Proxy Start Frequency	The number of times the IGMP Proxy has been stopped and started.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip igmp-proxy

Interface Index.......................................... 0/1
Admin Mode............................................... Enable
Operational Mode......................................... Enable
Version.................................................. 3
Num of Multicast Groups.............................. 0
Unsolicited Report Interval.......................... 1
Querier IP Address on Proxy Interface........ 5.5.5.50
Older Version 1 Querier Timeout.............. 0
Older Version 2 Querier Timeout.............. 00::00:00
Proxy Start Frequency................................ 1
```

9.5.0.5 show ip igmp-proxy interface

This command displays a detailed list of the host interface status parameters. It displays the following parameters only when you enable IGMP Proxy.

Format `show ip igmp-proxy interface`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Interface Index	The *slot/port* of the IGMP proxy.

The column headings of the table associated with the interface are as follows:

Term	Definition
Ver	The IGMP version.
Query Rcvd	Number of IGMP queries received.
Report Rcvd	Number of IGMP reports received.
Report Sent	Number of IGMP reports sent.
Leaves Rcvd	Number of IGMP leaves received. Valid for version 2 only.
Leaves Sent	Number of IGMP leaves sent on the Proxy interface. Valid for version 2 only.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip igmp-proxy interface

Interface Index.............................. 0/1

Ver  Query Rcvd  Report Rcvd  Report Sent  Leave Rcvd  Leave Sent
-----------------------------------------------------------------
1      0             0             0         -----        -----
2      0             0             0           0            0
3      0             0             0         -----        -----
```

9.5.0.6 show ip igmp-proxy groups

This command displays information about the subscribed multicast groups that IGMP Proxy reported. It displays a table of entries with the following as the fields of each column.

Format `show ip igmp-proxy groups`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Interface	The interface number of the IGMP Proxy.
Group Address	The IP address of the multicast group.
Last Reporter	The IP address of host that last sent a membership report for the current group on the network attached to the IGMP Proxy interface (upstream interface).
Up Time (in secs)	The time elapsed since last created.
Member State	The status of the entry. Possible values are IDLE_MEMBER or DELAY_MEMBER. ■ IDLE_MEMBER - interface has responded to the latest group membership query for this group. ■ DELAY_MEMBER - interface is going to send a group membership report to respond to a group membership query for this group.
Filter Mode	Possible values are **Include** or **Exclude**.
Sources	The number of sources attached to the multicast group.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip igmp-proxy groups

Interface Index.............................. 0/1

Group Address    Last Reporter    Up Time   Member State  Filter Mode  Sources
-------------    -------------- ---------- ------------- ------------- -------
225.4.4.4        5.5.5.48         00:02:21  DELAY_MEMBER     Include       3

226.4.4.4        5.5.5.48         00:02:21  DELAY_MEMBER     Include       3

227.4.4.4        5.5.5.48         00:02:21  DELAY_MEMBER     Exclude       0

228.4.4.4        5.5.5.48         00:02:21  DELAY_MEMBER     Include       3
```

9.5.0.7 show ip igmp-proxy groups detail

This command displays complete information about multicast groups that IGMP Proxy reported. It displays a table of entries with the following as the fields of each column.

Format `show ip igmp-proxy groups detail`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Interface	The interface number of the IGMP Proxy.
Group Address	The IP address of the multicast group.
Last Reporter	The IP address of host that last sent a membership report for the current group, on the network attached to the IGMP-Proxy interface (upstream interface).
Up Time (in secs)	The time elapsed since last created.
Member State	The status of the entry. Possible values are IDLE_MEMBER or DELAY_MEMBER. ■ IDLE_MEMBER - interface has responded to the latest group membership query for this group. ■ DELAY_MEMBER - interface is going to send a group membership report to respond to a group membership query for this group.
Filter Mode	Possible values are **Include** or **Exclude**.
Sources	The number of sources attached to the multicast group.
Group Source List	The list of IP addresses of the sources attached to the multicast group.
Expiry Time	Time left before a source is deleted.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip igmp-proxy groups

Interface Index.............................. 0/1

Group Address    Last Reporter    Up Time   Member State Filter Mode  Sources
-------------    -------------- ----------- ------------ ------------ ---------
225.4.4.4        5.5.5.48         00:02:21  DELAY_MEMBER     Include         3

Group Source List             Expiry Time
-----------------           -----------------
5.1.2.3                       00:02:21
```

```
6.1.2.3                       00:02:21
7.1.2.3                       00:02:21

226.4.4.4       5.5.5.48         00:02:21  DELAY_MEMBER     Include          3

Group Source List             Expiry Time
------------------           ---------------
2.1.2.3                       00:02:21
6.1.2.3                       00:01:44
8.1.2.3                       00:01:44

227.4.4.4       5.5.5.48         00:02:21  DELAY_MEMBER     Exclude        0



228.4.4.4       5.5.5.48         00:03:21  DELAY_MEMBER     Include          3

Group Source List             Expiry Time
------------------           ---------------
9.1.2.3                       00:03:21
6.1.2.3                       00:03:21
7.1.2.3                       00:03:21
```

Chapter 10: IPv6 Multicast Commands

This chapter describes the IPv6 Multicast commands available in the EFOS CLI.

NOTE: There is no specific IP multicast enable for IPv6. Enabling of multicast at global config is common for both IPv4 and IPv6.

10.1 IPv6 Multicast Forwarder

10.1.0.1 ipv6 mroute

This command configures an IPv6 Multicast Static Route for a source.

Default No MRoute is configured on the system.

Format ipv6 mroute *src-ip-addr src-mask rpf-addr* [interface] *preference*

Mode Global Config

Parameter	Description
src-ip-addr	The IP address of the multicast source network.
src-mask	The IP mask of the multicast data source.
rpf-ip-addr	The IP address of the RPF next-hop router toward the source.
interface	Specify the interface if the RPF Address is a link-local address.
preference	The administrative distance for this Static MRoute, that is, the preference value. The range is 1 to 255.

10.1.0.1.1 no ipv6 mroute

This command removes the configured IPv6 Multicast Static Route.

Format no ipv6 mroute *src-ip-addr*

Mode Global Config

10.1.0.2 show ipv6 mroute

NOTE: There is no specific IP multicast enable for IPv6. Enabling of multicast at global config is common for both IPv4 and IPv6.

Use this command to show the mroute entries specific for IPv6. (This command is the IPv6 equivalent of the IPv4 `show ip mcast mroute` command.)

Format `show ipv6 mroute {[detail] | [summary] | [group {`*`group-address`*`} [detail | summary]] | [source {`*`source-address`*`} [`*`grpaddr`*` | summary ]]}`

Modes
- Privileged EXEC
- User EXEC

If you use the *detail* parameter, the command displays the following Multicast Route Table fields:

Term	Definition
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Expiry Time	The time of expiry of this entry in seconds.
Up Time	The time elapsed since the entry was created in seconds.
RPF Neighbor	The IP address of the RPF neighbor.
Flags	The flags associated with this entry.

If you use the *summary* parameter, the command displays the following fields:

Term	Definition
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Protocol	The multicast routing protocol by which the entry was created.
Incoming Interface	The interface on which the packet for the source/group arrives.
Outgoing Interface List	The list of outgoing interfaces on which the packet is forwarded.

10.1.0.3 show ipv6 mroute group

This command displays the multicast configuration settings specific to IPv6 such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the given group IPv6 address *group-address*.

Format `show ipv6 mroute group` *group-address* `{detail | summary}`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Protocol	The multicast routing protocol by which this entry was created.
Incoming Interface	The interface on which the packet for this group arrives.
Outgoing Interface List	The list of outgoing interfaces on which this packet is forwarded.

10.1.0.4 show ipv6 mroute source

This command displays the multicast configuration settings specific to IPv6 such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the given source IP address or source IP address and group IP address pair.

Format `show ipv6 mroute source` *source-address* `{`*grpaddr* `| summary}`

Modes
- Privileged EXEC
- User EXEC

If you use the *groupipaddr* parameter, the command displays the following column headings in the output table:

Term	Definition
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Expiry Time	The time of expiry of this entry in seconds.
Up Time	The time elapsed since the entry was created in seconds.
RPF Neighbor	The IP address of the RPF neighbor.
Flags	The flags associated with this entry.

If you use the *summary* parameter, the command displays the following column headings in the output table:

Term	Definition
Source IP Addr	The IP address of the multicast data source.
Group IP Addr	The IP address of the destination of the multicast packet.
Protocol	The multicast routing protocol by which this entry was created.
Incoming Interface	The interface on which the packet for this source arrives.
Outgoing Interface List	The list of outgoing interfaces on which this packet is forwarded.

10.1.0.5 show ipv6 mroute static

Use the `show ipv6 mroute static` command in Privileged EXEC or User EXEC mode to display all the configured IPv6 multicast static routes.

Format `show ipv6 mroute static [source-address]`

Modes
- Privileged EXEC
- User EXEC

Parameter	Description
Source Address	IP address of the multicast source network.
Source Mask	The subnetwork mask pertaining to the sourceIP.
RPF Address	The IP address of the RPF next-hop router toward the source.
Interface	The interface that is used to reach the RPF next-hop. This is valid if the RPF address is a link-local address.
Preference	The administrative distance for this Static MRoute.

10.1.0.6 clear ipv6 mroute

This command deletes all or the specified IPv6 multicast route entries.

NOTE: This command only clears dynamic mroute entries. It does not clear static mroutes.

Format `clear ipv6 mroute {*|group-address[source-address]}`

Modes Privileged EXEC

Parameter	Description
*	Deletes all IPv6 entries from the IPv6 multicast routing table.
group-address	IPv6 address of the multicast group.
source-address	The IPv6 address of a multicast source that is sending multicast traffic to the group.

Example: The following deletes all entries from the IPv6 multicast routing table:

```
(Routing) # clear ipv6 mroute *
```

Example: The following deletes all entries from the IPv6 multicast routing table that match the given multicast group address (FF4E::1), irrespective of which source is sending for this group:

```
(Routing) # clear ipv6 mroute FF4E::1
```

Example: The following deletes all entries from the IPv6 multicast routing table that match the given multicast group address (FF4E::1) and the multicast source address (2001::2):

```
(Routing) # clear ip mroute FF4E::1 2001::2
```

10.2 IPv6 PIM Commands

This section describes the commands you use to configure Protocol Independent Multicast -Dense Mode (PIM-DM) and Protocol Independent Multicast - Sparse Mode (PIM-SM) for IPv6 multicast routing. PIM-DM and PIM-SM are multicast routing protocols that provides scalable inter-domain multicast routing across the Internet, independent of the mechanisms provided by any particular unicast routing protocol. Only one PIM mode can be operational at a time.

10.2.0.1 ipv6 pim dense

This command enables the administrative mode of PIM-DM in the router.

Default disabled
Format `ipv6 pim dense`
Mode Global Config

Example: The following shows an example of the command.

```
(Routing) (Config) #ipv6 pim dense
```

10.2.0.1.1 no ipv6 pim dense

This command disables the administrative mode of PIM-DM in the router.

Format `no ipv6 pim dense`
Mode Global Config

10.2.0.2 ipv6 pim sparse

This command enables the administrative mode of PIM-SM in the router.

Default disabled
Format `ipv6 pim sparse`
Mode Global Config

Example: The following shows an example of the command.

```
(Routing) (Config) #ipv6 pim sparse
```

10.2.0.2.1 no ipv6 pim sparse

This command disables the administrative mode of PIM-SM in the router.

Format `no ipv6 pim sparse`
Mode Global Config

10.2.0.3 ipv6 pim

This command administratively enables PIM on an interface or range of interfaces.

Default disabled

Format `ipv6 pim`
Mode Interface Config

Example: The following shows example CLI display output for the command.

```
(Routing) (Interface 0/1) #ipv6 pim
```

10.2.0.3.1 no ipv6 pim

This command sets the administrative mode of PIM on an interface to disabled.

Format `no ipv6 pim`
Mode Interface Config

10.2.0.4 ipv6 pim hello-interval

Use this command to configure the PIM hello interval for the specified router interface or range of interfaces. The hello-interval is specified in seconds and is in the range 0–18000.

Default 30
Format `ipv6 pim hello-interval` ***0-18000***
Mode Interface Config

Example: The following shows an example of the command.

```
(Routing) (Interface 0/1) #ipv6 pim hello-interval 50
```

10.2.0.4.1 no ipv6 pim hello-interval

Use this command to set the PIM hello interval to the default value.

Format `no ipv6 pim hello-interval`
Mode Interface Config

10.2.0.5 ipv6 pim bsr-border

Use this command to prevent bootstrap router (BSR) messages from being sent or received on the specified interface.

NOTE: This command takes effect only when PIM-SM is enabled in the Global mode.

Default disabled
Format `ipv6 pim bsr-border`
Mode Interface Config

Example: The following shows an example of the command.

```
(Routing) (Interface 0/1) #ipv6 pim bsr-border
```

10.2.0.5.1 no ipv6 pim bsr-border

Use this command to disable the setting of BSR border on the specified interface.

Format `no ipv6 pim bsr-border`

Mode Interface Config

10.2.0.6 ipv6 pim bsr-candidate

This command is used to configure the router to announce its candidacy as a bootstrap router (BSR). The argument *slot/port* corresponds to a physical routing interface or VLAN routing interface. The keyword **vlan** is used to specify the VLAN ID of the routing VLAN directly instead of in a *slot/port* format.

NOTE: This command takes effect only when PIM-SM is configured as the PIM mode.

Default Disabled

Format `ipv6 pim bsr-candidate interface {slot/port|vlan 1-4093} hash-mask-length [bsr-priority] [interval interval]`

Mode Global Config

Parameters	Description
slot/port	Interface number on this router from which the BSR address is derived, to make it a candidate. This interface must be enabled with PIM.
hash-mask-length	Length of a mask (32 bits maximum) that is to be ANDed with the group address before the hash function is called. All groups with the same seed hash correspond to the same RP. For example, if this value was 24, only the first 24 bits of the group addresses matter. This allows you to get one RP for multiple groups.
bsr-priority	Priority of the candidate BSR. The range is an integer from 0 to 255. The BSR with the larger priority is preferred. If the priority values are the same, the router with the larger IPv6 address is the BSR. The default value is 0.
interval	[Optional] Indicates the BSR candidate advertisement interval. The range is from 1 to 16383 seconds. The default value is 60 seconds.

Example: The following shows examples of the command.

```
(Routing) (Config)#ipv6 pim bsr-candidate interface 0/1 32 5
(Routing) (Config)#ipv6 pim bsr-candidate interface 0/1 32 5 interval 100
```

10.2.0.6.1 no ipv6 pim bsr-candidate

This command is used to remove the configured PIM Candidate BSR router.

Format `no ipv6 pim bsr-candidate interface {slot/port|vlan 1-4093} hash-mask-length [priority]`

Mode Global Config

10.2.0.7 ipv6 pim dr-priority

Use this command to set the priority value for which a router is elected as the designated router (DR).

NOTE: This command takes effect only when PIM-SM is enabled in the Global mode.

Default 1

Format `ipv6 pim dr-priority 0-2147483647`

Mode Interface Config

Example: The following shows example CLI display output for the command.

```
(Routing) (Interface 0/1) #ipv6 pim dr-priority 10
```

10.2.0.7.1 no ipv6 pim dr-priority

Use this command to return the DR Priority on the specified interface to its default value.

Format `no ipv6 pim dr-priority`
Mode Interface Config

10.2.0.8 ipv6 pim join-prune-interval

This command is used to configure the join/prune interval for the PIM-SM router on an interface or range of interfaces. The join/prune interval is specified in seconds. This parameter can be configured to a value from 0 to 18000.

NOTE: This command takes effect only when PIM-SM is enabled in the Global mode.

Default 60
Format `ipv6 pim join-prune-interval` *`0-18000`*
Mode Interface Config

Example: The following shows examples of the command.

```
(Routing) (Interface 0/1) #ipv6 pim join-prune-interval 90
```

10.2.0.8.1 no ipv6 pim join-prune-interval

Use this command to set the join/prune interval on the specified interface to the default value.

Format `no ipv6 pim join-prune-interval`
Mode Interface Config

10.2.0.9 ipv6 pim rp-address

This command defines the address of a PIM Rendezvous point (RP) for a specific multicast group range.

NOTE: This command takes effect only when PIM-SM is configured as the PIM mode.

Default 0
Format `ipv6 pim rp-address {`*`rp-address`* `|` *`group-address/group-mask`* `} [override]`
Mode Global Config

Parameter	Description
rp-address	The IPv6 address of the RP.
group-address	The group address supported by the RP.
group-mask	The group mask for the group address.
override	[Optional] Indicates that if there is a conflict, the RP configured with this command prevails over the RP learned by BSR.

Example: The following shows an example of the command.

```
(Routing) (Config)#ipv6 pim rp-address 2001::1 ff1e::0/64
```

10.2.0.9.1 no ipv6 pim rp-address

This command is used to remove the address of the configured PIM Rendezvous point (RP) for the specified multicast group range.

Format `no ipv6 pim rp-address {`*`rp-address | group-address/group-mask`*` } [override]`

Mode Global Config

10.2.0.10 ipv6 pim rp-candidate

This command is used to configure the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR) for a specific multicast group range. The argument *slot/port* corresponds to a physical routing interface or VLAN routing interface. The keyword **vlan** is used to specify the VLAN ID of the routing VLAN directly instead of in a *slot/port* format.

NOTE: This command takes effect only when PIM-SM is configured as the PIM mode.

Default Disabled

Format `ipv6 pim rp-candidate interface {`*`slot/port|vlan 1-4093} group-address group-mask [interval interval]`*

Mode Global Config

Parameter	Description
slot/port	The IP address associated with this interface type and number is advertised as a candidate RP address. This interface must be enabled with PIM.
group-address	The multicast group address that is advertised in association with the RP address.
group-mask	The multicast group prefix that is advertised in association with the RP address.
interval	[Optional] Indicates the RP candidate advertisement interval. The range is from 1 to 16383 seconds. The default value is 60 seconds.

Example: The following shows examples of the command.

```
(Routing) (Config) ipv6 pim rp-candidate interface 0/1 ff1e::0/64
(Routing) (Config) ipv6 pim rp-candidate interface 0/1 ff1e::0/64 interval 200
```

10.2.0.10.1 no ipv6 pim rp-candidate

This command is used to disable the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR).

Format `no ipv6 pim rp-candidate interface {`*`slot/port|vlan 1-4093} group-address group-mask`*

Mode Global Config

10.2.0.11 ipv6 pim ssm

Use this command to define the Source Specific Multicast (SSM) range of IPv6 multicast addresses on the router.

NOTE: Note the following:

- This command takes effect only when PIM-SM is configured as the PIM mode.
- Some EFOS platforms do not support a non-zero data threshold rate. For these platforms, only a “Switch on First Packet” policy is supported.

Default disabled

Format `ipv6 pim ssm {default | group-address group-mask}`

Mode Global Config

Parameter	Description
default-range	Defines the SSM range access list FF3x::/32.

Example: The following shows an example of the command.

```
(Routing) (Config) #ipv6 pim ssm default
(Routing) (Config) #ipv6 pim ssm ff32::/32
```

10.2.0.11.1 no ipv6 pim ssm

Use this command to remove the Source Specific Multicast (SSM) range of IP multicast addresses on the router.

Format `no ipv6 pim ssm {default | group-address group-mask}`

Mode Global Config

10.2.0.12 show ipv6 pim

This command displays the system-wide information for PIM-DM or PIM-SM.

Format `show ipv6 pim`

Modes
- Privileged EXEC
- User EXEC

NOTE: If the PIM mode is PIM-DM (dense), some of the fields in the following table do not display in the command output because they are applicable only to PIM-SM.

Term	Definition
PIM Mode	Indicates whether the PIM mode is dense (PIM-DM) or sparse (PIM-SM)
Interface	*slot/port*
Interface Mode	Indicates whether PIM is enabled or disabled on this interface.
Operational Status	The current state of PIM on this interface: Operational or Non-Operational.

Example: The following shows example CLI display output for the command.

Example #1: PIM Mode - Dense

```
(Routing) #show ipv6 pim
PIM Mode..................................... Dense

Interface  Interface-Mode  Operational-Status
```

```
---------  --------------  ------------------
0/1        Enabled         Non-Operational
0/3        Disabled        Non-Operational
0/21       Enabled         Operational
```

Example #2: PIM Mode - Sparse

```
(Routing) #show ipv6 pim
PIM Mode..................................... Sparse

Interface  Interface-Mode  Operational-Status
---------  --------------  ------------------
0/1        Enabled         Non-Operational
0/3        Disabled        Non-Operational
0/21       Enabled         Operational
```

Example #3: PIM Mode - None

```
(Routing) #show ipv6 pim

PIM Mode..................................... None

None of the routing interfaces are enabled for PIM.
```

10.2.0.13 show ipv6 pim ssm

This command displays the configured source specific IPv6 multicast addresses. If no SSM Group range is configured, this command output is `No SSM address range is configured.`

Format `show ipv6 pim ssm`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Group Address	The IPv6 multicast address of the SSM group.
Prefix Length	The network prefix length.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ipv6 pim ssm

Group Address/Prefix Length
---------------------------
ff32::/32
```

If no SSM Group range is configured, this command displays the following message:

```
No SSM address range is configured.
```

10.2.0.14 show ipv6 pim interface

This command displays the interface information for PIM on the specified interface. The argument *slot/port* corresponds to a physical routing interface or VLAN routing interface. The keyword **vlan** is used to specify the VLAN ID of the routing VLAN directly instead of in a *slot/port* format. If no interface is specified, the command displays the status parameters for all PIM-enabled interfaces.

Format `show ipv6 pim interface [{slot/port|vlan 1-4093}]`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Interface	*slot/port*
Mode	Indicates whether the PIM mode enabled on the interface is dense or sparse.
Hello Interval	The frequency at which PIM hello messages are transmitted on this interface. By default, the value is 30 seconds.
Join Prune Interval	The join/prune interval for the PIM router. The interval is in seconds.
DR Priority	The priority of the Designated Router configured on the interface. This field is not applicable if the interface mode is Dense
BSR Border	Identifies whether this interface is configured as a bootstrap router border interface.
Neighbor Count	The number of PIM neighbors learned on this interface. This is a dynamic value and is shown only when a PIM interface is operational.
Designated Router	The IP address of the elected Designated Router for this interface. This is a dynamic value and will only be shown when a PIM interface is operational. This field is not applicable if the interface mode is Dense

Example: The following shows example CLI display output for the command.

```
(Routing) #show ipv6 pim interface

Interface..................................... 0/1
Mode.......................................... Sparse
Hello Interval (secs)......................... 30
Join Prune Interval (secs).................... 60
DR Priority................................... 1
BSR Border.................................... Disabled

Interface..................................... 0/21
Mode.......................................... Sparse
Hello Interval (secs)......................... 30
Join Prune Interval (secs).................... 60
DR Priority................................... 1
BSR Border.................................... Disabled
Neighbor Count ............................... 1
Designated Router............................. fe80::20a:f7ff:fe81:8ad9
```

If none of the interfaces are enabled for PIM, the following message is displayed:

```
None of the routing interfaces are enabled for PIM.
```

10.2.0.15 show ipv6 pim neighbor

This command displays PIM neighbors discovered by PIMv2 Hello messages. The argument *slot/port* corresponds to a physical routing interface or VLAN routing interface. The keyword **vlan** is used to specify the VLAN ID of the routing VLAN directly instead of in a *slot/port* format. If the interface number is not specified, this command displays the neighbors discovered on all the PIM-enabled interfaces.

Format `show ipv6 pim neighbor [{slot/port|vlan 1-4093}]`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Neighbor Address	The IPv6 address of the PIM neighbor on an interface.
Interface	*slot/port*
Up Time	The time since this neighbor has become active on this interface.
Expiry Time	Time remaining for the neighbor to expire.
DR Priority	The DR Priority configured on this Interface (PIM-SM only). **NOTE:** DR Priority is applicable only when sparse-mode configured routers are neighbors. Otherwise, NA is displayed in this field.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ipv6 pim neighbor

Neighbor Addr                           Interface Up Time   Expiry Time DR
                                                  hh:mm:ss  hh:mm:ss    Priority
--------------------------------------- --------- --------- ----------- --------
fe80::200:52ff:feb7:58ac                0/21      00:00:03  00:01:43    0 (DR)
```

If no neighbors have been learned on any of the interfaces, the following message is displayed:

```
No neighbors are learnt on any interface.
```

10.2.0.16 show ipv6 pim bsr-router

This command displays the bootstrap router (BSR) information.

Format `show ipv6 pim bsr-router {candidate | elected}`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
BSR Address	IPv6 address of the BSR.
BSR Priority	Priority as configured in the `ipv6 pim bsr-candidate` command.
BSR Hash Mask Length	Length of a mask (maximum 32 bits) that is to be ANDed with the group address before the hash function is called. This value is configured in the `ipv6 pim bsr-candidate` command.
C-BSR Advertisement Interval	Indicates the configured C-BSR Advertisement interval with which the router, acting as a C-BSR, will periodically send the C-BSR advertisement messages.
Next Bootstrap Message	Time (in hours, minutes, and seconds) in which the next bootstrap message is due from this BSR.

Example: The following shows example CLI display output for the command.

Example #1:

```
(Routing) #show ipv6 pim bsr-router elected
BSR Address..................................... 3001::1
  BSR Priority.................................. 150
  BSR Hash Mask Length.......................... 120
  Next Bootstrap message (hh:mm:ss)............. 00:00:15
Example #2:
(Routing) #show ipv6 pim bsr-router candidate
BSR Address..................................... 3001::1
  BSR Priority.................................. 150
  BSR Hash Mask Length.......................... 120
```

```
C-BSR Advertisement Interval (secs)..... 60
Next Bootstrap message (hh:mm:ss)..... NA
```

If no configured or elected BSRs exist on the router, the following message is displayed:

```
No BSR's exist/learned on this router.
```

10.2.0.17 show ipv6 pim rp-hash

This command displays which rendezvous point (RP) is being used for a specified group.

Format `show ipv6 pim rp-hash` *`group-address`*

Modes
- Privileged EXEC
- User EXEC

Term	Definition
RP Address	The IPv6 address of the RP for the group specified.
Type	Indicates the mechanism (BSR or static) by which the RP was selected.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ipv6 pim rp-hash ff1e::

RP Address..................................... 2001::1
   Type..................................... Static
```

If no RP Group mapping exist on the router, the following message is displayed:

```
No RP-Group mappings exist/learned on this router.
```

10.2.0.18 show ipv6 pim rp mapping

Use this command to display the mapping for the PIM group to the active Rendezvous points (RP) of which the router is a aware (either configured or learned from the bootstrap router (BSR)). Use the optional parameters to limit the display to a specific RP address or to view group-to-candidate RP or group to Static RP mapping information.

Format `show ipv6 pim rp mapping [{`*`rp-address`* `| candidate | static}]`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
RP Address	The IPv6 address of the RP for the group specified.
Group Address	The IPv6 address and prefix length of the multicast group.
Origin	Indicates the mechanism (BSR or static) by which the RP was selected.
C-RP Advertisement Interval	Indicates the configured C-RP Advertisement interval with which the router acting as a Candidate RP will periodically send the C-RP advertisement messages to the elected BSR.

Example: The following show examples of CLI display output for the command.

Example #1:

```
(Routing) #show ipv6 pim rp mapping 2001::1
```

```
RP Address..................................... 2001::1
   Group Address............................... ff1e::/64
   Origin...................................... Static
   Expiry Time (hh:mm:ss)...................... NA
   Next Candidate RP Advertisement (hh:mm:ss).. NA
```

Example #2:

```
(Routing) #show ipv6 pim rp mapping
RP Address..................................... 2001::1
   Group Address............................... ff1e::/64
   Origin...................................... Static
   Expiry Time (hh:mm:ss)...................... NA
   Next Candidate RP Advertisement (hh:mm:ss).. NA
```

Example #3:

```
(Routing) # show ipv6 pim rp mapping candidate
RP Address..................................... 2001::1
   Group Address............................... ff1e::/64
   Origin...................................... BSR
   C-RP Advertisement Interval (secs).......... 200
```

If no RP Group mapping exist on the router, the following message is displayed:

```
No RP-Group mappings exist on this router.
```

10.3 IPv6 MLD Commands

IGMP/MLD Snooping is Layer 2 functionality but IGMP/MLD are Layer 3 multicast protocols. It requires that in a network setup there should be a multicast router (which can act as a querier) to be present to solicit the multicast group registrations. However some network setup does not need a multicast router as multicast traffic is destined to hosts within the same network. In this situation, EFOS has an IGMP/MLD Snooping Querier running on one of the switches and Snooping enabled on all the switches. For more information, see Section 5.28, IGMP Snooping Configuration Commands.

10.3.0.1 ipv6 mld router

Use this command, in the administrative mode of the router, to enable MLD in the router.

Default Disabled
Format `ipv6 mld router`
Mode Global Config

10.3.0.1.1 no ipv6 mld router

Use this command, in the administrative mode of the router, to disable MLD in the router.

Default Disabled
Format `no ipv6 mld router`
Mode Global Config

10.3.0.2 ipv6 mld query-interval

Use this command to set the MLD router's query interval for the interface or range of interfaces. The query-interval is the amount of time between the general queries sent when the router is the querier on that interface. The range for *`query-interval`* is 1 to 3600 seconds.

Default 125
Format `ipv6 mld query-interval` *`query-interval`*
Mode Interface Config

10.3.0.2.1 no ipv6 mld query-interval

Use this command to reset the MLD query interval to the default value for that interface.

Format `no ipv6 mld query-interval`
Mode Interface Config

10.3.0.3 ipv6 mld query-max-response-time

Use this command to set the MLD querier's maximum response time for the interface or range of interfaces and this value is used in assigning the maximum response time in the query messages that are sent on that interface. The range for *`query-max-response-time`* is 0 to 65535 milliseconds.

Default 10000 milliseconds

Format `ipv6 mld query-max-response-time` *`query-max-response-time`*
Mode Interface Config

10.3.0.3.1 no ipv6 mld query-max-response-time

This command resets the MLD query max response time for the interface to the default value.

Format `no ipv6 mld query-max-response-time`
Mode Interface Config

10.3.0.4 ipv6 mld last-member-query-interval

Use this command to set the last member query interval for an MLD interface or range of interfaces, which is the value of the maximum response time parameter in the group specific queries sent out of this interface. The range for *`last-member-query-interval`* is 0 to 65535 milliseconds.

Default 1000 milliseconds
Format `ipv6 mld last-member-query-interval` *`last-member-query-interval`*
Mode Interface Config

10.3.0.4.1 no ipv6 mld last-member-query-interval

Use this command to reset the *`last-member-query-interval`* parameter of the interface to the default value.

Format `no ipv6 mld last-member-query-interval`
Mode Interface Config

10.3.0.5 ipv6 mld last-member-query-count

Use this command to set the number of listener-specific queries sent before the router assumes that there are no local members on an interface or range of interfaces. The range for *`last-member-query-count`* is 1 to 20.

Default 2
Format `ipv6 mld last-member-query-count` *`last-member-query-count`*
Mode Interface Config

10.3.0.5.1 no ipv6 mld last-member-query-count

Use this command to reset the *`last-member-query-count`* parameter of the interface to the default value.

Format `no ipv6 mld last-member-query-count`
Mode Interface Config

10.3.0.6 ipv6 mld version

Use this command to configure the MLD version that the interface uses.

Default	2
Format	`ipv6 mld version { 1 | 2 }`
Mode	Interface Config

10.3.0.6.1 no ipv6 mld version

This command resets the MLD version used by the interface to the default value.

Format	`no ipv6 mld`
Mode	Interface Config

10.3.0.7 show ipv6 mld groups

Use this command to display information about multicast groups that MLD reported. The information is displayed only when MLD is enabled on at least one interface. If MLD was not enabled on even one interface, there is no group information to be displayed. The argument *slot/port* corresponds to a physical routing interface or VLAN routing interface. The keyword **vlan** is used to specify the VLAN ID of the routing VLAN directly instead of in a *slot/port* format.

Format	`show ipv6 mld groups {`*`slot/port`*`|`*`vlan 1-4093`*`|`*`group-address`*`}`
Mode	■ Privileged EXEC ■ User EXEC

The following fields are displayed as a table when *`slot/port is specified`*.

Field	Description
Group Address	The address of the multicast group.
Interface	Interface through which the multicast group is reachable.
Up Time	Time elapsed in hours, minutes, and seconds since the multicast group has been known.
Expiry Time	Time left in hours, minutes, and seconds before the entry is removed from the MLD membership table.

When *`group-address`* is specified, the following fields are displayed for each multicast group and each interface.

Field	Description
Interface	Interface through which the multicast group is reachable.
Group Address	The address of the multicast group.
Last Reporter	The IP Address of the source of the last membership report received for this multicast group address on that interface.
Filter Mode	The filter mode of the multicast group on this interface. The values it can take are *`include`* and *`exclude`*.
Version 1 Host Timer	The time remaining until the router assumes there are no longer any MLD version-1 Hosts on the specified interface.
Group Compat Mode	The compatibility mode of the multicast group on this interface. The values it can take are *`MLDv1`* and *`MLDv2`*.

The following table is displayed to indicate all the sources associated with this group.

Field	Description
Source Address	The IP address of the source.

Field	Description
Uptime	Time elapsed in hours, minutes, and seconds since the source has been known.
Expiry Time	Time left in hours, minutes, and seconds before the entry is removed.

Example: The following shows examples of CLI display output for the commands.

```
(Routing) #show ipv6 mld groups ?

group-address           Enter Group Address Info.
<slot/port>          Enter interface in slot/port format.


(Routing) #show ipv6 mld groups 0/1

Group Address................................. FF43::3
Interface..................................... 0/1
Up Time (hh:mm:ss)............................ 00:03:04
Expiry Time (hh:mm:ss)........................ ------


(Routing) #show ipv6 mld groups ff43::3

Interface..................................... 0/1
Group Address................................. FF43::3
Last Reporter................................. FE80::200:FF:FE00:3
Up Time (hh:mm:ss)............................ 00:02:53
Expiry Time (hh:mm:ss)........................ ------
Filter Mode................................... Include
Version1 Host Timer........................... ------
Group compat mode............................. v2
Source Address    ExpiryTime
-----------------  -----------
  2003::10        00:04:17
  2003::20        00:04:17
```

10.3.0.8 show ipv6 mld interface

Use this command to display MLD-related information for the interface. The argument *slot/port* corresponds to a physical routing interface or VLAN routing interface. The keyword **vlan** is used to specify the VLAN ID of the routing VLAN directly instead of in a *slot/port* format.

Format `show ipv6 mld interface {slot/port|vlan 1-4093}`

Mode
- Privileged EXEC
- User EXEC

The following information is displayed for each of the interfaces or for only the specified interface.

Field	Description
Interface	The interface number in *slot/port* format.
MLD Mode	Displays the configured administrative status of MLD.
Operational Mode	The operational status of MLD on the interface.
MLD Version	Indicates the version of MLD configured on the interface.

Field	Description
Query Interval	Indicates the configured query interval for the interface.
Query Max Response Time	Indicates the configured maximum query response time (in seconds) advertised in MLD queries on this interface.
Robustness	Displays the configured value for the tuning for the expected packet loss on a subnet attached to the interface.
Startup Query interval	This valued indicates the configured interval between General Queries sent by a Querier on startup.
Startup Query Count	This value indicates the configured number of Queries sent out on startup, separated by the Startup Query Interval.
Last Member Query Interval	This value indicates the configured Maximum Response Time inserted into Group-Specific Queries sent in response to Leave Group messages.
Last Member Query Count	This value indicates the configured number of Group-Specific Queries sent before the router assumes that there are no local members.

The following information is displayed if the operational mode of the MLD interface is enabled.

Field	Description
Querier Status	This value indicates whether the interface is an MLD querier or non-querier on the subnet it is associated with.
Querier Address	The IP address of the MLD querier on the subnet the interface is associated with.
Querier Up Time	Time elapsed in seconds since the querier state has been updated.
Querier Expiry Time	Time left in seconds before the Querier loses its title as querier.
Wrong Version Queries	Indicates the number of queries received whose MLD version does not match the MLD version of the interface.
Number of Joins	The number of times a group membership has been added on this interface.
Number of Leaves	The number of times a group membership has been removed on this interface.
Number of Groups	The current number of membership entries for this interface.

10.3.0.9 show ipv6 mld traffic

Use this command to display MLD statistical information for the router.

Format `show ipv6 mld traffic`

Mode
- Privileged EXEC
- User EXEC

Field	Description
Valid MLD Packets Received	The number of valid MLD packets received by the router.
Valid MLD Packets Sent	The number of valid MLD packets sent by the router.
Queries Received	The number of valid MLD queries received by the router.
Queries Sent	The number of valid MLD queries sent by the router.
Reports Received	The number of valid MLD reports received by the router.
Reports Sent	The number of valid MLD reports sent by the router.
Leaves Received	The number of valid MLD leaves received by the router.
Leaves Sent	The number of valid MLD leaves sent by the router.
Bad Checksum MLD Packets	The number of bad checksum MLD packets received by the router.

Field	Description
Malformed MLD Packets	The number of malformed MLD packets received by the router.

10.3.0.10 clear ipv6 mld counters

Use this command to reset the MLD counters to zero on the specified interface.

Format `clear ipv6 mld` *slot/port*
Mode Privileged EXEC

10.3.0.11 clear ipv6 mld traffic

Use this command to clear all entries in the MLD traffic database.

Format `clear ipv6 mld` *slot/port*
Mode Privileged EXEC

10.4 IPv6 MLD-Proxy Commands

MLD-Proxy is the IPv6 equivalent of IGMP-Proxy. MLD-Proxy commands allow you to configure the network device as well as to view device settings and statistics using either serial interface or telnet session. The operation of MLD-Proxy commands is the same as for IGMP-Proxy: MLD is for IPv6 and IGMP is for IPv4.MGMD is a term used to refer to both IGMP and MLD.

10.4.0.1 ipv6 mld-proxy

Use this command to enable MLD-Proxy on the interface or range of interfaces. To enable MLD-Proxy on the interface, you must enable multicast forwarding. Also, make sure that there are no other multicast routing protocols enabled n the router.

Format `ipv6 mld-proxy`
Mode Interface Config

10.4.0.1.1 no ipv6 mld-proxy

Use this command to disable MLD-Proxy on the router.

Format `no ipv6 mld-proxy`
Mode Interface Config

10.4.0.2 ipv6 mld-proxy unsolicit-rprt-interval

Use this command to set the unsolicited report interval for the MLD-Proxy interface or range of interfaces. This command is only valid when you enable MLD-Proxy on the interface. The value of *interval* is 1-260 seconds.

Default `1`
Format `ipv6 mld-proxy unsolicit-rprt-interval interval`
Mode Interface Config

10.4.0.2.1 no ipv6 mld-proxy unsolicited-report-interval

Use this command to reset the MLD-Proxy router’s unsolicited report interval to the default value.

Format `no ipv6 mld-proxy unsolicit-rprt-interval`
Mode Interface Config

10.4.0.3 ipv6 mld-proxy reset-status

Use this command to reset the host interface status parameters of the MLD-Proxy interface or range of interfaces. This command is only valid when you enable MLD-Proxy on the interface.

Format `ipv6 mld-proxy reset-status`
Mode Interface Config

10.4.0.4 show ipv6 mld-proxy

Use this command to display a summary of the host interface status parameters.

Format `show ipv6 mld-proxy`

Mode
- Privileged EXEC
- User EXEC

The command displays the following parameters only when you enable MLD-Proxy.

Field	Description
Interface Index	The interface number of the MLD-Proxy.
Admin Mode	Indicates whether MLD-Proxy is enabled or disabled. This is a configured value.
Operational Mode	Indicates whether MLD-Proxy is operationally enabled or disabled. This is a status parameter.
Version	The present MLD host version that is operational on the proxy interface.
Number of Multicast Groups	The number of multicast groups that are associated with the MLD-Proxy interface.
Unsolicited Report Interval	The time interval at which the MLD-Proxy interface sends unsolicited group membership report.
Querier IP Address on Proxy Interface	The IP address of the Querier, if any, in the network attached to the upstream interface (MLD-Proxy interface).
Older Version 1 Querier Timeout	The interval used to timeout the older version 1 queriers.
Proxy Start Frequency	The number of times the MLD-Proxy has been stopped and started.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ipv6 mld-proxy
Interface Index..................................... 0/3
Admin Mode.......................................... Enable
Operational Mode.................................... Enable
Version..................................................... 3
Num of Multicast Groups............................. 0
Unsolicited Report Interval......................... 1
Querier IP Address on Proxy Interface........ fe80::1:2:5
Older Version 1 Querier Timeout................. 00:00:00
Proxy Start Frequency.............................
```

10.4.0.5 show ipv6 mld-proxy interface

This command displays a detailed list of the host interface status parameters. It displays the following parameters only when you enable MLD-Proxy.

Format `show ipv6 mld-proxy interface`

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Interface Index	The *slot/port* of the MLD-proxy.

The column headings of the table associated with the interface are as follows:

Term	Definition
Ver	The MLD version.
Query Rcvd	Number of MLD queries received.
Report Rcvd	Number of MLD reports received.
Report Sent	Number of MLD reports sent.
Leaves Rcvd	Number of MLD leaves received. Valid for version 2 only.
Leaves Sent	Number of MLD leaves sent on the Proxy interface. Valid for version 2 only.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ipv6 mld-proxy interface

Interface Index.............................. 0/1

Ver  Query Rcvd  Report Rcvd  Report Sent  Leave Rcvd  Leave Sent
-----------------------------------------------------------------
1      2             0            0            0            2
2      3             0            4          -----        -----
```

10.4.0.6 show ipv6 mld-proxy groups

Use this command to display information about multicast groups that the MLD-Proxy reported.

Format `show ipv6 mld-proxy groups`

Mode
- Privileged EXEC
- User EXEC

Field	Description
Interface	The interface number of the MLD-Proxy.
Group Address	The IP address of the multicast group.
Last Reporter	The IP address of the host that last sent a membership report for the current group, on the network attached to the MLD-Proxy interface (upstream interface).
Up Time (in secs)	The time elapsed in seconds since last created.
Member State	Possible values are: ■ **Idle_Member**. The interface has responded to the latest group membership query for this group. ■ **Delay_Member**. The interface is going to send a group membership report to respond to a group membership query for this group.
Filter Mode	Possible values are **Include** or **Exclude.**
Sources	The number of sources attached to the multicast group.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ipv6 mld-proxy groups

Interface Index.............................. 0/3

Group Address    Last Reporter    Up Time   Member State           Filter Mode  Sources
-------------    -------------- ---------- ----------------- -------------- -------
FF1E::1          FE80::100:2.3    00:01:40  DELAY_MEMBER        Exclude        2
```

```
FF1E::2          FE80::100:2.3    00:02:40  DELAY_MEMBER        Include        1

FF1E::3          FE80::100:2.3    00:01:40  DELAY_MEMBER        Exclude        0

FF1E::4          FE80::100:2.3    00:02:44  DELAY_MEMBER         Include        4
```

10.4.0.7 show ipv6 mld-proxy groups detail

Use this command to display information about multicast groups that MLD-Proxy reported.

Format `show ipv6 mld-proxy groups detail`

Mode
- Privileged EXEC
- User EXEC

Field	Description
Interface	The interface number of the MLD-Proxy.
Group Address	The IP address of the multicast group.
Last Reporter	The IP address of the host that last sent a membership report for the current group, on the network attached to the MLD-Proxy interface (upstream interface).
Up Time (in secs)	The time elapsed in seconds since last created.
Member State	Possible values are: ■ **Idle_Member**. The interface has responded to the latest group membership query for this group. ■ **Delay_Member**. The interface is going to send a group membership report to respond to a group membership query for this group.
Filter Mode	Possible values are **Include** or **Exclude.**
Sources	The number of sources attached to the multicast group.
Group Source List	The list of IP addresses of the sources attached to the multicast group.
Expiry Time	The time left for a source to get deleted.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ipv6 igmp-proxy groups

Interface Index.............................. 0/3

Group Address    Last Reporter    Up Time   Member State           Filter Mode  Sources
-------------  ---------------- ----------- ----------------- ------------ -------
FF1E::1          FE80::100:2.3       244       DELAY_MEMBER     Exclude         2

Group Source List             Expiry Time
------------------          ---------------
2001::1                       00:02:40
2001::2                       --------


FF1E::2          FE80::100:2.3        243      DELAY_MEMBER   Include         1

Group Source List             Expiry Time
------------------          ---------------
3001::1                       00:03:32
```

```
3002::2                       00:03:32


FF1E::3          FE80::100:2.3        328      DELAY_MEMBER   Exclude        0

FF1E::4      FE80::100:2.3        255       DELAY_MEMBER   Include         4

Group Source List             Expiry Time
------------------          ---------------
4001::1                                 00:03:40
5002::2                                 00:03:40
4001::2                                 00:03:40
5002::2                                 00:03:40
```

Chapter 11: Border Gateway Protocol Commands

This section describes the commands you use to view and configure Border Gateway Protocol (BGP), which is an exterior gateway routing protocol that you use to route traffic between autonomous systems. The BGP CLI commands are available in the EFOS software BGP package.

11.1 BGP Commands

11.1.0.1 router bgp

This command enables BGP and identifies the autonomous system (AS) number of the router. Only a single instance of BGP can be run and the router can only belong to a single AS.

Default `BGP is inactive by default.`
Format `router bgp as-number`
Mode Global Config

Parameter	Description
as-number	The router's autonomous system number (ASN). The `as-number` ranges from 1-429496729.

11.1.0.1.1 no router bgp

If you invoke **no router bgp**, BGP is disabled and all BGP configuration reverts to default values. Alternatively, you can use Section 11.1.0.33.1, no enable (BGP) in BGP Router Configuration mode to disable BGP globally without clearing the BGP configuration.

Default `BGP is inactive by default.`
Format `no router bgp as-number`
Mode Global Config

11.1.0.2 address-family

To configure policy parameters within a peer template to be applied to a specific address family, use the **address-family** command in Peer Template Configuration mode. This command enters an Address Family Configuration mode within the peer template. Policy commands configured within this mode apply to the address family. The following commands can be added to a peer template in Address Family Configuration mode:

- activate
- advertisement-interval seconds
- default-originate
- filter-list as-path-list-number {in | out}
- maximum-prefix {maximum | unlimited} [threshold]
- next-hop-self
- prefix-list prefix-list-name {in | out}
- remove-private-as [all replace-as]

- route-map map-name {in | out}
- route-reflector-client
- send-community

The `activate` command is not available in Address-family IPv4 mode.

In Address-family L2VPN mode, only `maximum-prefix`, `route-map`, r`oute-reflector-client`, and `send-community` commands are available.

If an IPv6 peer inherits a template that specifies address-family IPv4 parameters, those parameters are ignored.

Format `address-family {ipv4 | ipv6 | l2vpn evpn}`

Mode Peer Template Config

Parameter	Description
ipv4	Configure policy parameters to be applied to IPv4 routes.
ipv6	Configure policy parameters to be applied to IPv6 routes.
l2vpn evpn	Configure policy parameters to be applied to L2VPN routes.

Example: In the following example of the command, the peer template AGGR sets the keepalive timer to 3 seconds, the hold timer to 9 seconds, allows communities to be sent for both IPv4 and IPv6 routes, and configures different inbound and outbound route maps for IPv4 and IPv6. Two neighbors, 172.20.1.2 and 172.20.2.2, inherit these parameters from the template.

```
(R1) (Config)# router bgp 65000
(R1) (Config-router)# neighbor 172.20.1.2 remote-as 65001
(R1) (Config-router)# neighbor 172.20.2.2 remote-as 65001
(R1) (Config-router)# template peer AGGR
(R1) (Config-rtr-tmplt)# timers 3 9
(R1) (Config-rtr-tmplt)# address-family ipv4
(R1) (Config-rtr-tmplt-af)# send-community
(R1) (Config-rtr-tmplt-af)# route-map RM4-IN in
(R1) (Config-rtr-tmplt-af)# route-map RM4-OUT out
(R1) (Config-rtr-tmplt-af)# exit
(R1) (Config-rtr-tmplt)# address-family ipv6
(R1) (Config-rtr-tmplt-af)# send-community
(R1) (Config-rtr-tmplt-af)# route-map RM6-IN in
(R1) (Config-rtr-tmplt-af)# route-map RM6-OUT out
(R1) (Config-rtr-tmplt-af)# exit
(R1) (Config-rtr-tmplt)# exit
(R1) (Config-router)# neighbor 172.20.1.2 inherit peer AGGR
(R1) (Config-router)# neighbor 172.20.2.2 inherit peer AGGR
(R1) (Config-router)# address-family ipv6
(R1) (Config-router)# neighbor 172.20.1.2 activate
(R1) (Config-router)# neighbor 172.20.2.2 activate
```

11.1.0.2.1 no address-family

To delete all policy commands for an address family in a peer template, use the **no** form of this command.

Format `no address-family {ipv4|ipv6}`

Mode Privileged EXEC

Parameter	Description
ipv4	Configure policy parameters to be applied to IPv4 routes.
ipv6	Configure policy parameters to be applied to IPv6 routes.

11.1.0.3 address-family ipv4

To enter IPv4 VRF Address Family Configuration mode to configure BGR VRF parameters, use the **address-family ipv4 vrf** command in BGP Router Configuration mode. Commands entered in this mode enable peering with BGP neighbors in this VRF instance. All the neighbor-specific commands are given in this mode as well.

Default `VRF configuration is disabled by default.`
Format `address-family ipv4 vrf` *`vrf-name`*
Mode BGP Router Config

11.1.0.3.1 no address-family ipv4

Use the **no** form of this command to delete the IPv4 VRF configuration.

Format `no address-family ipv4 vrf` *`vrf-name`*
Mode BGP Router Config

11.1.0.4 address-family ipv6

To enter IPv6 Address Family Configuration mode in order to specify IPv6-specific configuration parameters, use the **address-family ipv6** command in BGP Router Configuration mode. Commands entered in this mode can be used to enable exchange of IPv6 routes, specify IPv6 prefixes to be originated, and configure inbound and outbound policies to be applied to IPv6 routes.

Default `Exchange of IPv6 routes is disabled by default.`
Format `address-family ipv6`
Mode BGP Router Config

11.1.0.4.1 no address-family ipv6

Use the no form of this command to clear all IPv6 address family configuration.

Format `no address-family ipv6`
Mode BGP Router Config

11.1.0.5 address-family vpnv4 unicast

This command enters into VPN4 Address Family Configuration mode and sets up a routing session to carry VPN IPv4 (VPNv4) addresses across the backbone. When an iBGP neighbor is in this mode, each VPNv4 prefix is made globally unique by the addition of an 8-byte Route distinguisher (RD). Only unicast prefixes are carried to its peer.

The following commands are available in VPNv4 address family configuration mode.

- `neighbor` *`ip-address`* `activate`

- `neighbor` *ip-address* `send-community extended`

To exit from the VPNv4 address family mode, use the **exit** command.

Default The VPNv4 address family is disabled.

Format `address-family vpnv4 unicast`

Mode BGP Router Config

Example:

The following example shows how to enter the VPNv4 address family mode and configure neighbor commands:

```
(Router) (Config)# router bgp 10
(Router) (Config-router)# neighbor 1.1.1.1 remote-as 10
(Router) (Config-router)# address-family vpnv4 unicast
(Router) (Config-router-af-vpnv4)# neighbor 1.1.1.1 activate
(Router) (Config-router-af-vpnv4)# neighbor 1.1.1.1 send-community extended
(Router) (Config-router-af-vpnv4)# exit
(Router) (Config-router)#
```

11.1.0.5.1 no address-family vpnv4 unicast

Use the **no** form of this command to delete the configuration done in this mode.

Format `no address-family vpnv4 unicast`

Mode BGP Router Config

11.1.0.6 advertisement-interval (BGP Router Config)

Use this command to configure the minimum time that must elapse between advertisements of the same route to a given neighbor. RFC 4271 recommends the interval for internal peers be shorter than the interval for external peers to enable fast convergence within an autonomous system. This value does not limit the rate of route selection, only the rate of route advertisement. If BGP changes the route to a destination multiple times while waiting for the advertisement interval to expire, only the final result is advertised to the neighbor.

EFOS BGP enforces the advertisement interval by limiting how often phase 3 of the decision process can run for each update group. The interval applies to withdrawals as well as active advertisements.

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Default
- 30 seconds for external peers
- 5 seconds for internal peers

Format `advertisement-interval seconds`

Mode BGP Router Config

Parameter	Description
ip-address	The neighbor’s IP address.
seconds	The minimum time between route advertisement, in seconds. The range is 0 to 600 seconds.

11.1.0.6.1 no advertisement-interval (BGP Router Config)

Use this command to return to the default the minimum time that must elapse between advertisements of the same route to a given neighbor.

Format `no advertisement-interval`
Mode BGP Router Config

11.1.0.7 advertisement-interval (IPv6 Address Family Config)

In IPv6 Address Family mode, this command controls the time between sending Update messages containing IPv6 routes.

EFOS BGP enforces the advertisement interval by limiting how often phase 3 of the decision process can run for each update group. The interval applies to withdrawals as well as active advertisements.

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Default
- 30 seconds for external peers
- 5 seconds for internal peers

Format `advertisement-interval seconds`
Mode IPv6 Address Family Config

Parameter	Description
ip-address	The neighbor's IP address.
seconds	The minimum time between route advertisement, in seconds. The range is 0 to 600 seconds.

11.1.0.7.1 no advertisement-interval (IPv6 Address Family Config)

Use this command to return to the default the minimum time that must elapse between advertisements of the same IPv6 route to a given neighbor.

Format `no advertisement-interval`
Mode IPv6 Address Family Config

11.1.0.8 address-family l2vpn evpn

Use this command in BGP router configuration mode to enter the Layer 2 VPN EVPN configuration mode. BGP neighbor has to be activated in this mode to enable the transmit and receive capability of the EVPN routes with the peer.

Default Not configured
Format `address-family l2vpn evpn`
Mode BGP Router Config

Usage Guidelines

This command takes the user into the Layer 2 VPN EVPN address family configuration mode. The following commands are available in this mode.

- `neighbor ip-address activate`

- `neighbor ip-address send-community extended`
- `neighbor ip-address send-community both`
- `retain route-target all`
- `neighbor ip-address route-map route-map out`
- `neighbor ip-address maximum-prefix { maximum | unlimited } [threshold]`
- `neighbor ip-address route-reflector-client`

Example: The following example shows how to enter the Layer 2 VPN EVPN address family mode and configure the available neighbor commands:

```
(Router) (Config)# route-map permit-all permit 20
(Router) (route-map)# set ip next-hop unchanged
(Router) (route-map)# exit

(Router) (Config)# router bgp 10
(Router) (Config-router)# neighbor 1.1.1.1 remote-as 10
(Router) (Config-router)# address-family l2vpn evpn
(Router) (Config-router-af-evpn)# neighbor 1.1.1.1 activate
(Router) (Config-router-af-evpn)# neighbor 1.1.1.1 send-community extended
(Router) (Config-router-af-evpn)# neighbor 1.1.1.1 route-map permit-all out
(Router) (Config-router-af-evpn)# neighbor 1.1.1.1 maximum-prefix 100
(Router) (Config-router-af-evpn)# neighbor 1.1.1.1 route-reflector-client
(Router) (Config-router-af-evpn)# retain route-target all
(Router) (Config-router-af-evpn)# exit
(Router) (Config-router)#
```

11.1.0.9 aggregate-address (BGP Router Config)

To configure a summary address for BGP, use the **aggregate-address** command in Router Configuration mode. No aggregate addresses are configured by default. Unless the options are specified, the aggregate is advertised with the *ATOMIC_AGGREGATE* attribute and an empty AS path, and the more specific routes are advertised along with the aggregate.

To be considered a match for an aggregate address, a prefix must be more specific (i.e. have a longer prefix length) than the aggregate address. A prefix whose prefix length equals the length of the aggregate address is not considered a match.

When BGP originates a summary address, it installs a reject route in the common routing table for the summary prefix. Any received packets that match the summary prefix, but not a more specific route, match the reject route and are dropped.

BGP accepts up to 128 summary addresses for each address family.

Default	No aggregate addresses are configured by default. Unless the options are specified, the aggregate is advertised with the ATOMIC_AGGREGATE attribute and an empty AS path, and the more specific routes are advertised along with the aggregate.
Format	`aggregate-address {address mask|ipv6-prefix/pfx-len} [as-set] [summary-only]`
Mode	BGP Router Config

Parameter	Description
address mask	Summary IPv4 prefix and mask. The default route (0.0.0.0 0.0.0.0) cannot be configured as an aggregate-address. The mask cannot be a 32-bit mask (255.255.255.255). The combination of prefix and mask must be a valid unicast destination prefix.
ipv6-prefix/pfx-len	Summary IPv6 prefix and prefix length. The range for prefix length is 1 to 127.

Parameter	Description
as-set	(Optional) Normally, the aggregate is advertised with an empty AS path and the *ATOMIC_AGGREGATE* attribute. If the **as-set** option is configured, then the aggregate is advertised with a non-empty AS_PATH. If the AS_PATH of all contained routes is the same, then the AS_PATH of the aggregate is the AS_PATH of the contained routes. Otherwise, if the contained routes have different AS_PATHs, the AS_PATH attribute includes an AS_SET with each of the AS numbers listed in the AS PATHs of the aggregated routes. If the as-set option is not configured, the aggregate is advertised with an empty AS_PATH.
summary-only	(Optional) When the **summary-only** option is given, the more-specific routes within the aggregate address are not advertised to neighbors.

11.1.0.9.1 no aggregate-address

Use this command to delete a summary address for BGP. The *address mask* is a summary prefix and mask.

Format `no aggregate-address address mask`

Mode BGP Router Config

11.1.0.10 aggregate-address (IPv4 VRF Address Family)

To configure a summary address for BGP, use the **aggregate-address** command in Router Configuration mode. No aggregate addresses are configured by default. Unless the options are specified, the aggregate is advertised with the *ATOMIC_AGGREGATE* attribute and an empty AS path, and the more specific routes are advertised along with the aggregate.

To be considered a match for an aggregate address, a prefix must be more specific (i.e. have a longer prefix length) than the aggregate address. A prefix whose prefix length equals the length of the aggregate address is not considered a match.

When BGP originates a summary address, it installs a reject route in the common routing table for the summary prefix. Any received packets that match the summary prefix, but not a more specific route, match the reject route and are dropped.

BGP accepts up to 128 summary addresses for each address family.

Default No aggregate addresses are configured by default. Unless the options are specified, the aggregate is advertised with the ATOMIC_AGGREGATE attribute and an empty AS path, and the more specific routes are advertised along with the aggregate.

Format `aggregate-address address mask [as-set] [summary-only]`

Mode IPv4 VRF Address Family

Parameter	Description
address mask	Summary IPv4 prefix and mask. The default route (0.0.0.0 0.0.0.0) cannot be configured as an aggregate-address. The mask cannot be a 32-bit mask (255.255.255.255). The combination of prefix and mask must be a valid unicast destination prefix.
as-set	(Optional) Normally, the aggregate is advertised with an empty AS path and the *ATOMIC_AGGREGATE* attribute. If the **as-set** option is configured, then the aggregate is advertised with a non-empty AS_PATH. If the AS_PATH of all contained routes is the same, then the AS_PATH of the aggregate is the AS_PATH of the contained routes. Otherwise, if the contained routes have different AS_PATHs, the AS_PATH attribute includes an AS_SET with each of the AS numbers listed in the AS PATHs of the aggregated routes. If the as-set option is not configured, the aggregate is advertised with an empty AS_PATH.
summary-only	(Optional) When the **summary-only** option is given, the more-specific routes within the aggregate address are not advertised to neighbors.

11.1.0.10.1 no aggregate-address

Use this command to delete a summary address for BGP. The *address mask* is a summary prefix and mask.

Format `no aggregate-address address mask`

Mode IPv4 VRF Address Family

11.1.0.11 bgp aggregate-different-meds

Use the **bgp aggregate-different meds** command in BGP Router Configuration mode to allow the aggregation of routes with different MED attributes. By default, BGP only aggregates routes that have the same MED value, as prescribed by RFC 4271.

When this command is given, the path for an active aggregate address is advertised without a MED attribute. When this command is not given, if multiple routes match an aggregate address, but have different MEDs, the aggregate takes the MED of the first matching route. Any other matching prefix with the same MED is included in the aggregate. Matching prefixes with different MEDs are not considered to be part of the aggregate and continue to be advertised as individual routes.

Default All the routes aggregated by a given aggregate address must have the same MED value.

Format `bgp aggregate-different-meds`

Mode
- BGP Router Config
- IPv6 Address Family Config
- IPv4 VRF Address Family

11.1.0.11.1 no bgp aggregate-different-meds

Use the **no bgp aggregate-different meds** command in BGP Router Configuration mode to return the command to the default.

Format `no bgp aggregate-different-meds`

Mode
- BGP Router Config
- IPv6 Address Family Config
- IPv4 VRF Address Family

11.1.0.12 bgp always-compare-med

To compare MED values during the decision process in paths received from different ASs, use the **bgp always-compare med** command. The MED is a 32-bit integer, commonly set by an external peer to indicate the internal distance to a destination. The decision process compares MED values to prefer paths that have a shorter internal distance. Since different ASs may use different internal distance metrics or have different policies for setting the MED, the decision process normally does not compare MED values in paths received from peers in different autonomous systems. This command allows you to force BGP to compare MEDs, regardless of whether paths are received from a common AS.

Default `By default, MED values are only compared for paths received from peers in the same AS.`

Format `bgp always-compare-med`

Mode
- BGP Router Config
- IPv6 Address Family Config
- IPv4 VRF Address Family

11.1.0.12.1 no bgp always-compare-med

Use the no form of this command to revert to the default behavior, only comparing MED values from paths received from neighbors in the same AS.

Format `no bgp always-compare-med`

Mode
- BGP Router Config
- IPv6 Address Family Config
- IPv4 VRF Address Family

11.1.0.13 bgp bestpath as-path ignore

To ignore the AS PATH length in the best path calculation during the decision process, use the `bgp bestpath as-path ignore` command in Router Configuration mode. For IPv6 routes, configure this command in Address Family IPv6 mode. To influence ECMP route calculations, configure the AS PATH parameter.

Default `By default, AS PATH length is not ignored in the BGP best path calculations.`

Format `bgp bestpath as-path ignore`

Mode
- BGP Router Config
- IPv6 Address Family Config
- IPv4 VRF Address Family

11.1.0.13.1 no bgp bestpath as-path ignore

Use the no form of this command to revert to the default behavior, where AS PATH length is not ignored in the BGP best path calculation.

Format `no bgp bestpath as-path ignore`

Mode
- BGP Router Config
- IPv6 Address Family Config
- IPv4 VRF Address Family

11.1.0.14 bgp client-to-client reflection

By default, a route reflector reflects routes received from its clients to its other clients. However, if a route reflector's clients have a full BGP mesh, the route reflector does not reflect to the clients. The *bgp client-to-client reflection* command enables client-to-client reflection for IPv4, IPV6, or IPv4 VRF routes.

Route reflection can change the routes clients select. A route reflector only reflects those routes it selects as best routes. Best route selection can be influenced by the IGP metric of the route to reach the BGP next hop. Since a client's IGP distance to a given next hop may differ from the route reflector's IGP distance, a route reflector may not readvertise a route a client would have selected as best in the absence of route reflection. One way to avoid this effect is to fully mesh the clients within a cluster. When clients are fully meshed, there is no need for the cluster's route reflectors to reflect client routes to other clients within the cluster. When client-to-client reflection is disabled, a route reflector continues to reflect routes from non-clients to clients and from clients to non-clients.

Default `Client-to-client reflection is enabled when a router is configured as a route reflector.`

Format `bgp client-to-client reflection`

Mode
- BGP Router Config
- IPv4 VRF Address Family

11.1.0.14.1 no bgp client-to-client reflection

Format `no bgp client-to-client reflection`

Mode
- BGP Router Config
- IPv4 VRF Address Family

11.1.0.15 bgp cluster-id

Use the *bgp cluster-id* command to specify the cluster ID of a route reflector. To revert the cluster ID to its default, use the `no` form of this command.

A route reflector and its clients form a cluster. Since a cluster with a single route reflector has a single point of failure, a cluster may be configured with multiple route reflectors. To avoid sending multiple copies of a route to a client, each route reflector in a cluster should be configured with the same cluster ID. Route reflectors with the same cluster ID must have the same set of clients; otherwise, some routes may not be reflected to some clients. The same cluster ID is used for both IPv4 and IPv6 route reflection.

Default A route reflector with an unconfigured cluster ID uses its BGP router ID (configured with Section 11.1.0.22, bgp router-id) as the cluster ID.

Format **`bgp cluster-id`** *`cluster-id`*

Mode
- BGP Router Config
- IPv4 VRF Address Family

Parameter	Description
cluster-id	A non-zero 32-bit identifier that uniquely identifies a cluster of route reflectors and their clients. The cluster ID may be entered in dotted notation like an IPv4 address or as an integer.

11.1.0.15.1 no bgp cluster-id

Format `no bgp cluster-id` *`cluster-id`*

Mode
- BGP Router Config
- IPv4 VRF Address Family

11.1.0.16 bgp default local-preference

Use this command to specify the default local preference. Local preference is an attribute sent to internal peers to indicate the degree of preference for a route. A route with a numerically higher local preference value is preferred.

BGP assigns the default local preference to each path received from an external peer. (BGP retains the **LOCAL_PREF** on paths received from internal peers.) BGP also assigns the default local preference to locally-originated paths. If you change the default local preference, BGP automatically initiates a soft inbound reset for all peers to apply the new local preference.

Default If this command is not given, BGP advertises a local preference of 100 in Update messages to internal peers.

Format `bgp default local-preference` *`number`*

Mode
- BGP Router Config
- IPv4 VRF Address Family

Parameter	Description
number	The value to use as the local preference for routes advertised to internal peers. The range is 0 to 4,294,967,295.

11.1.0.16.1 no bgp default local-preference

This command sets the default value of local preference of the BGP router.

Format `no bgp default local-preference`

Mode
- BGP Router Config
- IPv4 VRF Address Family

11.1.0.17 bgp fast-external-failover

Use this command to configure BGP to immediately reset the adjacency with an external peer if the routing interface to the peer goes down. When BGP gets a routing interface down event, BGP drops the adjacency with all external peers whose IPv4 address is in one of the subnets on the failed interface. This behavior can be overridden for specific interfaces using the Section 11.1.0.38, ip bgp fast-external-failover command.

Default Fast external failover is enabled by default.

Format `bgp fast-external-failover`

Mode
- BGP Router Config
- IPv4 VRF Address Family

11.1.0.17.1 no bgp fast-external-failover

Use this command to disable BGP fast-external-failover.

Format `no bgp fast-external-failover`

Mode
- BGP Router Config
- IPv4 VRF Address Family

11.1.0.18 bgp fast-internal-failover

Use this command to configure BGP to immediately reset the adjacency with an internal peer when there is a loss of reachability to an internal peer. BGP tracks the reachability of each internal peer's IP address. If a peer becomes unreachable (that is, the RIB no longer has a non-default route to the peer's IP address), then BGP drops the adjacency.

Default Fast internal failover is enabled by default.

Format `bgp fast-internal-failover`

Mode
- BGP Router Config
- IPv4 VRF Address Family

11.1.0.18.1 no bgp fast-internal-failover

Use this command to return the Section 11.1.0.18, bgp fast-internal-failover command to the default.

Format `no bgp fast-internal-failover`

Mode
- BGP Router Config
- IPv4 VRF Address Family

11.1.0.19 bgp listen

Use this command to activate the IPv4 BGP dynamic neighbors feature and create an IPv4 or IPv6 listen range and associate it with a specified peer template.

Use limit *max-number* to define the global maximum number of IPv4 BGP dynamic neighbors that can be created.

BGP dynamic neighbors are configured using a range of IP addresses and BGP peer groups. Each range can be configured as a subnet IP address. After a subnet range is configured for a BGP peer group, and a TCP session is initiated for an IP address in the subnet range, a new BGP neighbor is dynamically created. Dynamically created neighbors are not displayed in the running-config.

If a template peer name is not specified, all dynamic neighbors that are created will inherit default parameters. The template peer name can be assigned/changed for a listen range in any time.

The total number of both IPv4 and IPv6 listen range groups you can configure are 10.

Default No subnets are associated with a BGP listen subnet range, and the BGP dynamic neighbor feature is not activated.

Format `bgp listen { limit max-number | range network/length [ inherit peer peer-template-name ] }`

Mode
- BGP Router Config
- IPv6 Address Family Config

Parameter	Description
limit *max-number*	Sets a maximum limit number of IPv4 BGP dynamic subnet range neighbors. Number from 1 to 100. Default is 20.
range *network/length*	Specifies a listen subnet range that is to be created. *length* is the IP prefix representing a subnet, and the length of the subnet mask in bits. *network* is a valid IPv4 prefix.
inherit peer *peer-template-name*	(Optional) Specifies a BGP peer template name that is to be associated with the specified listen subnet range and inherited with dynamically created neighbors. The template will be inherited with dynamically created neighbors.

Example:

The following commands show how to create a listen range with a template to be inherited with dynamically created BGP neighbors:

```
(R1) # configure
(R1) (Config) # router bgp 100
```

```
(R1) (Config-router)# bgp listen limit 10
(R1) (Config-router)# bgp listen range 10.12.0.0/16
(R1) (Config-router)# bgp listen range 10.27.0.0/16 inherit peer ABC
```

11.1.0.19.1 no bgp listen

Use this command to deactivate the IPv4 BGP dynamic neighbors feature and delete an IPv4 listen range and deassociate it with a specified peer template.

Format `no bgp listen { limit | range` *`network/length`* `[ inherit peer` *`peer-template-name`* `] }`

Mode BGP Router Config

11.1.0.20 bgp log-neighbor-changes

Use this command to enable logging of adjacency state changes. Both backward and forward adjacency state changes are logged. Forward state changes, except for transitions to the **Established** state, are logged at the **Informational** severity level. Backward state changes and forward changes to **Established** are logged at the **Notice** severity level.

Default Neighbor state changes are not logged by default.

Format `bgp log-neighbor-changes`

Mode
- BGP Router Config
- IPv4 VRF Address Family

11.1.0.20.1 no bgp log-neighbor-changes

Use this command to return the Section 11.1.0.20, bgp log-neighbor-changes command to the default.

Format `no bgp log-neighbor-changes`

Mode
- BGP Router Config
- IPv4 VRF Address Family

11.1.0.21 bgp maxas-limit

To specify a limit on the length of AS Paths that BGP accepts from its neighbors, use the bgp maxas-limit in Router Configuration mode. If BGP receives a path whose AS Path attribute is longer than the configured limit, BGP sends a NOTIFICATION and resets the adjacency.

Default `EFOS BGP accepts AS paths with up to 75 AS numbers.`

Format `bgp maxas-limit number`

Mode
- BGP Router Config
- IPv4 VRF Address Family

Parameter	Description
number	The maximum length of an AS Path that BGP will accept from any of its neighbors. The length is the number of autonomous systems listed in the path. The limit may be set to any value from 1 to 100.

11.1.0.21.1 no bgp maxas-limit

To revert to the default the limit on the length of AS Paths that BGP accepts from its neighbors, use the no form of this command.

Format `no bgp maxas-limit`

Mode
- BGP Router Config
- IPv4 VRF Address Family

11.1.0.22 bgp router-id

Use this command to set the BGP router ID. There is no default BGP router ID. The system does not select a router ID automatically. You must configure one manually.

The BGP router ID must be a valid IPv4 unicast address, but is not required to be an address assigned to the router. The router ID is specified in the dotted notation of an IP address. Setting the router ID to 0.0.0.0 disables BGP. Changing the router ID disables and reenables BGP, causing all adjacencies to be reestablished.

Default 0.0.0.0

Format `bgp router-id router-id`

Mode BGP Router Config

Parameter	Description
router-id	An IPv4 address for BGP to use as its router ID.

11.1.0.22.1 no bgp router-id

Use this command to reset the BGP router ID, disabling BGP.

Format `no bgp router-id router-id`

Mode BGP Router Config

11.1.0.23 default-information originate

Use this command to allow BGP to originate a default route (either BGP, IPv4 VRF, or IPv6, depending on the mode). By default, BGP does not originate a default route. If a default route is redistributed into BGP, BGP does not advertise the default route unless the **default-information originate** command has been given. The **always** option is disabled by default.

Default BGP does not originate a default route. The **always** option is disabled by default.

Format `default-information originate [always]`

Mode
- BGP Router Config
- IPv4 VRF Address Family
- IPv6 Address Family Config

Parameter	Description
always	(Optional) This optional keyword allows BGP to originate a default route, even if the common routing table has no default route.

11.1.0.23.1 no default-information originate

Use this command to disable BGP from originating a default route.

Format `no default-information originate`

Mode
- BGP Router Config
- IPv4 VRF Address Family
- IPv6 Address Family Config

11.1.0.24 default metric

Use this command to set the value of the Multi Exit Discriminator (MED) attribute on redistributed routes (either BGP, IPv4 VRF, or IPv6 routes, depending on the mode) when no metric has been specified in the Section 11.1.0.102, redistribute (BGP Router Config) command.

Default No default metric is set and no MED is included in redistributed routes.

Format `default-metric value`

Mode
- BGP Router Config
- IPv4 VRF Address Family
- IPv6 Address Family Config

Parameter	Description
value	The value to set as the MED. The range is 1 to 4,294,967,295.

11.1.0.24.1 no default metric

Use this command to delete the default for the metric of redistributed routes.

Format `no default-metric`

Mode
- BGP Router Config
- IPv4 VRF Address Family
- IPv6 Address Family Config

11.1.0.25 default-originate (BGP Router Config)

To configure BGP to originate a default route to a specific neighbor, use the neighbor default-originate command in BGP router configuration mode. By default, a neighbor-specific default has no MED and the Origin is IGP. Attributes may be set using an optional route map. A neighbor-specific default is only advertised if the Adj-RIB-Out does not include a default learned by other means, either from the Section 11.1.0.23, default-information originate command or a default learned from a peer. This type of default origination is not conditioned on the presence of a default route in the routing table. This form of default origination does not install a default route in the BGP routing table (it will not appear in the Section 11.1.0.114, show ip bgpcommand), nor does it install a default route in the Adj-RIB-Out for the update group of peers so configured (it will not appear in the Section 11.1.0.122, show ip bgp neighbors advertised-routes command).

Origination of the default route is not subject to a prefix filter configured with the command Section 11.1.0.32, distribute-list prefix out.

A route map may be configured to set attributes on the default route sent to the neighbor. If the route map includes a **match ip-address** term, that term is ignored. If the route map includes **match community** or **match as-path** terms, the default route is not advertised. If there is no route map with the route map name given, the default route is not advertised.

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Default No default is originated by default.

Format `default-originate [route-map` *`map-name`*`]`

Mode BGP Router Config

Parameter	Description
map-name	(Optional) A route map may be configured to set attributes on the default route advertised to the neighbor.

11.1.0.25.1 no default-originate (BGP Router Config)

Use this command to prevent BGP from originating a default route to a specific neighbor.

Format `no default-originate`

Mode BGP Router Config

11.1.0.26 neighbor default-originate (IPv6 Address Family Config)

To configure BGP to originate a default IPv6 route to a specific neighbor, use the **neighbor default-originate** command in IPv6 Address Family configuration mode. By default, a neighbor-specific default has no MED and the Origin is IGP. Attributes may be set using an optional route map. A neighbor-specific default is only advertised if the Adj-RIB-Out does not include a default learned by other means, either from the Section 11.1.0.23, default-information originate command or a default learned from a peer. This type of default origination is not conditioned on the presence of a default route in the routing table. This form of default origination does not install a default route in the BGP routing table (it will not appear in the Section 11.1.0.114, show ip bgpcommand), nor does it install a default route in the Adj-RIB-Out for the update group of peers so configured (it will not appear in the Section 11.1.0.122, show ip bgp neighbors advertised-routes command).

Origination of the default route is not subject to a prefix filter configured with the command Section 11.1.0.32, distribute-list prefix out.

A route map may be configured to set attributes on the default route sent to the neighbor. If the route map includes a **match ip-address** term, that term is ignored. If the route map includes **match community** or **match as-path** terms, the default route is not advertised. If there is no route map with the route map name given, the default route is not advertised.

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Default No default is originated by default.

Format `default-originate [route-map` *`map-name`*`]`

Mode IPv6 Address Family Config

Parameter	Description
map-name	(Optional) A route map may be configured to set attributes on the default route advertised to the neighbor.

11.1.0.26.1 no default-originate (IPv6 Address Family Config)

Use this command to prevent BGP from originating a default IPv6 route to a specific neighbor.

Format `no default-originate [route-map` *`map-name`*`]`

Mode IPv6 Address Family Config

11.1.0.27 distance (BGP Router Config)

Use this command to set the preference (also known as administrative distance) of BGP routes to specific destinations. You may enter up to 128 instances of this command. Two instances of this command may not have the same prefix and wildcard mask. If a distance command is configured that matches an existing distance command's prefix and wildcard mask, the new command replaces the existing command. There can be overlap between the prefix and mask configured for different commands. When there is overlap, the command whose prefix and wildcard mask are the longest match for a neighbor's address is applied to routes from that neighbor.

An ECMP route's distance is determined by applying distance commands to the neighbor that provided the best path.

The distance command is not applied to existing routes. To apply configuration changes to the distance command itself or the prefix list to which a distance command applies, you must force a hard reset of affected neighbors.

Default BGP assigns preference values according to the **distance bgp** command, unless overridden for specific neighbors or prefixes by this command.

Format `distance distance [prefix wildcard-mask [prefix-list]]`

Mode BGP Router Config

Parameter	Description
distance	The preference value for matching routes. The range is 1 to 255.
prefix wildcard-mask	[Optional] Routes learned from BGP peers whose address falls within this prefix are assigned the configured distance value. The wildcard-mask is an inverted network mask whose 1 bits indicate the don't care portion of the prefix.
prefix-list	[Optional] A prefix list can optionally be specified to limit the distance value to a specific set of destination prefixes learned from matching neighbors.

Example: The following shows examples of the command.

Example #1: To set the preference value of the BGP route to 100.0.0.0/8 from neighbor 10.1.1.1, use the following **distance** command:

```
(Routing) (Config)# ip prefix-list pfx-list1 permit 100.0.0.0/8
(Routing) (Config)# router bgp 1
(Routing) (Config-router)# distance 25 10.1.1.1 0.0.0.0 pfx-list1
```

Example #2: To set the preference value to 12 for all BGP routes from neighbor 10.1.1.1, use the following distance command:

```
(Routing) (Config-router)# distance 12  10.1.1.1  0.0.0.0
```

Example #3: To set the preference value of all routes within 100.0.0.0/8 from any neighbor, use the following distance command:

```
(Routing) (Config)# ip prefix-list pfx-list2 permit 100.0.0.0/8 ge 8
(Routing) (Config)# router bgp 1
(Routing) (Config-router)#distance 25 0.0.0.0 255.255.255.255 pfx-list2
```

11.1.0.27.1 no distance (BGP Router Config)

Use this command to set the preference of BGP routes to the default.

Format `no distance distance [prefix wildcard-mask [prefix-list]]`

Mode BGP Router Config

11.1.0.28 distance BGP (BGP Router Config)

Use this command to set the preference, (also known as administrative distance), of BGP routes. Different distance values can be configured for routes learned from external peers, routes learned from internal peers, and BGP routes locally originated. A route with a lower preference value is preferred to a route with a higher preference value to the same destination. Routes with a preference of 255 may not be selected as best routes and used for forwarding.

The change to the default BGP distances does not affect existing routes. To apply a distance change to existing routes, you must force the routes to be deleted from the RIB and relearned, either by resetting the peers from which the routes are learned or by disabling and reenabling BGP.

Default
- external – 20
- internal – 200
- local – 200

Format `distance bgp external-distance internal-distance local-distance`

Mode BGP Router Config

Parameter	Description
external-distance	The preference value for routes learned from external peers. The range is 1 to 255.
internal-distance	The preference value for routes learned from internal peers. The range is 1 to 255.
local-distance	The preference value for locally-originated routes. The range is 1 to 255.

11.1.0.28.1 no distance BGP (BGP Router Config)

Use this command to set the default route preference value of BGP routes in the router.

Format `no distance bgp`

Mode BGP Router Config

11.1.0.29 distance BGP (IPv4 VRF Address Family)

Use this command to set the preference, (also known as administrative distance), of BGP routes. Different distance values can be configured for routes learned from external peers, routes learned from internal peers, and BGP routes locally originated. A route with a lower preference value is preferred to a route with a higher preference value to the same destination. Routes with a preference of 255 may not be selected as best routes and used for forwarding.

The change to the default BGP distances does not affect existing routes. To apply a distance change to existing routes, you must force the routes to be deleted from the RIB and relearned, either by resetting the peers from which the routes are learned or by disabling and re-enabling BGP.

Default
- external – 20
- internal – 200
- local – 200

Format `distance bgp external-distance internal-distance local-distance`

Mode IPv4 VRF Address Family

Parameter	Description
external-distance	The preference value for routes learned from external peers. The range is 1 to 255.
internal-distance	The preference value for routes learned from internal peers. The range is 1 to 255.
local-distance	The preference value for locally-originated routes. The range is 1 to 255.

11.1.0.29.1 no distance BGP (IPv4 VRF Address Family)

Use this command to set the default route preference value of BGP routes in the router.

Format `no distance bgp`

Mode IPv4 VRF Address Family

11.1.0.30 distance BGP (IPv6 Address Family Config)

Use this command to set the preference, (also known as administrative distance), for eBGP, iBGP, and locally-originated BGP IPv6 routes. Different distance values can be configured for routes learned from external peers, routes learned from internal peers, and BGP routes locally originated. A route with a lower preference value is preferred to a route with a higher preference value to the same destination. Routes with a preference of 255 may not be selected as best routes and used for forwarding.

The change to the default BGP distances does not affect existing routes. To apply a distance change to existing routes, you must force the routes to be deleted from the RIB and relearned, either by resetting the peers from which the routes are learned or by disabling and reenabling BGP.

Default
- external – 20
- internal – 200
- local – 200

Format `distance bgp external-distance internal-distance local-distance`

Mode IPv6 Address Family Config

Parameter	Description
external-distance	The preference value for routes learned from external peers. The range is 1 to 255.
internal-distance	The preference value for routes learned from internal peers. The range is 1 to 255.
local-distance	The preference value for locally-originated routes. The range is 1 to 255.

11.1.0.30.1 no distance BGP (IPv6 Address Family Config)

Use this command to set the default route preference value for eBGP, iBGP, and locally-originated BGP IPv6 routes in the router.

Format `no distance bgp`

Mode IPv6 Address Family Config

11.1.0.31 distribute-list prefix in

Use this command to configure a filter that restricts the routes that BGP accepts from all neighbors based on destination prefix. The distribute list is applied to all routes received from all neighbors. Only routes permitted by the prefix list are accepted. If the command refers to a prefix list that does not exist, the command is accepted and all routes are permitted.

Default No distribute lists are defined by default.

Format `distribute-list prefix list-name in`

Mode
- BGP Router Config
- IPv4 VRF Address Family Config

Parameter	Description
list-name	A prefix list used to filter routes received from all peers based on destination prefix.

11.1.0.31.1 no distribute-list prefix in

Use this command to disable a filter that restricts the routes that BGP accepts from all neighbors based on destination prefix.

Format `no distribute-list prefix list-name in`

Mode
- BGP Router Config
- IPv4 VRF Address Family Config

11.1.0.32 distribute-list prefix out

Use this command to configure a filter that restricts the advertisement of routes based on destination prefix. Only one instance of this command may be defined for each route source (RIP, OSPF, static, connected). One instance of this command may also be configured as a global filter for outbound prefixes.

If the command refers to a prefix list that does not exist, the command is accepted and all routes are permitted.

When a distribute list is added, changed, or deleted for route redistribution, BGP automatically reconsiders all best routes.

Default No distribute lists are defined by default.

Format `distribute-list prefix list-name out [ protocol | connected | static ]`

Mode
- BGP Router Config
- IPv4 VRF Address Family Config

Parameter	Description
prefix list-name	A prefix list used to filter routes advertised to neighbors.

Parameter	Description
protocol|connected|static	(Optional) When a route source is specified, the distribute list applies to routes redistributed from that source. Only routes that pass the distribute list are redistributed. The protocol value may be either **rip** or **ospf**.

11.1.0.32.1 no distribute-list prefix out

Use this command to reset the **distribute-list out (BGP)** command to the default.

Format `no distribute-list prefix list-name out [ protocol | connected | static ]`

Mode
- BGP Router Config
- IPv4 VRF Address Family Config

11.1.0.33 enable (BGP)

This command globally enables BGP, while retaining the configuration. BGP is enabled by default once you specify the local AS number with the Section 11.1.0.1, router bgp command and configure a router ID with the Section 11.1.0.21, bgp maxas-limit command. When you disable BGP, BGP retains its configuration. If you invoke the Section 11.1.0.1.1, no router bgp command, all BGP configuration is reset to the default values.

When BGP is administratively disabled, BGP sends a **Notification** message to each peer with a Cease error code.

Format `enable`

Mode BGP Router Config

11.1.0.33.1 no enable (BGP)

This command globally disables the administrative mode of BGP on the system, while retaining the configuration.

Format `no enable`

Mode BGP Router Config

11.1.0.34 filter-list (BGP Router Config)

This command filters advertisements to or from a specific neighbor according to the advertisement's AS Path. Only a single AS path list can be configured in each direction for each neighbor. If you invoke the command a second time for a given neighbor, the new AS path list number replaces the previous AS path list number.

If you assign a neighbor filter list to a nonexistent AS path access list, all routes are filtered. Issue this command in Address Family Configuration Mode to add it to a peer template.

Default No neighbor filter lists are configured by default.

Format `filter-list` *`as-path-list-number`* `{in | out}`

Mode BGP Router Config

Parameter	Description
as-path-list-number	Identifies an AS path list.
in	The AS Path list is applied to advertisements received from the neighbor.

Parameter	Description
out	The AS Path list is applied to advertisements to be sent to the neighbor.

11.1.0.34.1 no filter-list (BGP Router Config)

Use this command to unconfigure neighbor filter lists.

Format `filter-list` *`as-path-list-number`* `{in | out}`
Mode BGP Router Config

11.1.0.35 filter-list (IPv6 Address Family Config)

This command filters BGP to apply an AS path access list to UPDATE messages received from or sent to a specific neighbor. Filtering for IPv6 is independent of filtering configured for IPv4. If an UPDATE message includes both IPv4 and IPv6 NLRI, it could be filtered for IPv4 but accepted for IPv6 or vice versa.

If you assign a neighbor filter list to a nonexistent AS path access list, all routes are filtered.

Issue this command in Address Family Configuration Mode to add it to a peer template.

Default No neighbor filter lists are configured by default.
Format `filter-list` *`as-path-list-number`* `{in | out}`
Mode IPv6 Address Family Config

Parameter	Description
as-path-list-number	Identifies an AS path list.
in	The AS Path list is applied to advertisements received from the neighbor.
out	The AS Path list is applied to advertisements to be sent to the neighbor.

11.1.0.35.1 no filter-list (IPv6 Address Family Config)

Use this command to unconfigure neighbor IPv6 filter lists.

Format `filter-list` *`as-path-list-number`* `{in | out}`
Mode IPv6 Address Family Config

11.1.0.36 bgp graceful-restart

This command enables the graceful restart capability, as specified in RFC 4724.

Default Disabled
Format `bgp graceful-restart [restart-time restart-time | stalepath-time stalepath-time]`
Mode BGP Router Config

Parameter	Description
restart-time	The maximum time in seconds, before which the graceful restart is supposed to be complete by the restarting router. The allowed range is 1–3600 seconds. The default value is 120 seconds.
stalepath-time	The maximum time that the helper router keeps the stale routes from the restarting BGP peer. The allowed range is 1–3600 seconds. The default value is 300 seconds

11.1.0.36.1 no bgp graceful-restart

This command resets the graceful restart capability to the default value.

Format `no bgp graceful-restart [restart-time | stalepath-time]`
Mode BGP Router Config

11.1.0.37 bgp graceful-restart-helper

This command enables the graceful restart helper capability.

Default Enabled
Format `bgp graceful-restart-helper`
Mode BGP Router Config

11.1.0.37.1 no bgp graceful-restart-helper

This command resets the graceful restart helper capability to the default value.

Format `no bgp graceful-restart-helper`
Mode BGP Router Config

11.1.0.38 ip bgp fast-external-failover

This command configures fast external failover behavior for a specific routing interface.

This command overrides for a specific routing interface the fast external failover behavior configured globally. If **permit** is specified, the feature is enabled on the interface, regardless of the global configuration. If **deny** is specified, the feature is disabled on the interface, regardless of the global configuration.

Default Fast external failover is enabled globally by default. There is no interface configuration by default.
Format `ip bgp fast-external-failover { permit | deny }`
Mode Interface Config

Parameter	Description
permit	This keyword enables fast external failover on the interface, regardless of the global configuration of the feature.
deny	This keyword disables fast external failover on the interface, regardless of the global configuration of the feature.

11.1.0.38.1 no ip bgp fast-external-failover

This command unconfigures the feature on the interface, and the interface uses the global setting.

Format `no ip bgp fast-external-failover`
Mode Interface Config

11.1.0.39 maximum-paths (BGP Router Config)

Use this command to specify the maximum number of next hops BGP may include in an Equal Cost Multipath (ECMP) route derived from paths received from neighbors outside the local autonomous system.

Paths are considered for ECMP when their attributes are the same (local preference, AS path, origin, MED, peer type and IGP distance). When BGP uses multiple paths in an ECMP route, BGP still selects one path as the best path and advertises only that path to its peers.

Default BGP uses a single next hop by default
Format `maximum-paths number-of-paths`
Mode BGP Router Config

Parameter	Description
number-of-paths	The maximum number of next hops in a BGP route. The range is from 1 to 32 unless the platform or SDM template further restricts the range.

11.1.0.39.1 no maximum-paths (BGP Router Config)

This command resets back to the default the number of next hops BGP may include in an ECMP route.

Format `no maximum-paths`
Mode BGP Router Config

11.1.0.40 maximum-paths (IPv4 VRF Address Family Config)

Use this command to specify the maximum number of next hops BGP may include in an Equal Cost Multipath (ECMP) route derived from paths received from neighbors outside the local autonomous system.

Paths are considered for ECMP when their attributes are the same (local preference, AS path, origin, MED, peer type and IGP distance). When BGP uses multiple paths in an ECMP route, BGP still selects one path as the best path and advertises only that path to its peers.

Default BGP uses a single next hop by default
Format `maximum-paths number-of-paths`
Mode IPv4 VRF Address Family Config

Parameter	Description
number-of-paths	The maximum number of next hops in a BGP route. The range is from 1 to 32 unless the platform or SDM template further restricts the range.

11.1.0.40.1 no maximum-paths (IPv4 VRF Address Family Config)

This command resets back to the default the number of next hops BGP may include in an ECMP route.

Format `no maximum-paths`
Mode IPv4 VRF Address Family Config

11.1.0.41 maximum-paths (IPv6 Address Family Config)

Use this command to limit the number of Equal Cost Multipath (ECMP) next hops in IPv6 routes from external peers. BGP may include in an ECMP route derived from paths received from neighbors outside the local autonomous system.

Paths are considered for ECMP when their attributes are the same (local preference, AS path, origin, MED, peer type and IGP distance). When BGP uses multiple paths in an ECMP route, BGP still selects one path as the best path and advertises only that path to its peers.

Default BGP uses a single next hop by default
Format `maximum-paths number-of-paths`
Mode IPv6 Address Family Config

Parameter	Description
number-of-paths	The maximum number of next hops in a BGP route. The range is from 1 to 32 unless the platform or SDM template further restricts the range.

11.1.0.41.1 no maximum-paths (IPv6 Address Family Config)

This command resets back to the default the number of ECMP next hops in IPv6 routes BGP may include in an ECMP route.

Format `no maximum-paths`
Mode IPv6 Address Family Config

11.1.0.42 maximum-paths igbp (BGP Router Config)

Use this command to specify the maximum number of next hops BGP may include in an Equal Cost Multipath (ECMP) route derived from paths received from neighbors within the local autonomous system.

Paths are considered for ECMP when their attributes are the same (local preference, AS path, origin, MED, peer type, and IGP distance). When BGP uses multiple paths in an ECMP route, BGP still selects one path as the best path and advertises only that path to its peers.

Default BGP uses a single next hop by default.
Format `maximum-paths igbp number-of-paths`
Mode BGP Router Config

Parameter	Description
number-of-paths	The maximum number of next hops in a BGP router. The range is from 1 to 32 unless the platform or SDM template further restricts the range.

11.1.0.42.1 no maximum-paths igbp (BGP Router Config)

Use this command to reset back to the default the number of next hops BGP may include in an ECMP route derived from paths received from neighbors within the local autonomous system.

Format `no maximum-paths igbp`
Mode BGP Router Config

11.1.0.43 maximum-paths igbp (IPv4 VRF Address Family Config)

Use this command to specify the maximum number of next hops BGP may include in an Equal Cost Multipath (ECMP) route derived from paths received from neighbors within the local autonomous system.

Paths are considered for ECMP when their attributes are the same (local preference, AS path, origin, MED, peer type, and IGP distance). When BGP uses multiple paths in an ECMP route, BGP still selects one path as the best path and advertises only that path to its peers.

Default BGP uses a single next hop by default.
Format `maximum-paths igbp number-of-paths`
Mode IPv4 VRF Address Family Config

Parameter	Description
number-of-paths	The maximum number of next hops in a BGP router. The range is from 1 to 32 unless the platform or SDM template further restricts the range.

11.1.0.43.1 no maximum-paths igbp (IPv4 VRF Address Family Config)

Use this command to reset back to the default the number of next hops BGP may include in an ECMP route derived from paths received from neighbors within the local autonomous system.

Format `no maximum-paths igbp`
Mode IPv4 VRF Address Family Config

11.1.0.44 maximum-paths igbp (IPv6 Address Family Config)

Use this command to limit the number of ECMP next hops in IPv6 routes from internal peers.

Paths are considered for ECMP when their attributes are the same (local preference, AS path, origin, MED, peer type, and IGP distance). When BGP uses multiple paths in an ECMP route, BGP still selects one path as the best path and advertises only that path to its peers.

Default BGP uses a single next hop by default.
Format `maximum-paths igbp number-of-paths`
Mode IPv6 Address Family Config

Parameter	Description
number-of-paths	The maximum number of next hops in a BGP router. The range is from 1 to 32 unless the platform or SDM template further restricts the range.

11.1.0.44.1 no maximum-paths igbp (IPv6 Address Family Config)

Use this command to reset back to the default the number of ECMP next hops BGP may include in an ECMP route derived from IPv6 routes received from neighbors within the local autonomous system.

Format `no maximum-paths igbp`

Mode IPv6 Address Family Config

11.1.0.45 maximum-prefix (BGP Router Config)

This command configures the maximum number of prefixes that BGP will accept from a specified neighbor. The prefix limit is compared against the number of prefixes received from the neighbor, including prefixes that are rejected by inbound policy. If the peering session is shut down, the adjacency stays down until the Section 11.1.0.112, clear ip bgp command is issued for the neighbor. The neighbor can also be brought back up using the Section 11.1.0.83, neighbor route-map (BGP Router Config) command followed by the command Section 11.1.0.92.1, no neighbor shutdown.

Issue this command in Address Family Configuration Mode to add it to a peer template.

Default By default the prefix limit is set to the maximum number of routes that can be installed in the forwarding table. The default warning threshold is 75%. A neighbor that exceeds the limit is shutdown unless the **warning-only** option is configured.

Format `maximum-prefix { maximum | unlimited } [threshold] [warning-only]`

Mode BGP Router Config

Parameter	Description
maximum	The maximum number of prefixes BGP will accept from this neighbor. Range is 0 to the maximum number of routes the router supports.
unlimited	Do not enforce any prefix limit.
threshold	(Optional) When the number of prefixes received from the neighbor exceeds this percentage of the maximum, BGP writes a log message. The range is 1 to 100 percent. The default is 75%.
warning-only	(Optional) If BGP receives more than the maximum number of prefixes, BGP accepts excess prefixes and writes a log message rather than shutting down the adjacency.

11.1.0.45.1 no maximum-prefix (BGP Router Config)

This command reverts to the default value for the maximum the number of prefixes that BGP will accept from a specified neighbor.

Format `no maximum-prefix`

Mode BGP Router Config

11.1.0.46 maximum-prefix (IPv6 Address Family Config)

This command specifies the maximum number of IPv6 prefixes that BGP will accept from a specified neighbor. The prefix limit is compared against the number of prefixes received from the neighbor, including prefixes that are rejected by inbound policy. If the peering session is shut down, the adjacency stays down until the Section 11.1.0.112, clear ip bgp command is issued for the neighbor. The neighbor can also be brought back up using the Section 11.1.0.92, neighbor shutdown command followed by the command Section 11.1.0.92.1, no neighbor shutdown.

Issue this command in Address Family Configuration Mode to add it to a peer template.

Default By default the prefix limit is set to the maximum number of routes that can be installed in the forwarding table. The default warning threshold is 75%. A neighbor that exceeds the limit is shutdown unless the **warning-only** option is configured.

Format `maximum-prefix { maximum | unlimited } [threshold] [warning-only]`

Mode IPv6 Address Family Config

Parameter	Description
maximum	The maximum number of prefixes BGP will accept from this neighbor. Range is 0 to the maximum number of routes the router supports.
unlimited	Do not enforce any prefix limit.
threshold	(Optional) When the number of prefixes received from the neighbor exceeds this percentage of the maximum, BGP writes a log message. The range is 1 to 100 percent. The default is 75 %.
warning-only	(Optional) If BGP receives more than the maximum number of prefixes, BGP accepts excess prefixes and writes a log message rather than shutting down the adjacency.

11.1.0.46.1 no maximum-prefix (IPv6 Address Family Config)

This command reverts to the default value for the maximum the number of prefixes that BGP will accept from a specified neighbor.

Format `no maximum-prefix`

Mode IPv6 Address Family Config

11.1.0.47 neighbor activate (IPv4 VRF/VPNv4/L2VPN Address Family Config)

Use the **neighbor activate** command in IPv4 VRF Address Family Config mode to enable exchange of IPv4 VRF prefixes with a neighbor.

Using this command under the **address-family vpnv4 unicast** mode enables the local BGP router to send VPNv4 prefixes to its BGP peer across the backbone. Each address carried in an NLRI is prefixed with an 8-byte Route distinguisher value.

Using this command under the **address-family l2vpn** mode enables the local BGP router to send L2VPN prefixes to its BGP peer across the backbone. Each address carried in an NLRI is prefixed with an 8-byte Route distinguisher value.

When IPv4 VRF/VPNv4/L2VPN is enabled for a neighbor, the adjacency is brought down and restarted to communicate the change to the peer. It is recommended that the user completely configures all the required IPv4 routing policies for the peer before activating the peer.

When L2VPN is disabled for a neighbor, the configured commands for L2VPN address family will be cleared and set the default configuration in L2VPN EVPN address family.

Default	IPv4 VRF/VPNv4/L2VPN prefixes are not sent to the neighbor
Format	`neighbor` ***`prefix`*** `activate`
Mode	IPv4 VRF Address Family Config VPNv4 Address Family Config L2VPN Address Family Config

Parameter	Description
prefix	An IPv4 address in dotted notation.

Example:

The following example enables the exchange of VPNv4 and L2VPN prefixes with the external peer at 1.1.1.1.

```
(R1) (Config)# router bgp 1
(R1) (Config-router)# neighbor 1.1.1.1 remote-as 2
(R1) (Config-router)# address-family vpnv4 unicast
(R1) (Config-router-af-vpnv4)# neighbor 1.1.1.1 activate
(R1) (Config-router-af-vpnv4)# exit
(R1) (Config-router)# address-family l2vpn evpn
(R1) (config-router-af-l2vpn-evpn)# neighbor 1.1.1.1 activate
```

11.1.0.47.1 no neighbor activate (IPv4 VRF/VPNv4/L2VPN

Use the **no** form of this command to disable exchange of IPv4 VRF/VPNv4/L2VPN prefixes with the neighbor and to disassociate the export map for the specified VRF instance.

Format	`no neighbor` ***`prefix`*** `activate`
Mode	IPv4 VRF Address Family Config VPNv4 Address Family Config L2VPN Address Family Config

11.1.0.48 neighbor activate (IPv6)

To enable exchange of IPv6 routes with a neighbor, use the neighbor activate command in IPv6 Address Family Configuration mode. The neighbor address must be the same IP address used in the neighbor remote-as command to create the peer.

When IPv6 is enabled or disabled for a neighbor, the adjacency is brought down and restarted to communicate to the change to the peer. You should completely configure IPv6 policy for the peer before activating the peer.

Default	Exchange of IPv6 routes is disabled by default.
Format	`neighbor {`***`ipv4-address`*** `|` ***`ipv6-address`*** `[interface` ***`interface-name`***`]	autodetect interface` ***`interface-name`***`} activate`
Mode	IPv6 Address Family Config

Parameter	Description
ipv4-address	The IPv4 address of a peer.
ipv6-address	The IPv6 address of a peer.

Parameter	Description
interface	If the neighbor's IPv6 address is a link local address, the local interface must also be specified.
autodetect interface	The routing interface on which the neighbor's link local IPv6 address is auto detected.

Example: The following example enables the exchange of IPv6 routes with the external peer at 172.20.1.2 and sets the next hop for IPv6 routes sent to that peer.

```
(R1) (Config)# router bgp 1
(R1) (Config-router)# neighbor 172.20.1.2 remote-as 2
(R1) (Config-router)# address-family ipv6
(R1) (Config-router-af)# neighbor 172.20.1.2 activate
(R1) (Config-router-af)# neighbor 172.20.1.2 route-map SET-V6-NH out
(R1) (Config-router-af)# exit
(R1) (Config-router)# exit
(R1) (Config)# route-map SET-V6-NH permit 10
(R1) (route-map)# set ipv6 next-hop 2001:1:200::1
```

11.1.0.48.1 no neighbor activate

Use the no version of the command to disable exchange of IPv6 routes.

Format `no neighbor` *`ipv4-address`* `activate`

Mode IPv6 Address Family Config

Parameter	Description
ipv4-address	The IPv4 address of a peer.

11.1.0.49 neighbor advertisement-interval (BGP Router Config)

Use this command to configure the minimum time that must elapse between advertisements of the same route to a given neighbor. RFC 4271 recommends the interval for internal peers be shorter than the interval for external peers to enable fast convergence within an autonomous system. This value does not limit the rate of route selection, only the rate of route advertisement. If BGP changes the route to a destination multiple times while waiting for the advertisement interval to expire, only the final result is advertised to the neighbor.

EFOS BGP enforces the advertisement interval by limiting how often phase 3 of the decision process can run for each update group. The interval applies to withdrawals as well as active advertisements.

Default
- 30 seconds for external peers
- 5 seconds for internal peers

Format `neighbor {ipv4-address | ipv6-address} advertisement-interval seconds`

Mode BGP Router Config

Parameter	Description
ipv4-address|ipv6-address	The neighbor's IP address.
seconds	The minimum time between route advertisement, in seconds. The range is 0 to 600 seconds.

11.1.0.49.1 no neighbor advertisement-interval (BGP Router Config)

Use this command to return to the default the minimum time that must elapse between advertisements of the same route to a given neighbor.

Format `no neighbor ip-address advertisement-interval`

Mode BGP Router Config

11.1.0.50 neighbor allowas-in (BGP Router Config)

Use this command to configure BGP to accept prefixes even if local ASN is part of the AS_PATH attribute.

A neighbor can inherit this configuration from a peer template.

Default Disabled

Format `neighbor {ipv4-address | ipv6-address [interface` ***`interface-name`***`] | autodetect interface` ***`interface-name`***`} allowas-in`

Mode BGP Router Config

Parameter	Description
ipv4-address	The neighbor's IPv4 address.
ipv6-address **[interface interface-name]**	The neighbor's IPv6 address. If the neighbor's IPv6 address is a link local address, the local interface must also be specified.
autodetect interface ***interface-name***	The routing interface on which the neighbor's link local IPv6 address is auto detected.
allowas-in ***count***	The maximum no of occurrences of the local ASN allowed in the AS_PATH attribute received in the prefix updates. The allowed range is 1 to 10.

Example:

```
(R1) (Config)# router bgp 65000
(R1) (Config-router)# neighbor 172.20.1.2 remote-as 65001
(R1) (Config-router)# neighbor 172.20.1.2 allowas-in 1
(R1) (Config-router)# neighbor 2001::2 remote-as 65003
(R1) (Config-router)# neighbor 2001::2 allowas-in 3
```

11.1.0.50.1 no neighbor allowas-in (BGP Router Config)

Use this command to prevent BGP from accepting prefixes even if local ASN is part of the AS_PATH attribute.

Format `no neighbor { ip-address | ipv6-address [ interface interface-name ] | autodetect interface interface-name } allowas-in`

Mode BGP Router Config

11.1.0.51 neighbor advertisement-interval (IPv4 VRF Address Family Config)

Use this command to configure the minimum time that must elapse between advertisements of the same route to a given neighbor. RFC 4271 recommends the interval for internal peers be shorter than the interval for external peers to enable fast convergence within an autonomous system. This value does not limit the rate of route selection, only the rate of route advertisement. If BGP changes the route to a destination multiple times while waiting for the advertisement interval to expire, only the final result is advertised to the neighbor.

EFOS BGP enforces the advertisement interval by limiting how often phase 3 of the decision process can run for each update group. The interval applies to withdrawals as well as active advertisements.

Default
- 30 seconds for external peers
- 5 seconds for internal peers

Format `neighbor ip-address advertisement-interval seconds`

Mode IPv4 VRF Address Family Config

Parameter	Description
ip-address	The neighbor's IPv4 address.
seconds	The minimum time between route advertisement, in seconds. The range is 0 to 600 seconds.

11.1.0.51.1 no neighbor advertisement-interval (IPv4 VRF Address Family Config)

Use this command to return to the default the minimum time that must elapse between advertisements of the same route to a given neighbor.

Format `no neighbor ip-address advertisement-interval`

Mode IPv4 VRF Address Family Config

11.1.0.52 neighbor advertisement-interval (IPv6 Address Family Config)

In IPv6 Address Family mode, this command controls the time between sending Update messages containing IPv6 routes. EFOS BGP enforces the advertisement interval by limiting how often phase 3 of the decision process can run for each update group. The interval applies to withdrawals as well as active advertisements.

Default
- 30 seconds for external peers
- 5 seconds for internal peers

Format `neighbor ip-address advertisement-interval seconds`

Mode IPv6 Address Family Config

Parameter	Description
ip-address	The neighbor's IP address.
seconds	The minimum time between route advertisement, in seconds. The range is 0 to 600 seconds.

11.1.0.52.1 no neighbor advertisement-interval (IPv6 Address Family Config)

Use this command to return to the default the minimum time that must elapse between advertisements of the same IPv6 route to a given neighbor.

Format `no neighbor ip-address advertisement-interval`

Mode IPv6 Address Family Config

11.1.0.53 neighbor connect-retry-interval

Use this command to configure the initial connection retry time for a specific neighbor. If a neighbor does not respond to an initial TCP connection attempt, EFOS retries three times. The first retry is after the retry interval configured with neighbor connect-retry-interval. Each subsequent retry doubles the previous retry interval. So by default, the TCP connection is retried after 2, 4, and 8 seconds. If none of the retries is successful, the adjacency is reset to the IDLE state and the IDLE hold timer is started. BGP skips the retries and transitions to IDLE state if TCP returns an error, such as destination unreachable, on a connection attempt.

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Default `2 seconds`

Format `neighbor {ip-address | ipv6-address [interface` ***`interface-name`***`] | autodetect interface` ***`interface-name`***`} connect-retry-interval retry-time`

Mode
- BGP Router Config
- IPv4 VRF Address Family Config
- Peer Template Config

Parameter	Description
ip-address	The neighbor's IP address.
ipv6-address [interface *interface-name*]	The neighbor's IPv6 address. If the neighbor's IPv6 address is a link local address, the local interface must also be specified.
autodetect interface *interface-name*	The routing interface on which the neighbor's link local iPv6 address is auto-detected.
retry-time	The number of seconds to wait before attempting to establish a TCP connection with a neighbor after a previous attempt failed.

11.1.0.53.1 no neighbor connect-retry-interval

This command resets to the default the initial connection retry time for a specific neighbor.

Format `no neighbor ip-address connect-retry-interval`

Mode
- BGP Router Config
- IPv4 VRF Address Family Config

11.1.0.54 neighbor connect-retry-interval (IPv4 Address Family Config)

Use this command to configure the initial connection retry time for a specific neighbor. If a neighbor does not respond to an initial TCP connection attempt, EFOS retries three times. The first retry is after the retry interval configured with neighbor connect-retry-interval. Each subsequent retry doubles the previous retry interval. So by default, the TCP connection is retried after 2, 4, and 8 seconds. If none of the retries is successful, the adjacency is reset to the IDLE state and the IDLE hold timer is started. BGP skips the retries and transitions to IDLE state if TCP returns an error, such as destination unreachable, on a connection attempt.

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Default `2 seconds`

Format `neighbor {ip-address | autodetect interface` ***`interface-name`***`} connect-retry-interval retry-time`

Mode IPv4 VRF Address Family Config

Parameter	Description
ip-address	The neighbor's IP address.
autodetect interface *interface-name*	The routing interface on which the neighbor's link local iPv6 address is auto-detected.
retry-time	The number of seconds to wait before attempting to establish a TCP connection with a neighbor after a previous attempt failed.

11.1.0.54.1 no neighbor connect-retry-interval (IPv4 Address Family Config)

This command resets to the default the initial connection retry time for a specific neighbor.

Format `no neighbor ip-address connect-retry-interval`

Mode IPv4 VRF Address Family Config

11.1.0.55 neighbor default-originate (BGP Router Config)

To configure BGP to originate a default route to a specific neighbor, use the **neighbor default-originate** command in BGP router configuration mode. Use the optional `if-default-present` parameter to originate the default route to a specific neighbor only if the default route exists in the routing table.

By default, a neighbor-specific default has no MED and the Origin is IGP. Attributes may be set using an optional route map. A neighbor configured with the default-originate is placed in a separate update group from the neighbors that are not configured with this command which means the global default-originate command does not affect the neighbors configured with this command. The global default-originate command is overridden by the default-originate setting for a neighbor if enabled. The AS PATH sent in the default route update sent to the neighbor as a result of this command includes only the originator's AS. Giving the optional if-default-present tells to originate the default route to this neighbor only if the default route is present in the routing table. This form of default origination does not install a default route in the Adj RIB Out for the update group of peers so configured (it will not appear in **show ip bgp neighbor advertised-routes**).

A route map may be configured to set attributes on the default route sent to the neighbor. If the route map includes a **match ip-address** term, that term is ignored. If the route map includes **match community** or **match as-path** terms, the default route is not advertised. If there is no route map with the route map name given, the default route is not advertised.

Default No default is originated by default.

Format `neighbor` *`ip-address`* `default-originate [if-default-present][route-map` *`map-name`*`]`

Mode BGP Router Config

Parameter	Description
ip-address	The neighbor's IPv4 address.
map-name	(Optional) A route map may be configured to set attributes on the default route advertised to the neighbor.

11.1.0.55.1 no neighbor default-originate (BGP Router Config)

Use this command to prevent BGP from originating a default route to a specific neighbor.

Format	`no neighbor` *`ip-address`* `default-originate [if-default-present][route-map` *`map-name`*`]`
Mode	BGP Router Config

11.1.0.56 neighbor default-originate (IPv4 VRF Address Family Config)

To configure BGP to originate a default route to a specific neighbor, use the **neighbor default-originate** command in IPv4 VRF Address Family Config mode. Use the optional `if-default-present` parameter to originate the default route to a specific neighbor only if the default route exists in the routing table.

By default, a neighbor-specific default has no MED and the Origin is IGP. Attributes may be set using an optional route map. A neighbor configured with the default-originate is placed in a separate update group from the neighbors that are not configured with this command which means the global default-originate command does not affect the neighbors configured with this command. The global default-originate command is overridden by the default-originate setting for a neighbor if enabled. The AS PATH sent in the default route update sent to the neighbor as a result of this command includes only the originator's AS. Giving the optional if-default-present tells to originate the default route to this neighbor only if the default route is present in the routing table. This form of default origination does not install a default route in the Adj RIB Out for the update group of peers so configured (it will not appear in **show ip bgp neighbor advertised-routes**).

A route map may be configured to set attributes on the default route sent to the neighbor. If the route map includes a **match ip-address** term, that term is ignored. If the route map includes **match community** or **match as-path** terms, the default route is not advertised. If there is no route map with the route map name given, the default route is not advertised.

Default	No default is originated by default.
Format	`neighbor` *`ip-address`* `default-originate [if-default-present][route-map` *`map-name`*`]`
Mode	IPv4 VRF Address Family Config

Parameter	Description
ip-address	The neighbor's IPv4 address.
map-name	(Optional) A route map may be configured to set attributes on the default route advertised to the neighbor.

11.1.0.56.1 no neighbor default-originate (IPv4 VRF Address Family Config)

Use this command to prevent BGP from originating a default route to a specific neighbor.

Format	`no neighbor` *`ip-address`* `default-originate [if-default-present][route-map` *`map-name`*`]`
Mode	IPv4 VRF Address Family Config

11.1.0.57 neighbor default-originate (IPv6 Address Family Config)

To configure BGP to originate a default IPv6 route to a specific neighbor, use the **neighbor default-originate** command in IPv6 Address Family configuration mode. By default, a neighbor-specific default has no MED and the Origin is IGP. Attributes may be set using an optional route map. A neighbor-specific default is only advertised if the Adj-RIB-Out does not include a default learned by other means, either from the Section 11.1.0.23, default-information originate command or a default learned from a peer. This type of default origination is not conditioned on the presence of a default route in the routing table. This form of default origination does not install a default route in the BGP routing table (it will not appear in the Section 11.1.0.114, show ip bgpcommand), nor does it install a default route in the Adj-RIB-Out for the update group of peers so configured (it will not appear in the Section 11.1.0.122, show ip bgp neighbors advertised-routes command).

Origination of the default route is not subject to a prefix filter configured with the Section 11.1.0.32, distribute-list prefix out command.

A route map may be configured to set attributes on the default route sent to the neighbor. If the route map includes a **match ip-address** term, that term is ignored. If the route map includes **match community** or **match as-path** terms, the default route is not advertised. If there is no route map with the route map name given, the default route is not advertised.

Default No default is originated by default.

Format `neighbor ip-address default-originate [route-map map-name]`

Mode IPv6 Address Family Config

Parameter	Description
ip-address	The neighbor's IP address.
map-name	(Optional) A route map may be configured to set attributes on the default route advertised to the neighbor.

11.1.0.57.1 no neighbor default-originate (IPv6 Address Family Config)

Use this command to prevent BGP from originating a default IPv6 route to a specific neighbor.

Format `no neighbor ip-address default-originate [route-map map-name]`

Mode IPv6 Address Family Config

11.1.0.58 neighbor description

Use this command in BGP Router Config mode to record a text description of a neighbor. The description is informational and has no functional impact.

Default No description is originated by default.

Format `neighbor ip-address autodetect interface interface-name description text`

Mode
- BGP Router Config
- IPv4 VRF Address Family Config
- Peer Template Config

Parameter	Description
ip-address	The neighbor's IP address.
autodetect interface *interface-name*	The routing interface on which the neighbor's link local IPv6 address is auto-detected.
text	Text description of neighbor. Up to 80 characters are allowed.

11.1.0.58.1 no neighbor description

Use this command to delete the text description of a neighbor.

Format `no neighbor ip-address autodetect interface interface-name description`

Mode
- BGP Router Config
- IPv4 VRF Address Family Config
- Peer Template Config

11.1.0.59 neighbor ebgp-multihop

To configure BGP to form neighborship with non-directly-connected external peers, use the **neighbor ebgp-multihop** command.

This command is relevant only for external BGP neighbors. For internal BGP neighbors, the TTL value remains 64 and can't be modified. A neighbor can inherit this configuration from a peer template. To make the update-source config work for external BGP neighbors, **ebgp-multihop** *hop-count* should be configured to increase the TTL value instead of the default TTL of 1.

Issue this command in Peer Template Configuration mode to add it to a peer template.

Default The default value is 1.

Format `neighbor { ip-address | ipv6-address [ interface interface-name ] | autodetect interface interface-name } ebgp-multihop hop-count`

Mode
- BGP Router Config
- Peer Template Config

Parameter	Description
ip-address	The neighbor's IPv4 address.
ipv6-address [interface *interface-name*]	The neighbor's IPv6 address. If the neighbor's IPv6 address is a link local address, the local interface must also be specified.
autodetect interface *interface-name*	The routing interface on which the neighbor's link local IPv6 address is auto-detected.
ebgp-multihop *hop-count*	The maximum hop-count allowed to reach the neighbor. The allowed range is 1-255.

Example:

```
(R1) (Config)# router bgp 65000
(R1) (Config-router)# neighbor 172.20.1.2 remote-as 65001
(R1) (Config-router)# neighbor 172.20.1.2 ebgp-multihop 3
(R1) (Config-router)# neighbor 2001::2 remote-as 65003
(R1) (Config-router)# neighbor 2001::2 ebgp-multihop 4
```

11.1.0.59.1 no neighbor ebgp-multihop

Use this command to remove neighborships.

Format `no neighbor { ip-address | ipv6-address [ interface interface-name ] | autodetect interface interface-name } ebgp-multihop`

Mode
- BGP Router Config
- Peer Template Config

11.1.0.60 neighbor ebgp-multihop (IPv4 Address Family Config)

To configure BGP to form neighborship with non-directly-connected external peers, use the **neighbor ebgp-multihop** command.

This command is relevant only for external BGP neighbors. For internal BGP neighbors, the TTL value remains 64 and can't be modified. A neighbor can inherit this configuration from a peer template. To make the update-source config work for external BGP neighbors, **ebgp-multihop** *hop-count* should be configured to increase the TTL value instead of the default TTL of 1.

Default The default value is 1.

Format `neighbor { ip-address | autodetect interface interface-name } ebgp-multihop hop-count`

Mode IPv4 VRF Address Family Config

Parameter	Description
ip-address	The neighbor's IPv4 address.
autodetect interface *interface-name*	The routing interface on which the neighbor's link local IPv6 address is auto-detected.
ebgp-multihop *hop-count*	The maximum hop-count allowed to reach the neighbor. The allowed range is 1-255.

Example:

```
(R1) (Config)# router bgp 65000
(R1) (Config-router)# neighbor 172.20.1.2 remote-as 65001
(R1) (Config-router)# neighbor 172.20.1.2 ebgp-multihop 3
(R1) (Config-router)# neighbor 2001::2 remote-as 65003
(R1) (Config-router)# neighbor 2001::2 ebgp-multihop 4
```

11.1.0.60.1 no neighbor ebgp-multihop

Use this command to remove neighborships.

Format `no neighbor { ip-address | autodetect interface interface-name } ebgp-multihop`

Mode IPv4 VRF Address Family Config

11.1.0.61 neighbor filter-list (BGP Router Config)

This command filters advertisements to or from a specific neighbor according to the advertisement's AS Path. Only a single AS path list can be configured in each direction for each neighbor. If you invoke the command a second time for a given neighbor, the new AS path list number replaces the previous AS path list number.

If you assign a neighbor filter list to a non-existent AS path access list, all routes are filtered.

Default No neighbor filter lists are configured by default.

Format `neighbor {ipv4-address | ipv6-address} filter-list as-path-list-number {in | out}`

Mode BGP Router Config

Parameter	Description
ip-address	The neighbor's IP address.
as-path-list-number	Identifies an AS path list.
in	The AS Path list is applied to advertisements received from the neighbor.
out	The AS Path list is applied to advertisements to be sent to the neighbor.

11.1.0.61.1 no neighbor filter-list (BGP Router Config)

Use this command to unconfigure neighbor filter lists.

Format `no neighbor ip-address filter-list as-path-list-number {in | out}`

Mode BGP Router Config

11.1.0.62 neighbor filter-list (IPv4 VRF Address Family Config)

This command filters advertisements to or from a specific neighbor according to the advertisement's AS Path. Only a single AS path list can be configured in each direction for each neighbor. If you invoke the command a second time for a given neighbor, the new AS path list number replaces the previous AS path list number.

If you assign a neighbor filter list to a nonexistent AS path access list, all routes are filtered.

Default No neighbor filter lists are configured by default.

Format `neighbor ip-address filter-list as-path-list-number {in | out}`

Mode IPv4 VRF Address Family Config

Parameter	Description
ip-address	The neighbor's IPv4 address.
as-path-list-number	Identifies an AS path list.
in	The AS Path list is applied to advertisements received from the neighbor.
out	The AS Path list is applied to advertisements to be sent to the neighbor.

11.1.0.62.1 no neighbor filter-list (IPv4 VRF Address Family Config)

Use this command to unconfigure neighbor filter lists.

Format `no neighbor ip-address filter-list as-path-list-number {in | out}`

Mode IPv4 VRF Address Family Config

11.1.0.63 neighbor filter-list (IPv6 Address Family Config)

This command filters BGP to apply an AS path access list to UPDATE messages received from or sent to a specific neighbor. Filtering for IPv6 is independent of filtering configured for IPv4. If an UPDATE message includes both IPv4 and IPv6 NLRI, it could be filtered for IPv4 but accepted for IPv6 or vice versa.

If you assign a neighbor filter list to a non-existent AS path access list, all routes are filtered.

Default No neighbor filter lists are configured by default.

Format `neighbor ip-address filter-list as-path-list-number {in | out}`

Mode IPv6 Address Family Config

Parameter	Description
ip-address	The neighbor's IP address.
as-path-list-number	Identifies an AS path list.
in	The AS Path list is applied to advertisements received from the neighbor.
out	The AS Path list is applied to advertisements to be sent to the neighbor.

11.1.0.63.1 no neighbor filter-list (IPv6 Address Family Config)

Use this command to unconfigure neighbor IPv6 filter lists.

Format `no neighbor` *`ip-address`* `filter-list` *`as-path-list-number`* `{in | out}`

Mode IPv6 Address Family Config

11.1.0.64 neighbor inherit peer (BGP Router Config)

To configure a BGP peer to inherit peer configuration parameters from a peer template, use the neighbor inherit peer command in Router Configuration mode. Neighbor session and policy parameters can be configured once in a peer template and inherited by multiple neighbors, eliminating the need to configure the same parameters for each neighbor. Parameters are inherited from the peer template specified and from any templates it inherits from. A neighbor can inherit directly from only one peer template.

Default `No peer configuration parameters are inherited by default.`

Format `neighbor {`*`ip-address`*`| `*`ipv6-address`* `[interface` *`interface-name`*`] autodetect interface` *`interface-name`* `inherit peer` *`template-name`*

Mode BGP Router Config

Parameter	Description
ip-address	The IP address of a neighbor whose configuration parameters are inherited from the peer template.
ipv6-address [interface *interface-name*]	The neighbor's IPv6 address. if the neighbor's IPv6 address is a link local address, the local interface must be specified.
autodetect interface *interface-name*	The routing interface on which the neighbor's link local IPv6 address is auto-detected.
template-name	The name of the peer template whose peer configuration parameters are to be inherited by this neighbor.

Example: The following shows an example of the command.

```
(R1) (Config)# router bgp 65000
(R1) (Config-router)# neighbor 172.20.1.2 remote-as 65001
(R1) (Config-router)# neighbor 172.20.2.2 remote-as 65001
(R1) (Config-router)# template peer AGGR
(R1) (Config-rtr-tmp)# timers 3 9
(R1) (Config-rtr-tmp)# address-family ipv4
(R1) (Config-rtr-tmp-af)# send-community
(R1) (Config-rtr-tmp-af)# route-map RM4-IN in
(R1) (Config-rtr-tmp-af)# route-map RM4-OUT out
(R1) (Config-rtr-tmp-af)# exit
(R1) (Config-rtr-tmp)# exit
(R1) (Config-router)# neighbor 172.20.1.2 inherit peer AGGR
(R1) (Config-router)# neighbor 172.20.2.2 inherit peer AGGR
```

11.1.0.64.1 no neighbor inherit peer (BGP Router Config)

`Use the no neighbor inherit peer command in Router Configuration mode to remove the inheritance.`

Format `no neighbor` *`ip-address`* `inherit peer` *`template-name`*

Mode BGP Router Config

11.1.0.65 neighbor inherit peer (IPv4 Address Family Config)

To configure a BGP peer to inherit peer configuration parameters from a peer template, use the neighbor inherit peer command in Router Configuration mode. Neighbor session and policy parameters can be configured once in a peer template and inherited by multiple neighbors, eliminating the need to configure the same parameters for each neighbor. Parameters are inherited from the peer template specified and from any templates it inherits from. A neighbor can inherit directly from only one peer template.

Default No peer configuration parameters are inherited by default.

Format neighbor {*ip-address*|autodetect interface *interface-name*} inherit peer *template-name*

Mode IPv4 VRF Address Family Config

Parameter	Description
ip-address	The IP address of a neighbor whose configuration parameters are inherited from the peer template.
autodetect interface *interface-name*	The routing interface on which the neighbor's link local IPv6 address is auto-detected.
template-name	The name of the peer template whose peer configuration parameters are to be inherited by this neighbor.

Example: The following shows an example of the command.

```
(R1) (Config)# router bgp 65000
(R1) (Config-router)# neighbor 172.20.1.2 remote-as 65001
(R1) (Config-router)# neighbor 172.20.2.2 remote-as 65001
(R1) (Config-router)# template peer AGGR
(R1) (Config-rtr-tmp)# timers 3 9
(R1) (Config-rtr-tmp)# address-family ipv4
(R1) (Config-rtr-tmp-af)# send-community
(R1) (Config-rtr-tmp-af)# route-map RM4-IN in
(R1) (Config-rtr-tmp-af)# route-map RM4-OUT out
(R1) (Config-rtr-tmp-af)# exit
(R1) (Config-rtr-tmp)# exit
(R1) (Config-router)# neighbor 172.20.1.2 inherit peer AGGR
(R1) (Config-router)# neighbor 172.20.2.2 inherit peer AGGR
```

11.1.0.65.1 no neighbor inherit peer (IPv4 Address Family Config)

Use the no neighbor inherit peer command in Router Configuration mode to remove the inheritance.

Format no neighbor *ip-address* inherit peer *template-name*

Mode IPv4 VRF Address Family Config

11.1.0.66 neighbor local-as (BGP Router Config)

To configure BGP to advertise the local-as instead of the router's own AS in the routes advertised to the neighbor, use the **neighbor local-as** command in Router Configuration mode. This command is only allowed on the external BGP neighbors. A neighbor can inherit this configuration from a peer template.

Default No local AS is configured by default on a peer.

Format neighbor { *ip-address* | *ipv6-address* [interface *interface-name*] | autodetect interface *interface-name* } local-as *as-number* no-prepend replace-as

Mode BGP Router Config

Parameter	Description
ip-address	The neighbor's IPv4 address.
ipv6-address **[interface** ***interface-name*****]**	The neighbor's IPv6 address. If the neighbor's IPv6 address is a link local address, the local interface must also be specified.
autodetect interface ***interface-name***	The routing interface on which the neighbor's link local IPv6 address is auto-detected.
local-as ***as-number***	The AS number to advertise as the local AS in the AS PATH sent to the neighbor.
no-prepend	Does not prepend the local-AS in the AS PATH received in the updates from this neighbor.
replace-as	Replaces the router's own AS with the local-AS in the AS PATH sent to the neighbor.

Example:

```
(R1) (Config)# router bgp 65000
(R1) (Config-router)# neighbor 172.20.1.2 remote-as 65001
(R1) (Config-router)# neighbor 172.20.1.2 local-as 65002 no-prepend replace-as
(R1) (Config-router)# neighbor 2001::2 remote-as 65003
(R1) (Config-router)# neighbor 2001::2 local-as 65002 no-prepend replace-as
```

11.1.0.67 neighbor local-as (IPv4 VRF Address Family Config)

To configure BGP to advertise the local-as instead of the router's own AS in the routes advertised to the neighbor, use the **neighbor local-as** command in Router Configuration mode. This command is only allowed on the external BGP neighbors. A neighbor can inherit this configuration from a peer template.

Default `No local AS is configured by default on a peer.`

Format `neighbor { ip-address | autodetect interface interface-name } local-as as-number no-prepend replace-as`

Mode IPv4 VRF Address Family Config

Parameter	Description
ip-address	The neighbor's IPv4 address.
autodetect interface ***interface-name***	The routing interface on which the neighbor's link local IPv6 address is auto-detected.
local-as ***as-number***	The AS number to advertise as the local AS in the AS PATH sent to the neighbor.
no-prepend	Does not prepend the local-AS in the AS PATH received in the updates from this neighbor.
replace-as	Replaces the router's own AS with the local-AS in the AS PATH sent to the neighbor.

Example:

```
(R1) (Config)# router bgp 65000
(R1) (Config-router)# neighbor 172.20.1.2 remote-as 65001
(R1) (Config-router)# neighbor 172.20.1.2 local-as 65002 no-prepend replace-as
(R1) (Config-router)# neighbor 2001::2 remote-as 65003
(R1) (Config-router)# neighbor 2001::2 local-as 65002 no-prepend replace-as
```

11.1.0.68 neighbor maximum-prefix (BGP Router Config)

This command configures the maximum number of prefixes that BGP will accept from a specified neighbor. The prefix limit is compared against the number of prefixes received from the neighbor, including prefixes that are rejected by inbound policy. If the peering session is shut down, the adjacency stays down until the Section 11.1.0.112, clear ip bgp command is issued for the neighbor. The neighbor can also be brought back up using the Section 11.1.0.83, neighbor route-map (BGP Router Config) command followed by the Section 11.1.0.92.1, no neighbor shutdowncommand.

Default By default the prefix limit is set to the maximum number of routes that can be installed in the forwarding table. The default warning threshold is 75%. A neighbor that exceeds the limit is shutdown unless the **warning-only** option is configured.

Format `neighbor {ipv4-address | ipv6-address} maximum-prefix { maximum | unlimited } [threshold] [warning-only]`

Mode BGP Router Config

Parameter	Description
ipv4-address | ipv6-address	The neighbor's IPv4 or IPv6 address.
maximum	The maximum number of prefixes BGP will accept from this neighbor. Range is 0 to the maximum number of routes the router supports.
unlimited	Do not enforce any prefix limit.
threshold	(Optional) When the number of prefixes received from the neighbor exceeds this percentage of the maximum, BGP writes a log message. The range is 1 to 100 percent. The default is 75%.
warning-only	(Optional) If BGP receives more than the maximum number of prefixes, BGP accepts the excess prefixes and writes a log message rather than shutting down the adjacency.

11.1.0.68.1 no neighbor maximum-prefix (BGP Router Config)

This command reverts to the default value for the maximum the number of prefixes that BGP will accept from a specified neighbor.

Format `no neighbor ip-address maximum-prefix`

Mode BGP Router Config

11.1.0.69 neighbor maximum-prefix (IPv4 VRF Address Family Config)

This command configures the maximum number of prefixes that BGP will accept from a specified neighbor. The prefix limit is compared against the number of prefixes received from the neighbor, including prefixes that are rejected by inbound policy. If the peering session is shut down, the adjacency stays down until the Section 11.1.0.112, clear ip bgp command is issued for the neighbor. The neighbor can also be brought back up using the Section 11.1.0.92, neighbor shutdown command followed by the Section 11.1.0.92.1, no neighbor shutdown command.

Default By default the prefix limit is set to the maximum number of routes that can be installed in the forwarding table. The default warning threshold is 75%. A neighbor that exceeds the limit is shutdown unless the **warning-only** option is configured.

Format `neighbor ip-address maximum-prefix { maximum | unlimited } [threshold] [warning-only]`

Mode IPv4 VRF Address Family Config

Parameter	Description
ip-address	The neighbor's IPv4 address.
maximum	The maximum number of prefixes BGP will accept from this neighbor. Range is 0 to the maximum number of routes the router supports.
unlimited	Do not enforce any prefix limit.
threshold	(Optional) When the number of prefixes received from the neighbor exceeds this percentage of the maximum, BGP writes a log message. The range is 1 to 100 percent. The default is 75%.
warning-only	(Optional) If BGP receives more than the maximum number of prefixes, BGP accepts the excess prefixes and writes a log message rather than shutting down the adjacency.

11.1.0.69.1 no neighbor maximum-prefix (IPv4 VRF Address Family Config)

This command reverts to the default value for the maximum the number of prefixes that BGP will accept from a specified neighbor.

Format `no neighbor ip-address maximum-prefix`

Mode IPv4 VRF Address Family Config

11.1.0.70 neighbor maximum-prefix (IPv6 Address Family Config)

This command specifies the maximum number of IPv6 prefixes that BGP will accept from a specified neighbor. The prefix limit is compared against the number of prefixes received from the neighbor, including prefixes that are rejected by inbound policy. If the peering session is shut down, the adjacency stays down until the Section 11.1.0.112, clear ip bgp command is issued for the neighbor. The neighbor can also be brought back up using the Section 11.1.0.92, neighbor shutdown command followed by the Section 11.1.0.92.1, no neighbor shutdown command.

Default By default the prefix limit is set to the maximum number of routes that can be installed in the forwarding table. The default warning threshold is 75%. A neighbor that exceeds the limit is shutdown unless the **warning-only** option is configured.

Format `neighbor ip-address maximum-prefix { maximum | unlimited } [threshold] [warning-only]`

Mode IPv6 Address Family Config

Parameter	Description
ip-address	The neighbor's IP address.
maximum	The maximum number of prefixes BGP will accept from this neighbor. Range is 0 to the maximum number of routes the router supports.
unlimited	Do not enforce any prefix limit.
threshold	(Optional) When the number of prefixes received from the neighbor exceeds this percentage of the maximum, BGP writes a log message. The range is 1 to 100 percent. The default is 75 %.
warning-only	(Optional) If BGP receives more than the maximum number of prefixes, BGP accepts the excess prefixes and writes a log message rather than shutting down the adjacency.

11.1.0.70.1 no neighbor maximum-prefix (IPv6 Address Family Config)

This command reverts to the default value for the maximum the number of prefixes that BGP will accept from a specified neighbor.

Format `no neighbor ip-address maximum-prefix`
Mode IPv6 Address Family Config

11.1.0.71 neighbor next-hop-self (BGP Router Config)

This command configures BGP to set the next hop attribute to a local IP address when advertising a route to an internal peer. Normally, BGP would retain the next hop attribute received from the external peer.

When the next hop attribute in routes from external peers is retained, internal peers must have a route to the external peer's IP address. This is commonly done by configuring the IGP on the border router to advertise the external (or DMZ) subnet. The next-hop-self option eliminates the need to advertise the external subnet in the IGP.

Default not enabled
Format `neighbor {ipv4-address | ipv6-address} next-hop-self`
Mode BGP Router Config

Parameter	Description
ipv4-address|ipv6-address	The neighbor's IPv4 or IPv6 address.

11.1.0.71.1 no neighbor next-hop-self (BGP Router Config)

This command disables the peer as the next hop for the locally originated paths. After executing this command, the BGP peer must be reset before the changes take effect.

Format `no neighbor ip-address next-hop-self`
Mode BGP Router Config

11.1.0.72 neighbor next-hop-self (IPv4 VRF Address Family Config)

This command configures BGP to set the next hop attribute to a local IP address when advertising a route to an internal peer. Normally, BGP would retain the next hop attribute received from the external peer.

When the next hop attribute in routes from external peers is retained, internal peers must have a route to the external peer's IP address. This is commonly done by configuring the IGP on the border router to advertise the external (or DMZ) subnet. The next-hop-self option eliminates the need to advertise the external subnet in the IGP.

Default not enabled
Format `neighbor ip-address next-hop-self`
Mode IPv4 VRF Address Family Config

Parameter	Description
ip-address	The neighbor's IP address.

11.1.0.72.1 no neighbor next-hop-self (IPv4 VRF Address Family Config)

This command disables the peer as the next hop for the locally originated paths. After executing this command, the BGP peer must be reset before the changes take effect.

Format `no neighbor ip-address next-hop-self`
Mode IPv4 VRF Address Family Config

11.1.0.73 neighbor next-hop-self (IPv6 Address Family Config)

This command configures BGP to use a local address as the IPv6 next hop when advertising IPv6 routes to a specific peer. For IPv6, BGP uses an IPv6 address from the local interface that terminates the IPv4 peering session.

Default not enabled
Format `neighbor ip-address next-hop-self`
Mode IPv6 Address Family Config

Parameter	Description
ip-address	The neighbor's IP address.

11.1.0.73.1 no neighbor next-hop-self (IPv6 Address Family Config)

This command disables the peer as the next hop for the locally originated paths. After executing this command, the BGP peer must be reset before the changes take effect.

Format `no neighbor ip-address next-hop-self`
Mode IPv6 Address Family Config

11.1.0.74 neighbor password

Use this command to enable MD5 authentication of TCP segments sent to and received from a neighbor, and configures an authentication key.

MD5 must either be enabled or disabled on both peers. The same password must be configured on both peers. After a TCP connection is established, if the password on one end is changed, then the password on the other end must be changed to match before the hold time expires. With default hold times, both passwords must be changed within 120 seconds to guarantee the connection is not dropped.

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Default `MD5 authentication is disabled.`
Format `neighbor {ip-address | ipv6-address [interface interface-name] |autodetect interface interface-name} password string`
Mode
- BGP Router Config
- Peer Template Config

Parameter	Description
ipv4-address|ipv6 address	The neighbor's IPv4 or IPv6 address.
ipv6-address [interface *interface-name*]	The neighbor's IPv6 address. if the neighbor's IPv6 address is a link local address, the local interface must also be specified.
autodetect interface *interface-name*	The routing interface on which the neighbor's link local IPv6 address is auto-detected.
string	Case-sensitive password from 1 to 25 characters in length.

11.1.0.74.1 no neighbor password

This command disables MD5 authentication of TCP segments sent to and received from a neighbor.

Format `no neighbor {ip-address | ipv6-address [interface interface-name] |autodetect interface interface-name} password`

Mode BGP Router Config

11.1.0.75 neighbor password (IPv4 VRF Address Family Config)

Use this command to enable MD5 authentication of TCP segments sent to and received from a neighbor, and configures an authentication key.

MD5 must either be enabled or disabled on both peers. The same password must be configured on both peers. After a TCP connection is established, if the password on one end is changed, then the password on the other end must be changed to match before the hold time expires. With default hold times, both passwords must be changed within 120 seconds to guarantee the connection is not dropped.

Default `MD5 authentication is disabled.`

Format `neighbor {ip-address | autodetect interface interface-name} password string`

Mode IPv4 VRF Address Family Config

Parameter	Description
ipv4-address|ipv6 address	The neighbor's IPv4 or IPv6 address.
autodetect interface *interface-name*	The routing interface on which the neighbor's link local IPv6 address is auto-detected.
string	Case-sensitive password from 1 to 25 characters in length.

11.1.0.75.1 no neighbor password (IPv4 VRF Address Family Config)

This command disables MD5 authentication of TCP segments sent to and received from a neighbor.

Format `no neighbor {ip-address | autodetect interface interface-name} password`

Mode BGP Router Config

11.1.0.76 neighbor prefix-list

This command filters advertisements sent to a specific neighbor based on the destination prefix of each route.

Only one prefix list may be defined for each neighbor in each direction. If you assign a prefix list that does not exist, all prefixes are permitted.

Default No prefix list is configured.

Format `neighbor {ipv4-address | ipv6-address} prefix-list prefix-list-name { in | out }`

Mode BGP Router Config

Parameter	Description
ipv4-address|ipv6-address	The neighbor's IPv4 or IPv6 address.
prefix-list-name	The name of an IP prefix list.
in	Apply the prefix list to advertisements received from this neighbor.
out	Apply the prefix list to advertisements to be sent to this neighbor.

11.1.0.76.1 no neighbor prefix-list

This command disables filtering advertisements sent to a specific neighbor based on the destination prefix of each route.

Format `no neighbor ip-address prefix-list prefix-list-name { in | out }`

Mode BGP Router Config

11.1.0.77 neighbor remote-as (BGP Router Config)

This command configures a neighbor and identifies the neighbor's autonomous system. The neighbor's AS number must be specified when the neighbor is created. Up to 256 neighbors may be configured. Inheriting a template with the remote-as parameter automatically creates the neighbor if the neighbor does not exist.

Default `No neighbors are configured by default.`

Format `neighbor {ip-address | ipv6-address [interface interface-name] | autodetect interface interface-name remote-as as-number`

Mode
- BGP Router Config
- Peer Template Config

Parameter	Description
ipv4-address|ipv6-address	The neighbor's IPv4 or IPv6 address.
ipv6-address [interface *interface-name*]	The neighbor's IPv6 address. if the neighbor's IPv6 address is a link local address, the local interface must also be specified.
autodetect interface *interface-name*	The routing interface on which the neighbor's link local IPv6 address is auto-detected.
remote-as *as-number*	The autonomous system number of the neighbor's AS. The range is 1 to 429496729. If the neighbor's AS number is the same as the local router, the peer is an internal peer. Otherwise, the peer is an external peer. A neighbor can inherit this configuration from a peer template.

11.1.0.77.1 no neighbor remote-as

This command unconfigures neighbors.

Format `no neighbor {ip-address | ipv6-address [interface interface-name] | autodetect interface interface-name remote-as`

Mode
- BGP Router Config
- Peer Template Config

11.1.0.78 neighbor remote-as (IPv6 Address Family Config)

This command configures a neighbor and identifies the neighbor's autonomous system. The neighbor's AS number must be specified when the neighbor is created. Up to 128 neighbors may be configured. Inheriting a template with the remote-as parameter automatically creates the neighbor if the neighbor does not exist.

Default `No neighbors are configured by default.`

Format `neighbor {ip-address | ipv6-address [interface interface-name] | autodetect interface interface-name remote-as as-number`

Mode
- IPv6 Address Family Config
- Peer Template Config

Parameter	Description
ipv4-address|ipv6-address	The neighbor's IPv4 or IPv6 address.
ipv6-address [interface *interface-name*]	The neighbor's IPv6 address. if the neighbor's IPv6 address is a link local address, the local interface must also be specified.
autodetect interface *interface-name*	The routing interface on which the neighbor's link local IPv6 address is auto-detected.
remote-as *as-number*	The autonomous system number of the neighbor's AS. The range is 1 to 65,535. If the neighbor's AS number is the same as the local router, the peer is an internal peer. Otherwise, the peer is an external peer. A neighbor can inherit this configuration from a peer template.

11.1.0.78.1 no neighbor remote-as (IPv6 Address Family Config)

This command unconfigures neighbors.

Format `no neighbor {ip-address | ipv6-address [interface interface-name] | autodetect interface interface-name remote-as`

Mode
- IPv6 Address Family Config
- Peer Template Config

11.1.0.79 neighbor remove-private-as (BGP Router Config)

Use this command in router configuration mode to remove private AS numbers when advertising IPv4 routes to an external peer. To stop removing private AS numbers, use the `no` form of this command.

This command can only be applied to external peers. Private AS numbers are removed or replaced whether or not the original AS path includes any non-private AS numbers. The AS path advertised to the external peer always includes at least one instance of the local AS number; therefore, removing private AS numbers never results in advertisement of an empty AS_PATH attribute. AS numbers from 64512 to 65535 inclusive are considered private. Although 65535 is a reserved ASN and not technically part of the private range, it is treated as a private ASN when removing or replacing private ASNs.

Default Private AS numbers are not removed by default.

Format `neighbor ip-address remove-private-as [all replace-as]`

Mode BGP Router Config

Parameter	Description
ip-address	The neighbor's IPv4 address.
all replace-as	To retain the original AS path length, replace each private AS number with the local AS number. This is optional.

11.1.0.79.1 no neighbor remove-private-as (BGP Router Config)

Format `no neighbor` *`ip-address`* `remove-private-as`
Mode BGP Router Config

11.1.0.80 neighbor remove-private-as (IPv4 VRF Address Family Config)

Use this command in router configuration mode to remove private AS numbers when advertising IPv4 routes to an external peer. To stop removing private AS numbers, use the `no` form of this command.

This command can only be applied to external peers. Private AS numbers are removed or replaced whether or not the original AS path includes any non-private AS numbers. The AS path advertised to the external peer always includes at least one instance of the local AS number; therefore, removing private AS numbers never results in advertisement of an empty AS_PATH attribute. AS numbers from 64512 to 65535 inclusive are considered private. Although 65535 is a reserved ASN and not technically part of the private range, it is treated as a private ASN when removing or replacing private ASNs.

Default Private AS numbers are not removed by default.
Format `neighbor` *`ip-address`* `remove-private-as [all replace-as]`
Mode IPv4 VRF Address Family Config

Parameter	Description
ip-address	The neighbor's IPv4 address.
all replace-as	To retain the original AS path length, replace each private AS number with the local AS number. This is optional.

11.1.0.80.1 no neighbor remove-private-as (IPv4 VRF Address Family Config)

Format `no neighbor` *`ip-address`* `remove-private-as`
Mode IPv4 VRF Address Family Config

11.1.0.81 neighbor remove-private-as (IPv6 Address Family Config)

Use this command in router configuration mode to remove private AS numbers when advertising IPv6 routes to an external peer. To stop removing private AS numbers, use the `no` form of this command.

This command can only be applied to external peers. Private AS numbers are removed or replaced whether or not the original AS path includes any non-private AS numbers. The AS path advertised to the external peer always includes at least one instance of the local AS number; therefore, removing private AS numbers never results in advertisement of an empty AS_PATH attribute. AS numbers from 64512 to 65535 inclusive are considered private. Although 65535 is a reserved ASN and not technically part of the private range, it is treated as a private ASN when removing or replacing private ASNs.

Default Private AS numbers are not removed by default.
Format `neighbor` *`ip-address`* `remove-private-as [all replace-as]`

Mode IPv6 Address Family Config

Parameter	Description
ip-address	The neighbor's IPv4 or IPv6 address.
all replace-as	To retain the original AS path length, replace each private AS number with the local AS number. This is optional.

11.1.0.81.1 no neighbor remove-private-as (IPv6 Address Family Config)

Format `no neighbor` *`ip-address`* `remove-private-as`
Mode BGP Router Config

11.1.0.82 neighbor rfc5549-support

To enable advertisement of IPv4 routes over IPv6 next hops selectively to an external BGP IPv6 peer, use the **neighbor rfc5549-support** command. This command may only be applied to external BGP peers via single hop.

Default RFC 5549 support is enabled by default for all neighbors if IPv6 package is available in the build.
Format `neighbor { ipv6-address | autodetect interface interface-name } rfc5549-support`
Mode BGP Router Config

Parameter	Description
ipv6-address	The neighbor's IPv6 address
autodetect interface *interface-name*	The routing interface on which the neighbor's link local IPv6 address is auto detected.

Example:

```
(R1) # configure
(R1) (Config) # router bgp 100
(R1) (Config-router) # neighbor 2001::2 rfc5549-support
```

11.1.0.82.1 no neighbor rfc5549-support

This command disables advertisement of IPv4 routes over IPv6 next hops.

Format `no neighbor { ipv6-address | autodetect interface interface-name } rfc5549-support`
Mode BGP Router Config

11.1.0.83 neighbor route-map (BGP Router Config)

To apply a route map to incoming or outgoing routes for a specific neighbor, use the **neighbor route-map** command in Router Configuration mode. A route map can be used to change the local preference, MED, or AS Path of a route. Routes can be selected for filtering or modification using an AS path access list or a prefix list.

Default No route maps are applied by default.
Format `neighbor {ipv4-address | ipv6-address} route-map map-name {in|out}`
Mode BGP Router Config

Parameter	Description
ipv4-address|ipv6-address	The neighbor's IPv4 or IPv6 address.
map-name	The name of the route map to be applied.
in|out	Whether the route map is applied to incoming or outgoing routes.

11.1.0.83.1 no neighbor route-map (BGP Router Config)

Use the no neighbor route-map command to remove the route map.

Format `no neighbor ip-address route-map map-name {in|out}`
Mode BGP Router Config

11.1.0.84 neighbor route-map (IPv4 VRF Address Family Config)

To apply a route map to incoming or outgoing routes for a specific neighbor, use the **neighbor route-map** command in Router Configuration mode. A route map can be used to change the local preference, MED, or AS Path of a route. Routes can be selected for filtering or modification using an AS path access list or a prefix list.

Default No route maps are applied by default.
Format `neighbor ip-address route-map map-name {in|out}`
Mode IPv4 VRF Address Family Config

Parameter	Description
ip-address	The neighbor's IP address.
map-name	The name of the route map to be applied.
in|out	Whether the route map is applied to incoming or outgoing routes.

11.1.0.84.1 no neighbor route-map (IPv4 VRF Address Family Config)

Use the no neighbor route-map command to remove the route map.

Format `no neighbor ip-address route-map map-name {in|out}`
Mode IPv4 VRF Address Family Config

11.1.0.85 neighbor route-map (IPv6 Address Family Config)

This command specifies a route map to be applied to inbound or outbound IPv6 routes.

Default No route maps are applied by default.
Format `neighbor ip-address route-map map-name {in|out}`
Mode IPv6 Address Family Config

Parameter	Description
ip-address	The neighbor's IP address.

Parameter	Description
map-name	The name of the route map to be applied.
in|out	Whether the route map is applied to incoming or outgoing routes.

11.1.0.85.1 no neighbor route-map (IPv6 Address Family Config)

Use the no neighbor route-map command to remove the route map.

Format `no neighbor ip-address route-map map-name {in|out}`
Mode IPv6 Address Family Config

11.1.0.86 neighbor route-reflector-client (BGP Router Config)

Use this command in BGP router configuration mode to configure an internal peer as an IPv4 route reflector client.

Normally, a router does not readvertise BGP routes received from an internal peer to other internal peers. If you configure a peer as a route reflector client, this router readvertises such routes. A router is a route reflector if it has one or more route reflector clients. Configuring the first route reflector client automatically makes the router a route reflector.

If you configure multiple route reflectors within a cluster, you must configure each route reflector in the cluster with the same cluster ID. Use the Section 11.1.0.15, bgp cluster-id command to configure a cluster ID.

An external peer may not be configured as a route reflector client.

When reflecting a route, BGP ignores the set statements in an outbound route map to avoid causing the receiver to compute routes that are inconsistent with other routers in the AS.

Default Peers are not route reflector clients.
Format `neighbor {ip-address} reoute-reflector-client`
Mode BGP Router Config

Parameter	Description
ip-address	The neighbor's IPv4 address.

11.1.0.86.1 no neighbor route-reflector-client (BGP Router Config)

Format `no neighbor {ip-address} route-reflector-client`
Mode BGP Router Config

11.1.0.87 neighbor route-reflector-client (IPv4 VRF Address Family Config)

Use this command in IPv4 VRF Address Family mode to configure an internal peer as an IPv4 route reflector client.

Normally, a router does not readvertise BGP routes received from an internal peer to other internal peers. If you configure a peer as a route reflector client, this router readvertises such routes. A router is a route reflector if it has one or more route reflector clients. Configuring the first route reflector client automatically makes the router a route reflector.

If you configure multiple route reflectors within a cluster, you must configure each route reflector in the cluster with the same cluster ID. Use the Section 11.1.0.15, bgp cluster-id command to configure a cluster ID.

An external peer may not be configured as a route reflector client.

When reflecting a route, BGP ignores the set statements in an outbound route map to avoid causing the receiver to compute routes that are inconsistent with other routers in the AS.

Default Peers are not route reflector clients.

Format `neighbor {ip-address} route-reflector-client`

Mode IPv4 VRF Address Family Config

Parameter	Description
ip-address	The neighbor's IPv4 address.

11.1.0.87.1 no neighbor route-reflector-client (IPv4 VRF Address Family Config)

Format `no neighbor {ip-address} route-reflector-client`

Mode IPv4 VRF Address Family Config

11.1.0.88 neighbor route-reflector-client (IPv6 Address Family Config)

Use this command in IPv6 Address Family Config mode to configure an internal peer as an IPv6 route reflector client.

Normally, a router does not readvertise BGP routes received from an internal peer to other internal peers. If you configure a peer as a route reflector client, this router readvertises such routes. A router is a route reflector if it has one or more route reflector clients. Configuring the first route reflector client automatically makes the router a route reflector.

If you configure multiple route reflectors within a cluster, you must configure each route reflector in the cluster with the same cluster ID. Use the Section 11.1.0.15, bgp cluster-id command to configure a cluster ID.

An external peer may not be configured as a route reflector client.

When reflecting a route, BGP ignores the set statements in an outbound route map to avoid causing the receiver to compute routes that are inconsistent with other routers in the AS.

Default Peers are not route reflector clients.

Format `neighbor {ip-address} reoute-reflector-client`

Mode IPv6 Address Family Config

Parameter	Description
ip-address	The neighbor's IPv4 or IPv6 address.

11.1.0.88.1 no neighbor route-reflector-client (IPv6 Address Family Config)

Format `no neighbor {ip-address} route-reflector-client`

Mode IPv6 Address Family Config

11.1.0.89 neighbor send-community extended

To configure the local router to send the BGP community attributes in Update messages to a specific neighbor, use the **neighbor send-community extended** command in BGP VPNv4 Address Family Configuration mode.

Using this command under the **address-family vpnv4 unicast** mode enables the local BGP router to send extended communities attribute to its BGP peer across the backbone. The neighbor address must be the same IP address used in the **neighbor remote-as** command to create the peer.

Default The extended communities attribute is not sent.

Format `neighbor ip-address send-community [extended | both]`

Mode VPNv4 Address Family Config
L2VPN Address Family Config

Parameter	Description
ip-address	The neighbor's IPv4 address.
[extended | both]	One of the following: ■ extended enables the router to send only extended community attributes. ■ both enables the router to send both standard and extended community attributes.

Example:

The following example enables sending of the extended communities attribute to external peer at 1.1.1.1.

```
(Config)# router bgp 1
(Config-router)# neighbor 1.1.1.1 remote-as 2
(Config-router)# address-family vpnv4 unicast(R1) (Config-router-af-vpnv4)# neighbor 1.1.1.1 send-community extended
(Config-router-af-vpnv4)# neighbor 1.1.1.1 activate
```

11.1.0.89.1 no neighbor send-community extended

Use the **no neighbor send-community extended** command to disable the exchange of VPNv4 prefixes with the neighbor.

Format `no neighbor ip-address send-community`

Mode VPNv4 Address Family Config
L2VPN Address Family Config

11.1.0.90 neighbor send-community

To configure the local router to send the BGP community attributes in Update messages to a specific neighbor, use the **neighbor send-community** command.

Default The communities attribute is not sent to neighbors by default.

Format `neighbor {ipv4-address | ipv6-address} send-community`

Mode
- BGP Router Config
- IPv4 VRF Address Family Config
- IPv6 Address Family Config

Parameter	Description
ipv4-address|ipv6-address	The neighbor's IPv4 or IPv6 address.

11.1.0.90.1 no neighbor send-community

Use the **no neighbor send-community** command to return to the default configuration.

Format `no neighbor ip-address send-community`

Mode
- BGP Router Config
- IPv4 VRF Address Family Config
- IPv6 Address Family Config

11.1.0.91 neighbor send-community (IPv4 VRF Address Family Config)

To configure the local router to send the BGP community attributes in Update messages to a specific neighbor, use the **neighbor send-community** command.

Default The communities attribute is not sent to neighbors by default.

Format `neighbor ipv4-address send-community`

Mode IPv4 VRF Address Family Config

Parameter	Description
ipv4-address|ipv6-address	The neighbor's IPv4 or IPv6 address.

11.1.0.91.1 no neighbor send-community (IPv4 VRF Address Family Config)

Use the **no neighbor send-community** command to return to the default configuration.

Format `no neighbor ip-address send-community`

Mode IPv4 VRF Address Family Config

11.1.0.92 neighbor shutdown

Use this command to bring down the adjacency with a specific neighbor. If the adjacency is up when the command is given, the peering session is dropped and all route information learned from the neighbor is purged.

When a neighbor is shut down, BGP first sends a NOTIFICATION message with a Cease error code. When an adjacency is administratively shut down, the adjacency stays down until administratively reenabled (using the Section 11.1.0.92.1, no neighbor shutdown command below).

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Default Neighbors are not shutdown by default.

Format `neighbor {ipv4-address | ipv6-address [interface` *`interface-name`*`]| autodetect interface` *`interface-name`* `} shutdown`

Mode
- BGP Router Config
- Peer Template Config

Parameter	Description
ipv4-address|ipv6-address	The neighbor's IPv4 or IPv6 address on the link that connects the two peers. If the neighbor's IPv6 address is a link local address, the local interface must also be specified.
autodetect interface *interface-name*	The routing interface on which the neighbor's link local IPv6 address is auto-detected.

11.1.0.92.1 no neighbor shutdown

This command administratively enables a BGP peer.

Format `no neighbor {ipv4-address | ipv6-address [interface` ***interface-name***`]| autodetect interface` ***interface-name*** `} shutdown`

Mode
- BGP Router Config
- Peer Template Config

11.1.0.93 neighbor shutdown (IPv4 VRF Address Family Config)

Use this command to bring down the adjacency with a specific neighbor. If the adjacency is up when the command is given, the peering session is dropped and all route information learned from the neighbor is purged.

When a neighbor is shut down, BGP first sends a NOTIFICATION message with a Cease error code. When an adjacency is administratively shut down, the adjacency stays down until administratively reenabled (using the Section 11.1.0.92.1, no neighbor shutdown command below). Issue this command in Peer Template Configuration Mode to add it to a peer template.

Default Neighbors are not shutdown by default.

Format `neighbor {ipv4-address | autodetect interface` ***interface-name*** `} shutdown`

Mode IPv4 VRF Address Family Config

Parameter	Description
ipv4-address	The neighbor's IPv4 address on the link that connects the two peers. If the neighbor's IPv6 address is a link local address, the local interface must also be specified.
autodetect interface *interface-name*	The routing interface on which the neighbor's link local IPv6 address is auto-detected.

11.1.0.93.1 no neighbor shutdown (IPv4 VRF Address Family Config)

This command administratively enables a BGP peer.

Format `no neighbor {ipv4-address | autodetect interface` ***interface-name*** `} shutdown`

Mode IPv4 VRF Address Family Config

11.1.0.94 neighbor timers

Use this command to override the global timer values and set the keepalive and hold timers for a specific neighbor. The new values are not applied to adjacencies already in the ESTABLISHED state. A new keepalive or hold time is applied the next time an adjacency is formed.

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Default The keepalive and hold timers default to the globally configured values set with the Section 11.1.0.104, redistribute (IPv6 Address Family Config) command.

Format `neighbor {ipv4-address | ipv6-address [interface interface-name]| autodetect interface` ***`interface-name`*** `}timers keepalive holdtime`

Mode
- BGP Router Config
- Peer Template Config

Parameter	Description
ipv4-address|ipv6-address	The neighbor's IPv4 or IPv6 address. This is the IP address on the link that connects the two peers. If the neighbor's IPv6 address is a link local address, the local interface must also be specified.
autodetect interface ***interface-name***	The routing interface on which the neighbor's link local IPv6 address is auto-detected.
keepalive	The time, in seconds, between BGP KEEPALIVE packets sent to a neighbor. The range is 0 to 65,535 seconds. Jitter is applied to the keepalive interval.
holdtime	The time, in seconds, that BGP continues to consider a neighbor to be alive without receiving a BGP KEEPALIVE or UPDATE packet from the neighbor. If no KEEPALIVE is received from a neighbor for longer than the hold time, BGP drops the adjacency. If the hold time is set to 0, then BGP does not enforce a hold time and BGP does not send periodic KEEPALIVE messages. The range is 0 to 65,535 seconds.

11.1.0.94.1 no neighbor timers

This command reverts the keep alive and hold time for a peer to their defaults. After executing this command, the BGP peer must be reset before the changes will take effect.

Format `no neighbor {ipv4-address | ipv6-address [interface interface-name]| autodetect interface` ***`interface-name`*** `}timers`

Mode
- BGP Router Config
- Peer Template Config

11.1.0.95 neighbor timers (IPv4 VRF Address Family Config)

Use this command to override the global timer values and set the keepalive and hold timers for a specific neighbor. The new values are not applied to adjacencies already in the ESTABLISHED state. A new keepalive or hold time is applied the next time an adjacency is formed.

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Default The keepalive and hold timers default to the globally configured values set with the Section 11.1.0.103, redistribute (IPv4 VRF Address Family Config) command.

Format `neighbor {ipv4-address | autodetect interface` ***`interface-name`*** `}timers keepalive holdtime`

Mode IPv4 VRF Address Family Config

Parameter	Description
ipv4-address	The neighbor's IPv4 address. This is the IP address on the link that connects the two peers.
autodetect interface ***interface-name***	The routing interface on which the neighbor's link local IPv6 address is auto-detected.

Parameter	Description
keepalive	The time, in seconds, between BGP KEEPALIVE packets sent to a neighbor. The range is 0 to 65,535 seconds. Jitter is applied to the keepalive interval.
holdtime	The time, in seconds, that BGP continues to consider a neighbor to be alive without receiving a BGP KEEPALIVE or UPDATE packet from the neighbor. If no KEEPALIVE is received from a neighbor for longer than the hold time, BGP drops the adjacency. If the hold time is set to 0, then BGP does not enforce a hold time and BGP does not send periodic KEEPALIVE messages. The range is 0 to 65,535 seconds.

11.1.0.95.1 no neighbor timers (IPv4 VRF Address Family Config)

This command reverts the keep alive and hold time for a peer to their defaults. After executing this command, the BGP peer must be reset before the changes will take effect.

Format `no neighbor {ipv4-address | autodetect interface` *`interface-name`* `}timers`

Mode IPv4 VRF Address Family Config

11.1.0.96 neighbor update-source

Use this command to configure BGP to use a specific IP address as the source address for the TCP connection with a neighbor. This IP address must be the IP address configured on the peer as its neighbor address for this router.

The IP address used as the source address in IP packets sent to a neighbor must be the same address used to configure the local system as a neighbor of the neighbor router. In other words, if the update source is configured, it must be the same IP address used in the neighbor remote-as command on the peer.

It is common to use an IP address on a loopback interface because a loopback interface is always reachable, as long as any routing interface is up. The peering session can stay up as long as the loopback interface remains reachable. If you use an IP address on a routing interface, then the peering session will go down if that routing interface goes down.

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Default When no update source is configured, TCP connections use the primary IPv4 address on the outgoing interface to the neighbor.

Format `neighbor {ipv4-address | ipv6-address [interface interface-name]| autodetect interface` *`interface-name`* `} update-source interface`

Mode
- BGP Router Config
- Peer Template Config

Parameter	Description
ipv4-address|ipv6-address	The neighbor's IPv4 or IPv6 address. This is the IP address on the link that connects the two peers. If the neighbor's IPv6 address is a link local address, the local interface must also be specified.
auto-detect interface ***interface-name***	The neighbor's IPv6 link local address that will be auto detected on the specified interface.
update-source interface	The primary IPv4 address on this interface is used as the source IP address for the TCP connection with the neighbor.

11.1.0.96.1 no neighbor update-source

This command configures BGP to use the primary IPv4 address on the outgoing interface to the neighbor for the TCP connection.

Format `no neighbor {ipv4-address | ipv6-address [interface interface-name]| autodetect interface` ***`interface-name`*** `} update-source`

Mode
- BGP Router Config
- Peer Template Config

11.1.0.97 neighbor update-source (IPv4 VRF Address Family Config)

Use this command to configure BGP to use a specific IP address as the source address for the TCP connection with a neighbor. This IP address must be the IP address configured on the peer as its neighbor address for this router.

The IP address used as the source address in IP packets sent to a neighbor must be the same address used to configure the local system as a neighbor of the neighbor router. In other words, if the update source is configured, it must be the same IP address used in the neighbor remote-as command on the peer.

It is common to use an IP address on a loopback interface because a loopback interface is always reachable, as long as any routing interface is up. The peering session can stay up as long as the loopback interface remains reachable. If you use an IP address on a routing interface, then the peering session will go down if that routing interface goes down.

The *update-source* option is not allowed for eBGP peers as this requires multi-hop eBGP to be working. Multi-hop eBGP is not supported.

Issue this command in Peer Template Configuration Mode to add it to a peer template.

Default When no update source is configured, TCP connections use the primary IPv4 address on the outgoing interface to the neighbor.

Format `neighbor {ipv4-address | autodetect interface` ***`interface-name`*** `} update-source interface`

Mode IPv4 VRF Address Family Config

Parameter	Description
ipv4-address	The neighbor's IPv4 address. This is the IP address on the link that connects the two peers.
auto-detect interface ***interface-name***	The neighbor's IPv6 link local address that will be auto detected on the specified interface.
update-source interface	The primary IPv4 address on this interface is used as the source IP address for the TCP connection with the neighbor.

11.1.0.97.1 no neighbor update-source (IPv4 VRF Address Family Config)

This command configures BGP to use the primary IPv4 address on the outgoing interface to the neighbor for the TCP connection.

Format `no neighbor {ipv4-address | autodetect interface` ***`interface-name`*** `} update-source`

Mode IPv4 VRF Address Family Config

11.1.0.98 network (BGP Router Config)

This command configures BGP to advertise an address prefix.The prefix is only advertised if the common routing table includes a non-BGP route with the same prefix. The route may be a connected route, a static route, or a dynamic route from another routing protocol.

BGP accepts up to 64 networks per address family. The network command may specify a default route (network 0.0.0.0 mask 0.0.0.0).

If a route map is configured to set attributes on the advertised routes, **match as-path** and **match community** terms in the route map are ignored. A **match ip-address prefix-list** term is honored in this context. If your route map includes such a match term, the network is only advertised if the prefix list permits the network prefix. If there is no route map with the name given, the network is not advertised.

Default No networks are advertised by default.

Format `network prefix mask network-mask [route-map rm-name]`

Mode
- BGP Router Config
- IPv4 VRF Address Family Config

Parameter	Description
prefix	An IPv4 address prefix in dotted notation.
network-mask	The network mask for the prefix in dotted quad notation (e.g., 255.255.0.0).
rm-name	(Optional) A route map can be used to set path attributes on the route.

11.1.0.98.1 no network (BGP Router Config)

This command disables BGP from advertising an address prefix.

Format `no network prefix mask network-mask [route-map rm-name]`

Mode BGP Router Config

11.1.0.99 network (IPv6 Address Family Config)

This command identifies network IPv6 prefixes that BGP originates in route advertisements to its neighbors. The prefix is only advertised if the common routing table includes a non-BGP route with the same prefix. The route may be a connected route, a static route, or a dynamic route from another routing protocol.

BGP accepts up to 64 networks per address family. The network command may specify a default route (network 0.0.0.0 mask 0.0.0.0).

If a route map is configured to set attributes on the advertised routes, **match as-path** and **match community** terms in the route map are ignored. A **match ip-address prefix-list** term is honored in this context. If your route map includes such a match term, the network is only advertised if the prefix list permits the network prefix. If there is no route map with the name given, the network is not advertised.

Default No networks are advertised by default.

Format `network ipv6-address|prefix-length [route-map rm-name]`

Mode IPv6 Address Family Config

Parameter	Description
ipv6-address	Network IPv6 prefixes.
prefix	An IPv4 address prefix in dotted notation.
rm-name	(Optional) A route map can be used to set path attributes on the route.

11.1.0.99.1 no network (IPv6 Address Family Config)

This command disables BGP from advertising an address prefix.

Format `no network prefix mask network-mask [route-map rm-name]`
Mode IPv6 Address Family Config

11.1.0.100 nv overlay evpn

This command enables EVPN control plane for VXLAN. Only after enabling this mode does the BGP start advertising or accepting the EVPN routes with the EVPN address-family activated neighbors.

Default Inactive
Format `nv overlay evpn`
Mode Global Config

11.1.0.101 rd

Use this command to specify the route distinguisher (RD) for a VRF instance that is used to create a VPNv4 prefix. An RD creates routing and forwarding tables and specifies the default route distinguisher for a VPN. The RD is added to the beginning of the IPv4 prefixes to change them into globally unique VPNv4 prefixes.

An RD is either:
- 2-byte ASN-related: Composed of an autonomous system number and an arbitrary number.
- IP address-related: Composed of an IP address and an arbitrary number.
- 4-byte ASN related: Composed of an 4-byte autonomous system number and an arbitrary number.

Default A VRF does not associate with any RD
Format `rd` *`route-distinguisher`*
Mode Virtual Router Config

Parameter	Description
route-distinguisher	An 8-byte value to be added to an IPv4 prefix to create a VPNv4 prefix. The RD value can be specified in either of the following formats: ■ 16-bit AS number: your 32-bit value (Ex : 100 :11) ■ 32-bit IPv4 address: your 16-bit value (Ex : 10.1.1.1 :22) ■ 4-byte AS number: your 32-bit value (Ex : 66666 :33)

NOTE: This command is effective only if BGP is running on the router. The RD for a VRF once configured cannot be removed or changed. For this reason, this command does not have the no form. To change the configured RD value, remove the VRF (using the **no ip vrf** command) and reconfigure the VRF.

Example:

The following example shows how to configure a RD for a VRF instance in ASN format:

```
(Router) (Config)#ip vrf Red
(Router) (Config-vrf-Red)#rd 62001:10
(Router) (Config-vrf-Red)#exit
```

The following example shows how to configure a RD for a VRF instance in IP address format:

```
(Router) (Config)#ip vrf Red
(Router) (Config-vrf-Red)#rd 192.168.10.1:10
(Router) (Config-vrf-Red)#exit
```

The following example shows how to configure a RD for a VRF instance in 4-byte ASN format:

```
(Router) (Config)#ip vrf Green
(Router) (Config-vrf-Red)#rd 77777:20
(Router) (Config-vrf-Red)#exit
```

11.1.0.102 redistribute (BGP Router Config)

This command configures BGP to advertise routes learned by means outside of BGP. BGP can redistribute local (connected), static, and OSPF routes.

The distribute-list out command can also be used to filter redistributed routes by prefix. Either a redistribute route map or a distribute list may be configured, but not both.

A default route cannot be redistributed unless the Section 11.1.0.23, default-information originate command is given.

If a route map is configured, **match as-path** and **match community** terms are ignored. If no route map is configured with the name given, no prefixes are redistributed.

Default BGP redistributes no routes by default. When BGP redistributes OSPF routes, it redistributes only internal routes unless the **match** option specifies external routes.

Format `redistribute {ospf |connected | static} [metric metric-value] [match {internal | external 1 | external 2 | nssa-external 1 | nssa-external 2}] [route-map map-tag]`

Mode BGP Router Config

Parameter	Description
ospf, connected, static	A source of routes to redistribute.
metric metric-value	(Optional) When this option is specified, BGP advertises the prefix with the Multi Exit Discriminator path attribute set to the configured value. If this option is not specified, but a default metric is configured for BGP, the MED is set to the default metric. If a default metric is not configured, the prefix is advertised without a MED attribute.
match	(Optional) If you configure BGP to redistribute OSPF routes, BGP by default only redistributes internal routes (OSPF intra-area and inter-area routes). Use the **match** option to configure BGP to also redistribute specific types of external routes, or to disable redistribution of internal OSPF routes.
route-map map-tag	(Optional) A route map can be used to filter redistributed routes by destination prefix using a prefix list. A route map can be used to set attributes on redistributed routes.

Example: The routes obtained from the kernel can be configured to redistributed in the kernel. The following CLI commands (in both IPv4 and Pv6) BGP Router mode use the kernel option.

```
(7001) (Config)#router bgp 65401

(7001) (Config-router)#redistribute ?

<cr>                    Press enter to execute the command.
connected               Configure redistribution of Connected routes
kernel                  Configure redistribution of Kernel routes
ospf                    Configure redistribution of OSPF routes
rip                     Configure redistribution of RIP routes
static                  Configure redistribution of Static routes

(7001) (Config-router)#redistribute

Incorrect protocol! Use '<rip|ospf|static|connected>'

(7001) (Config-router)#address-family ipv6

(7001) (config-router-af)#redistribute ?

<cr>                    Press enter to execute the command.
connected               Configure redistribution of Connected routes
kernel                  Configure redistribution of Kernel routes
ospf                    Configure redistribution of OSPF routes
static                  Configure redistribution of Static routes
```

11.1.0.102.1 no redistribute (BGP Router Config)

This command removes the configuration for the redistribution for BGP protocol from the specified source protocol/routers. The command **no redistribute ospf match external 1** will withdraw only OSPF external type 1 routes, ospf inter routes will still be redistributing.

Format `no redistribute {ospf | connected | static} [metric metric-value] [match {internal | external 1 | external 2 | nssa-external 1 | nssa-external 2}] [route-map map-tag]`

Mode BGP Router Config

11.1.0.103 redistribute (IPv4 VRF Address Family Config)

This command configures BGP to advertise routes learned by means outside of BGP. BGP can redistribute local (connected), static, OSPF, and RIP routes.

The distribute-list out command can also be used to filter redistributed routes by prefix. Either a redistribute route map or a distribute list may be configured, but not both.

A default route cannot be redistributed unless the Section 11.1.0.23, default-information originate command is given.

If a route map is configured, **match as-path** and **match community** terms are ignored. If no route map is configured with the name given, no prefixes are redistributed.

Default BGP redistributes no routes by default. When BGP redistributes OSPF routes, it redistributes only internal routes unless the **match** option specifies external routes.

Format `redistribute {ospf | rip | connected | static} [metric metric-value] [match {internal | external 1 | external 2 | nssa-external 1 | nssa-external 2}] [route-map map-tag]`

Mode IPv4 VRF Address Family Config

Parameter	Description
ospf, rip, connected, static	A source of routes to redistribute.
metric metric-value	(Optional) When this option is specified, BGP advertises the prefix with the Multi Exit Discriminator path attribute set to the configured value. If this option is not specified, but a default metric is configured for BGP, the MED is set to the default metric. If a default metric is not configured, the prefix is advertised without a MED attribute.
match	(Optional) If you configure BGP to redistribute OSPF routes, BGP by default only redistributes internal routes (OSPF intra-area and inter-area routes). Use the **match** option to configure BGP to also redistribute specific types of external routes, or to disable redistribution of internal OSPF routes.
route-map map-tag	(Optional) A route map can be used to filter redistributed routes by destination prefix using a prefix list. A route map can be used to set attributes on redistributed routes.

11.1.0.103.1 no redistribute (IPv4 VRF Address Family Config)

This command removes the configuration for the redistribution for BGP protocol from the specified source protocol/routers. The command **no redistribute ospf match external 1** will withdraw only OSPF external type 1 routes, ospf inter routes will still be redistributing.

Format `no redistribute {ospf | rip | connected | static} [metric metric-value] [match {internal | external 1 | external 2 | nssa-external 1 | nssa-external 2}] [route-map map-tag]`

Mode IPv4 VRF Address Family Config

11.1.0.104 redistribute (IPv6 Address Family Config)

This command configures BGP to non-BGP routes from the IPv6 routing table.

The distribute-list out command can also be used to filter redistributed routes by prefix. Either a redistribute route map or a distribute list may be configured, but not both.

A default route cannot be redistributed unless the Section 11.1.0.23, default-information originate command is given.

If a route map is configured, **match as-path** and **match community** terms are ignored. If no route map is configured with the name given, no prefixes are redistributed.

Default BGP redistributes no routes by default. When BGP redistributes OSPF routes, it redistributes only internal routes unless the **match** option specifies external routes.

Format `redistribute {ospf | connected | static} [metric metric-value] [match {internal | external 1 | external 2 | nssa-external 1 | nssa-external 2}] [route-map map-tag]`

Mode IPv6 Address Family Config

Parameter	Description
ospf, connected, static	A source of routes to redistribute.

Parameter	Description
metric metric-value	(Optional) When this option is specified, BGP advertises the prefix with the Multi Exit Discriminator path attribute set to the configured value. If this option is not specified, but a default metric is configured for BGP, the MED is set to the default metric. If a default metric is not configured, the prefix is advertised without a MED attribute.
match	(Optional) If you configure BGP to redistribute OSPF routes, BGP by default only redistributes internal routes (OSPF intra-area and inter-area routes). Use the **match** option to configure BGP to also redistribute specific types of external routes, or to disable redistribution of internal OSPF routes.
route-map map-tag	(Optional) A route map can be used to filter redistributed routes by destination prefix using a prefix list. A route map can be used to set attributes on redistributed routes.

Example: The routes obtained from the kernel can be configured to redistributed in the kernel. The following CLI commands (in both IPv4 and Pv6) BGP Router mode use the kernel option.

```
(7001) (Config)#router bgp 65401

(7001) (Config-router)#redistribute ?

<cr>                    Press enter to execute the command.
connected               Configure redistribution of Connected routes
kernel                  Configure redistribution of Kernel routes
ospf                    Configure redistribution of OSPF routes
rip                     Configure redistribution of RIP routes
static                  Configure redistribution of Static routes

(7001) (Config-router)#redistribute

Incorrect protocol! Use '<rip|ospf|static|connected>'

(7001) (Config-router)#address-family ipv6

(7001) (config-router-af)#redistribute ?

<cr>                    Press enter to execute the command.
connected               Configure redistribution of Connected routes
kernel                  Configure redistribution of Kernel routes
ospf                    Configure redistribution of OSPF routes
static                  Configure redistribution of Static routes
```

11.1.0.104.1 no redistribute (IPv6 Address Family Config)

This command removes the configuration for the redistribution for BGP protocol from the specified source protocol/routers. The command **no redistribute ospf match external 1** will withdraw only OSPF external type 1 routes, ospf inter routes will still be redistributing.

Format `no redistribute {ospf | connected | static} [metric metric-value] [match {internal | external 1 | external 2 | nssa-external 1 | nssa-external 2}] [route-map map-tag]`

Mode IPv6 Address Family Config

11.1.0.105 route-reflector-client

Use this command in BGP router configuration mode to configure an internal peer as an IPv4 route reflector client.

Normally, a router does not readvertise BGP routes received from an internal peer to other internal peers. If you configure a peer as a route reflector client, this router readvertises such routes. A router is a route reflector if it has one or more route reflector clients. Configuring the first route reflector client automatically makes the router a route reflector.

If you configure multiple route reflectors within a cluster, you must configure each route reflector in the cluster with the same cluster ID. Use the Section 11.1.0.15, bgp cluster-id command to configure a cluster ID.

An external peer may not be configured as a route reflector client.

When reflecting a route, BGP ignores the set statements in an outbound route map to avoid causing the receiver to compute routes that are inconsistent with other routers in the AS.

Default Peers are not route reflector clients.

Format `neighbor {ip-address} route-reflector-client`

Mode BGP Router Config

Parameter	Description
ip-address	The neighbor's IPv4 address.

11.1.0.106 route-target

Use this command to create a list of export, import, or both route target (RT) extended communities for the specified VRF instance. Enter the route-target command one time for each target extended community. Routes that are learned and carry a specific route-target extended community are imported into all VRFs configured with that extended community as an import route target.

The configured export RT is carried as an extended community in the MP-BGP format to the eBGP peer. An RT is either:

- 2-byte ASN-related: Composed of an autonomous system number and an arbitrary number.
- IP address-related: Composed of an IP address and an arbitrary number.
- 4-byte ASN related: Composed of an 4-byte autonomous system number and an arbitrary number.

Default A VRF does not associate with any RT.

Format `route-target {export | import | both}` *`rt-ext-comm`*

Mode Virtual Router Config

Parameter	Description
export	Exports routing information to the target VPN extended community.
import	Imports routing information from the target VPN extended community.
both	Exports/imports the routing information to/from the target VPN extended community.
rt-ext-comm	The route-target extended community attributes to be added to the list of import, export or both (import and export) route-target extended communities. The route target specifies a target VPN extended community. Like a route distinguisher, the route-target extended community can be specified in one of the following formats: ■ 16-bit AS number: your 32-bit value (Ex : 100 :11) ■ 32-bit IPv4 address: your 16-bit value (Ex : 10.1.1.1 :22) ■ 4-byte AS number: your 32-bit value (Ex: 66666 :33)

NOTE: This command is effective only if BGP is running on the router.

Example:

The following example shows how to configure route target extended community attributes for a VRF instance in IPv4. The result of this command sequence is that VRF named Red has two export extended communities (100:10 and 300:10) and two import extended communities (300:10 and 192.168.10.1:10).

```
(Router) (Config)#ip vrf Red
(Router) (Config-vrf-Red)#route-target export 100:10
(Router) (Config-vrf-Red)#route-target import 192.168.10.1:10
(Router) (Config-vrf-Red)#route-target both 300:10
(Router) (Config-vrf-Red)#route-target export 88888:80
(Router) (Config-vrf-Red)#exit
```

11.1.0.106.1 no route-target

This command removes the route target specified for a VRF instance.

Format `no route-target {export | import | both} rt-ext-comm`

Mode Virtual Router Config

11.1.0.107 retain route-target all

This L2VPN EVPN command is configured on the Spine node to retain and advertise all the EVPN routes without changing their route-targets. That is because there are no local VNIs (VxLAN network identifiers) configured on the Spine node that import the matching route-targets. This setting is applied to all the BGP neighbors activated in the EVPN Address Family mode. The route-targets can be updated in the outbound using the outbound route-maps as usual.

Default Disabled

Format `retain route-target all`

Mode L2VPN Address-Family Config Mode

Example: Enabling the configuration to retain the route-targets on received EVPN routes from neighbors:

```
(Router) (Config)# router bgp 10
(Router) (Config-router)# address-family l2vpn evpn
(Router) (Config-router-af-evpn)# retain route-target all
(Router) (Config-router-af-evpn)# exit
```

11.1.0.107.1 no retain route-target all

This command resets the retaining of route targets to the default value.

Format `no retain route-target all`

Mode L2VPN Address-Family Config Mode

11.1.0.108 template peer

To create a BGP peer template and enter Peer Template Configuration mode, use the template peer command in Router Configuration mode. A peer template can be configured with parameters that apply to many peers. Neighbors can then be configured to inherit parameters from the peer template. A peer template can include both session parameters and peer policies. Peer policies are configured with an address family configuration mode and apply only to that address family. You can configure up to 32 peer templates. When you make a change to a template, the change is immediately applied to all neighbors that inherit from the template (although policy changes are subject to a three-minute delay).

NOTE: EFOS does not support a **remote-as** *as-numbe*r command in Peer Template Configuration mode. The neighbor's AS number must be specified when the neighbor is created.

Default No peer templates are configured by default.

Format `template peer` *name*

Mode BGP Router Config

Parameter	Description
name	The name of the template. The name may be no more than 32 characters.

Example: The following shows an example of the command.

```
(R1) (Config)# router bgp 65000
(R1) (Config-router)# neighbor 172.20.1.2 remote-as 65001
(R1) (Config-router)# neighbor 172.20.2.2 remote-as 65001
(R1) (Config-router)# template peer AGGR
(R1) (Config-rtr-tmplt)# timers 3 9
(R1) (Config-rtr-tmplt)# local-as 65002 no-prepend replace-as
(R1) (Config-rtr-tmplt)# address-family ipv4
(R1) (Config-rtr-tmplt-af)# send-community
(R1) (Config-rtr-tmplt-af)# route-map RM4-IN in
(R1) (Config-rtr-tmplt-af)# route-map RM4-OUT out
(R1) (Config-rtr-tmplt-af)# exit
(R1) (Config-rtr-tmplt)# address-family ipv6
(R1) (Config-rtr-tmplt-af)# send-community
(R1) (Config-rtr-tmplt-af)# route-map RM6-IN in
(R1) (Config-rtr-tmplt-af)# route-map RM6-OUT out
(R1) (Config-rtr-tmplt-af)# exit
(R1) (Config-rtr-tmplt)# exit
(R1) (Config-router)# neighbor 172.20.1.2 inherit peer AGGR
(R1) (Config-router)# neighbor 172.20.2.2 inherit peer AGGR
(R1) (Config-router)# address-family ipv6
(R1) (Config-router)# neighbor 172.20.1.2 activate
(R1) (Config-router)# neighbor 172.20.2.2 activate
```

11.1.0.108.1 no template peer

Use the no form of the command to delete a peer template.

Format `no template peer` *name*

Mode BGP Router Config

Parameter	Description
name	The name of the template. The name may be no more than 32 characters.

11.1.0.109 update-source

Use this command in Peer Template Configuration mode to configure a peer template to use a specific IP address as the source address for the TCP connection with a neighbor. This IP address must be the IP address configured on the peer as its neighbor address for this router.

Default When no update source is configured, TCP connections use the primary IPv4 address on the outgoing interface to the neighbor.

Format `update-source {slot/port | vlan id}`

Mode Peer Template Config

Parameter	Description
update-source interface	The primary IPv4 address on this interface is used as the source IP address for the TCP connection with the neighbor.

11.1.0.109.1 no update-source

This command configures the peer template to use the primary IPv4 address on the outgoing interface to the neighbor for the TCP connection.

Format `no update-source`

Mode Peer Template Config

11.1.0.110 timers bgp

This command configures the keepalive and hold times that BGP uses for all of its neighbors.

When BGP establishes an adjacency, the neighbors agree to use the minimum hold time configured on either neighbor. BGP sends KEEPALIVE messages at either 1/3 of the negotiated hold time or the configured keepalive interval, whichever is more frequent.

The new values are not applied to adjacencies already in the ESTABLISHED state. A new keepalive or hold time is applied the next time an adjacency is formed.

Default The default keepalive time is 30 seconds. The default hold time is 90 seconds.

Format `timers bgp` *`keepalive holdtime`*

Mode
- BGP Router Config
- IPv4 VRF Address Family Config

Parameter	Description
keepalive	The time, in seconds, between BGP KEEPALIVE packets sent to a neighbor. The range is 0 to 65,535 seconds. Jitter is applied to the keepalive time.

Parameter	Description
holdtime	The time, in seconds, that BGP continues to consider a neighbor to be alive without receiving a BGP KEEPALIVE or UPDATE packet from the neighbor. If no KEEPALIVE is received from a neighbor for longer than the hold time, BGP drops the adjacency. If the hold time is set to 0, then BGP does not enforce a hold time and BGP does not send periodic KEEPALIVE messages. The range is 0 to 65,535 seconds.

11.1.0.110.1 no timers bgp

This command sets to the default the keepalive and hold times that BGP uses for all of its neighbors.

Format `no timers bgp`

Mode BGP Router Config

11.1.0.111 timers policy-apply delay

This command configures the delay after which any change to the global or per BGP neighbor inbound/outbound policies are applied.

Whenever policies (route-maps/prefix-lists/as-path-lists) or neighbor attributes like send-community, remove-private-asn etc. are modified by the user, the policies are scheduled to be applied after the current delay timeout. Whenever the delay is configured by the user, the pending policy changes if any are rescheduled with the new delay if the previous delay timeout is not expired yet. Configuring the delay with the value of 0 seconds means, the changes are applied immediately.

For any change in the outbound policies applicable to a neighbor, the WITHDRAW packets are sent followed by the UPDATE packets when they are applied after the delay timeout. In case of changes to other neighbor attributes like send-community, remove-private-asn etc, the WITHDRAW packets are not sent—instead, the new UPDATEs are sent after the delay timeout.

Default The default delay time is 180 seconds.

Format `timers policy-apply delay delay`

Mode
- BGP Router Config
- IPv4 VRF Address Family Config

Parameter	Description
delay	The time, in seconds, after which the global or per neighbor policies are applied. The range is 0 to 180 seconds.

11.1.0.111.1 no timers policy-apply delay

This command sets to the default the delay after which any change to the global or per BGP neighbor inbound/outbound policies are applied.

Format `no timers policy-apply delay`

Mode BGP Router Config

11.1.0.112 clear ip bgp

This command resets peering sessions with all or a subnet of BGP peers. The command arguments specify which peering sessions are reset and the type of reset performed. Soft inbound reset causes BGP to send a Route Refresh request to each neighbor being reset. If a neighbor does not support the Route Refresh capability, then updated policy is applied to routes previously received from the neighbor.

When a change is made to an outbound policy, BGP schedules an outbound soft reset to update neighbors according to the new policy. Use `interface` specifies if the changes apply to a specific port or to a VLAN.

This command applies to routes for all address families.

Format `clear ip bgp [vrf` *`vrf-name`*`] {* | as-number | ipv4-address | ipv6-address [interface interface-name] | interface interface-name | [listen range network/length ]} [soft [in | out]`

Mode Privileged EXEC

Parameter	Description
vrf-name	The name of the VRF instance.
*	Reset adjacency with every BGP peer
as-number	Only reset adjacencies with BGP peers in the given autonomous system
ipv4-address	Only reset the adjacency with a single specified peer with a given IPv4 peer address.
ipv6-address	Only reset the adjacency with a single specified peer with a given IPv6 peer address. An adjacency that is formed with the autodetect feature cannot be reset with the command.
interface	Only reset the adjacency on a specified interface. The adjacency must be formed with IPv6 link-local or with the auto detect feature
listen range	Reset all adjacency that are included in the listen subnet range.
soft	(Optional) By default, adjacencies are torn down and reestablished. If the **soft** keyword is given, BGP resends all updates to the neighbors and reprocesses updates from the neighbors.
in | out	(Optional) If the **in** keyword is given, then updates from the neighbor are reprocessed. If the **out** keyword is given, then updates are resent to the neighbor. If neither keyword is given, then updates are reprocessed in both directions.

11.1.0.113 clear ip bgp counters

This command resets all BGP counters to 0. These counters include send and receive packet and prefix counters for all neighbors.

Format `clear ip bgp [vrf` *`vrf-name`*`]counters`

Mode Privileged EXEC

11.1.0.114 show ip bgp

To view IPv4 routes in the BGP routing table, use the **show ip bgp** command in Privileged EXEC mode. The output lists both best and non-best paths to each destination. If a VRF instance is specified, the IPv4 routes in the BGP routing table of the VRF instance are displayed.

Format `show ip bgp [vrf` *`vrf-name`*`] [`*`network/pfx-len`* `[ longer-prefixes | shorter-prefixes [` *`length`* `] ] | filter-list` *`as-path-list`*`| prefix-list` *`pfx-list-name`*`]`

Mode Privileged EXEC

Parameter	Description
network/pfx-len	(Optional) Display a specific route identified by its destination prefix
longer-prefixes	(Optional) Used with the network/pfx-len option to show routes whose prefix length is equal to or longer than pfx-len. This option may not be given if the **shorter-prefixes** option is given.
shorter-prefixes [length]	(Optional) Used with the network/pfx-len option to show routes whose prefix length is shorter than pfx-len, and, optionally, longer than a specified length. This option may not be given if the **longer-prefixes** option is given.
filter-list as-path-list	(Optional) Filter the output to the set of routes that match a given AS Path list. This option may not be given if a network/pfx-len option is given, or when a prefix list is given.
pfx-list-name	(Optional) Filter the output to the set of routes that match a given prefix list. This option may not be given if a network/pfx-len option is given or when a filter list is given.

The command output displays the following information.

Parameter	Description
BGP table version	Each time phase 2 of the BGP decision process runs to select new BGP routes, this number is incremented
Status codes	■ s – The route is aggregated into an aggregate address configured with the summary-only option ■ * – EFOS BGP never displays invalid routes; so this code is always displayed ■ > – Indicates that BGP has selected this path as the best path to the destination ■ i – If the route is learned from an internal peer ■ S – This path is STALE. This means either the sender of this path is gracefully restarting in case we are the helper BGP peer (or) the End-of-RIB is yet to be received from the helper BGP peer after this router restarted gracefully.
Network	Destination prefix
Next Hop	The route's BGP NEXT HOP
Metric	Multi Exit Discriminator
LocPrf	The local preference
Path	The AS path
NOTE: The value of the ORIGIN attribute follows immediately after the AS PATH.	

Example: The following shows example CLI display output for the command.

Example #1:

```
(Routing) # show ip bgp

BGP table version is 5, local router ID is 20.1.1.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network            Next Hop     Metric   LocPrf   Path
*> 172.20.1.0/24    100.10.1.1         10      100   20 10        i
                    200.10.1.1
*> 172.20.2.0/24    100.10.1.1         10      100   20 10        ?
```

Example #2: If one or more of the three well-known communities in RFC 1997 is attached to a path, **show ip bgp** lists them.

```
(Routing) # show ip bgp
```

```
BGP table version is 5, local router ID is 20.1.1.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network            Next Hop     Metric   LocPrf   Path
*> 172.20.1.0/24    100.10.1.1         10      100   20 10        i
   Communities: no-export
*> 24.95.16.0/24    100.10.1.1         10      100   20 10        i
   Communities: no-advertise
*> 24.14.8.0/24     100.10.1.1         10      100   20 10        i
   Communities: no-export-subconfed
S*>24.14.9.0/24     100.10.1.2         10      100   30 20  i
```

If the command is given with network/pfx-len option and without any additional options, then the output format lists more information about the individual prefix. The best path is always listed first, followed by any non-best paths. The output only shows attributes that are included with each path.

Parameter	Description
Prefix/Prefix Length	The destination prefix and prefix length.
Generation ID	The version of the BGP routing table when this route last changed.
Forwarding	Whether this BGP route is used for forwarding.
Advertised To Update Groups	The outbound update groups that this route is advertised to.
Local Preference	The local preference, either as received from the peer or as set according to local policy.
AS Path	The AS Path. This form of show ip bgp displays AS Paths as long as allowed by bgp maxas-limit.
Origin	Value of the ORIGIN attribute.
Metric	Value of the MED attribute, if included.
Type	Whether the path is received from an internal or external peer.
IGP Cost	The interior gateway cost (e.g., OSPF cost) to the BGP NEXT HOP.
Peer (Peer ID)	The IP address of the peer that sent this route, and its router ID.
BGP Next Hop	The BGP NEXT HOP attribute.
Atomic Aggregate	If the ATOMIC AGGEGATE attribute is attached to the path.
Aggregator	The AS number and router ID of the speaker that aggregated the route.
Communities	The BGP communities attached to the path.
Originator	The value of the ORIGINATOR attribute, if the attribute is attached to the path.
Cluster list	The value of the CLUSTER LIST attribute, if the attribute is attached to the path.

Example: The following shows example CLI display output for the command.

```
(R1)  # show ip bgp 172.20.1.0/24

Prefix/Prefix Length..................... 172.20.1.0/24
Generation ID............................ 2056
Forwarding............................... Yes
Advertised to Update Groups.............. 1, 5

Best Path:
Local Preference......................... 100
AS Path.................................. 20 10
Origin................................... IGP
Metric................................... 10
Type..................................... External
IGP Cost................................. 30
```

```
Peer (Peer ID)............................. 100.10.1.1 (32.4.1.1)
BGP Next Hop............................... 100.10.1.1
Atomic Aggregate........................... Included
Aggregator (AS, Router ID)................. 300, 14.1.1.1
Communities................................ no-export

Non-best Paths:
Local Preference........................... 200
AS Path.................................... 18 50 27
Origin..................................... Incomplete
Type....................................... External
IGP Cost................................... 10
Peer (Peer ID)............................. 200.1.1.1 (18.24.1.3)
BGP Next Hop............................... 200.1.1.1
```

11.1.0.115 show ip bgp aggregate-address

This command lists aggregate addresses that have been configured and indicates whether each is currently active. If a VRF is specified, the aggregate addresses configured in a VRF instance are displayed.

Format `show ip bgp [vrf vrf-name] aggregate-address`

Mode Privileged EXEC

Parameter	Description
Prefix/Len	Destination prefix and prefix length
AS Set	Indicates whether an empty AS path is advertised with the aggregate address (N) or an AS SET is advertised with the set of AS numbers for the paths contributing to the aggregate (Y)
Summary Only	Indicates whether the individual networks are suppressed (Y) or advertised (N).
Active	Indicates whether the aggregate is currently being advertised.

Example: The following shows example CLI display output for the command.

```
(Routing) # show ip bgp aggregate-address

Prefix/Len    AS Set    Summary Only    Active

10.0.0.0/8         N               Y         Y
20.0.0.0/8         N               Y         N
```

11.1.0.116 show ip bgp community

This command shows BGP IPv4 routes that belong to a specified set of communities.

Format *show ip bgp* `[vrf` *vrf-name*`]` *community communities [exact-match]*

Mode Privileged EXEC

Parameter	Description
vrf-name	(Optional) Displays routes belonging to communities within a VRF instance.

Parameter	Description
communities	A string of zero or more community values, which may be in either format and may contain the well-known community keywords no-advertise and no-export. The output displays routes that belong to every community specified in the command.
exact-match	(Optional) Only displays routes that are members of those and only those communities specified in the command.

11.1.0.117 show ip bgp community-list

This command displays IPv4 routes that match a community list. The output format and field descriptions are the same as for Section 11.1.0.114, show ip bgp.

Format *show ip bgp* [vrf *vrf-name*] *community communities [exact-match]*

Mode Privileged EXEC

Parameter	Description
vrf-name	(Optional) Displays routes belonging to communities within a VRF instance.
name	A standard community list name.
exact-match	(Optional) Display only routes that are an exact match for the set of communities in the matching community list statement.

11.1.0.118 show ip bgp extcommunity-list

This command displays all the permit and deny attributes of the given extended community list. If the *list-name* is specified, the output is displayed that matches the given *list-name*; else all the lists are displayed.

Format *show ip bgp extcommunity-list* [*list-name*]

Mode Privileged EXEC

Parameter	Description
list-name	A standard extended community list name.

The following information is displayed.

Field	Description
Standard extended community-list	The standard named extended community list
permit	Permits access for a matching condition. Once a permit value has been configured to match a given set of extended communities the extended community list defaults to an implicit deny for all other values.
RT	The route target extended community attribute.
deny	Denies access for a matching condition.

Example:

```
(Routing) # show ip bgp extcommunity-list 1
Standard extended community-list list1
permit RT:1:100 RT:2:100
```

```
deny RT:6:600
permit RT:5:200
permit SOO:9:900
```

11.1.0.119 show ip bgp listen range

This command displays information about the IPv4 BGP listen subnet ranges. If network/length are specified, information about the specified listen range are displayed.

Format *show ip bgp* [*network/length*]
Mode Privileged EXEC

Example:

```
(Routing) (Config-router)#show ip bgp listen range

Listen Range ................................... 10.27.0.0/16
Inherited Template ............................. template_10_27

  Member             ASN       State
  ---------------- ----- -----------
  10.27.8.189      65001 OPENCONFIRM
  10.27.128.235        0      ACTIVE


Listen Range ................................... 15.15.0.0/24
Inherited Template ............................. template_15_15

  Member             ASN       State
  ---------------- ----- -----------
```

11.1.0.120 show ip bgp neighbors policy

This command displays the inbound and outbound IPv4 policies configured for a specific peer. The output distinguishes policies that are configured on the peer itself and policies that the peer inherits from a peer template.

Format `show ip bgp [vrf` *vrf-name*`] neighbors` *ipv4-address* `[interface [`*interface-name*`] policy`
Mode Privileged EXEC

Parameter	Description
vrf-name	(Optional) Display routes belonging to communities within a VRF instance.
ip-address	(Optional) Specifies an IPv4 address of a neighbor to which to limit the output.

The command output displays the following information.

Parameter	Description
Neighbor	The peer address of a neighbor.
Policy	A neighbor-specific BGP policy.
Template	If the policy is inherited from a peer template, this field lists the template name.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip bgp neighbors 172.20.101.100 policy

Neighbor        Policy                          Template
--------------- ------------------------------- ------------------------
172.20.101.100  advertisement-interval 600
                default-originate
                filter-list 500 in
                filter-list 500 out
                prefix-list barney in
                prefix-list wilma out
                maximum-prefix unlimited 100 warning-only   torPeers
                route-map fred in                           torPeers
                route-map dino out                          torPeers
                send-community                              torPeers
                advertisement-interval 600                  torPeers
                default-originate                               torPeers
```

11.1.0.121 show ip bgp neighbors

This command shows details about BGP neighbor configuration and status. If the neighbor is configured to inherit configuration parameters from a peer template, the output shows the inherited values. If a VRF is specified, neighbors belonging to the VRF instance are displayed.

NOTE: Policy configuration is moved from this command to the Section 11.1.0.120, show ip bgp neighbors policy command.

Format *show ip bgp* [vrf *vrf-name*] *neighbors [ip-address]*

Mode Privileged EXEC

Parameter	Description
vrf-name	(Optional) Display routes belonging to communities within a VRF instance.
ip-address	(Optional) The IP address of a neighbor. Used to limit the output to show a single neighbor.

The command output displays the following information.

Parameter	Description
Description	Text string assigned using the command Section 11.1.0.58, neighbor description. This text string only appears if a description is configured.
Remote Address	The neighbor's IP address
Remote AS	The neighbor's autonomous system number
BFD Enabled to Detect Fast Failover	Specifies if BFD has been enabled for BGP neighbors.
Peer ID	The neighbor's BGP router ID
Peer Admin Status	START or STOP
Peer Type	If a neighbor was created with the BGP dynamic neighbors feature, Dynamic is shown.
Listen Range	If the neighbor was created with the BGP dynamic neighbors feature, the field shows the listen range to which the neighbor belongs.
Listen Range	The listen range.
Local Interface Address	The IPv4 address used as the source IP address in packets sent to this neighbor.

Parameter	Description
Local Port	TCP port number on the local end of the connection
Remote Port	TCP port number on the remote end of the connection
Connection Retry Interval	How long BGP waits between connection retries
Neighbor Capabilities	Optional capabilities reported by the neighbor, recognized and accepted by this router. Codes listed in the show output are as follows: ■ MP: Multiprotocol ■ RF: Route Refresh ■ AS4: 4-Byte ASN This version of EFOS does not support any multiprotocol AFI/SAFI pairs other than IPv4 unicast. The presence of this capability does not imply otherwise.
IPv4 Unicast Support	Indicates whether IPv4 unicast routes can be exchanged with this peer. **Both** indicates that IPv4 is active locally and the neighbor indicated support for IPv4 unicast in its OPEN message. **Sent** indicates that IPv4 unicast is active locally, but the neighbor did not include this AFI/SAFI pair in its OPEN message. IPv4 unicast is always enabled locally and cannot be disabled.
IPv6 Unicast Support	Indicates whether IPv6 unicast routes can be exchanged with this peer. **Both** and **Sent** have the same meaning as for IPv4. **None** indicates that neither the local router nor the peer has IPv6 enabled for this adjacency. **Received** indicates that the peer advertised the IPv6 unicast capability, but it is not enabled locally. IPv6 unicast is enabled locally using the neighbor activate command in address-family IPv6 configuration mode.
L2VPN EVPN Support	Indicates whether EVPN routes can be exchanged with this peer. This capability is enabled locally using the neighbor activate command in address-family l2vpn evpn configuration mode.
Graceful Restart Support	Indicates whether the neighbor supports the Graceful Restart behavior.
Graceful Restart Helper Support	Indicates whether the neighbor can help us to gracefully restart.
Update Source	The configured value for the source IP address of packets sent to this peer. This field is only included in the output if the update source is configured.
Configured Hold Time	The time, in seconds, that this router proposes to this neighbor as the hold time
Configured Keep Alive Time	The configured KEEPALIVE interval for this neighbor.
Negotiated Hold Time	The minimum of the configured hold time and the hold time in the OPEN message received from this neighbor. If the local router does not receive a KEEPALIVE or UPDATE message from this neighbor within this interval of time, the local router drops the adjacency. This field is only shown if the adjacency state is OPEN CONFIRM or greater.
MD5 Password	The TCP MD5 password, if one is configured, in plain text.
Keep Alive Time	The number of seconds between KEEPALIVE messages sent to this neighbor. This field is only shown if the adjacency state is OPEN CONFIRM or greater.
Last Error (Sent)	The last error that occurred on the connection to this neighbor
Last SubError	The suberror reported with the last error.
Established Transitions	The number of times the adjacency has transitioned into the Established state
Established Time	How long since the connection last transitioned to or from the Established state
Time Since Last Update	How long since an UPDATE message has been received from this neighbor
IPv4 Outbound Update Group	The outbound update group ID.
L2VPN Outbound Update Group	The outbound update group ID.
IPv6 Outbound Update Group	The outbound update group ID.
Message Table	The number of BGP messages sent to and received from this neighbor
Received UPDATE Queue Size	Received UPDATE messages are queued for processing. This section shows the current length of the neighbor's UPDATE queue in bytes, the high water mark, the limit, and the number of UPDATEs that have been dropped because the queue reached the limit.
The following fields are displayed for IPv4, L2VPN EVPN, and IPv6 (If active)	

Parameter	Description
Prefixes Advertised	A running count of the number of prefixes advertised to or received from this neighbor
Prefixes Withdrawn	A running count of the number of prefixes included in the Withdrawn Routes portion of UPDATE messages, to and from this neighbor
Prefixes Current	The number of prefixes currently advertised to or received from this neighbor. For inbound prefixes, this count only includes prefixes that passed inbound policy.
Prefixes Accepted	The number of prefixes from this neighbor that are eligible to become active in the local RIB. Received prefixes are ineligible if their BGP Next Hop is not resolvable or if the AS Path contains a loop. A prefix is only considered accepted if it passes inbound policy.
Prefixes Rejected	The number of prefixes currently received from this neighbor that fail inbound policy.
Max NLRI per Update	The maximum number of prefixes included in a single UPDATE message, to and from this neighbor
Min NLRI per Update	The minimum number of prefixes included in a single UPDATE message, to and from this neighbor

Example: The following shows example CLI display output for the command.

```
(Routing) # show ip bgp neighbors 172.20.1.100

Description: spine 1 router 1

Remote Address ................................ 172.20.1.100
Remote AS ..................................... 100
BFD Enabled to Detect Fast Fallover............ Yes
Peer ID ....................................... 14.3.0.1
Peer Admin Status ............................. START
Peer State .................................... ESTABLISHED
Peer Type ..................................... DYNAMIC
Listen Range .................................. 172.20.0.0/16
Local Interface Address ....................... 172.20.1.2
Local Port .................................... 179
Remote Port ................................... 58265
Connection Retry Interval ..................... 120 sec
Neighbor Capabilities ......................... None
IPv4 Unicast Support .......................... Both
IPv6 Unicast Support .......................... Sent
L2VPN EVPN Support   .......................... Advertised and Received
Graceful Restart Support....................... Enabled
Graceful Restart Helper Support................ Enabled

Update Source.................................
Configured Hold Time .......................... 90 sec
Configured Keep Alive Time..................... 30 sec
Negotiated Hold Time .......................... 30 sec
Keep Alive Time ............................... 10 sec

MD5 Password................................... password

Last Error (Sent).............................. Hold Timer Expired
Last SubError.................................. None
Time Since Last Error.......................... 0 day 0 hr 4 min 27 sec
Established Transitions ....................... 1
Established Time .............................. 0 day 0 hr 4 min 25 sec
Time Elapsed Since Last Update ................ 0 day 0 hr 4 min 245 sec
IPv4 Outbound Update Group..................... 3
```

```
L2VPN Outbound Update Group ..................... 0
IPv6 Outbound Update Group..................... 7



             Open   Update   Keepalive   Notification   Refresh   Total
Msgs Sent       1        0          10              0         0      11
Msgs Rcvd       1        1          11              0         0      12

Received UPDATE Queue Size:  0 bytes. High: 355. Limit 196096. Drops 0.

IPv4 Prefix Statistics:
                           Inbound       Outbound
Prefixes Advertised              1              0
Prefixes Withdrawn               0              0
Prefixes Current                 1              0
Prefixes Accepted              1          N/A
Prefixes Rejected                1            N/A
Max NLRI per Update              1              0
Min NLRI per Update              1              0

L2VPN Prefix Statistics:
                           Inbound       Outbound
Prefixes Advertised              3              3
Prefixes Withdrawn               0              0
Prefixes Current                 3              3
Prefixes Accepted                3            N/A
Prefixes Rejected                0            N/A
Max NLRI per Update              1              2
Min NLRI per Update              0              1

IPv6 Prefix Statistics:
                           Inbound       Outbound
Prefixes Advertised              1              0
Prefixes Withdrawn               0              0
Prefixes Current                 1              0
Prefixes Accepted1 N/A
Prefixes Rejected                1            N/A
Max NLRI per Update              1              0
Min NLRI per Update              1              0
```

If the router receives an UPDATE message with an invalid path attribute, the router will in most cases send a NOTIFICATION message and reset the adjacency. BGP maintains a per-neighbor counter for each type of path attribute error. This show command lists each non-zero counter, just after the LastSubError. The counters that may be listed are as follows:

Parameter	Description
Path with duplicate attribute	The peer sent an UPDATE message containing the same path attribute more than once.
Path with well-known/optional conflict	A received path attribute was flagged as both well-known and optional or neither well-known nor optional.
Transitive flag not set on transitive attr	A received path attribute is known to be transitive, but the transitive flag is not set.
Mandatory attribute non-transitive or partial	A mandatory path attribute was received with either the transitive or partial flag set.
Optional attribute non-transitive and partial	An optional path attribute has the transitive flag clear and the partial flag set.
Path attribute too long	A received path attribute was longer than the expected length.

Parameter	Description
Path attribute length error	A received path attribute has a length value that exceeds the remaining length of the path attributes field.
Invalid ORIGIN code	A received UPDATE message included an invalid ORIGIN code.
Unexpected first ASN in AS path	The AS Path attribute from an external peer did not include the peer's AS number as the first AS.
Invalid AS path segment type	The AS Path includes a segment with an invalid segment type.
Invalid BGP NEXT HOP	The BGP NEXT HOP is not a valid unicast address.
Bad BGP NEXT HOP	The BGP NEXT HOP was either the receiver's IP address or an IP address outside the subnet to the peer.
Invalid AGGREGATOR attribute	The AGGREGATOR attribute was invalid.
Unrecognized well-known path attribute	An UPDATE message contained a path attribute with the Optional flag clear, but this router does not recognize the attribute.
Missing mandatory path attribute	An UPDATE message was received without a mandatory path attribute.
Missing LOCAL PREF attribute	An UPDATE message was received from an internal peer without the LOCAL PREF attribute.
Invalid prefix in UPDATE NLRI	An UPDATE message received from this peer contained a syntactically incorrect prefix.

Example: In this example, BGP has received an UPDATE message from an external peer 172.20.101.100 with something other than the peer's ASN as the first ASN in the AS Path. The additional counter shows that this occurred one time.

```
(Routing) #show ip bgp neighbors 172.20.101.100

Remote Address ............................... 172.20.101.100
Remote AS .................................... 101
...

Last Error ................................... UPDATE Message Error
Last SubError ................................ Malformed AS_PATH
Unexpected first ASN in AS path ............... 1

Established Transitions ...................... 1
Established Time ..............................   0 days 00 hrs 00 mins 10 secs
```

11.1.0.122 show ip bgp neighbors advertised-routes

This command displays the list of IPv4 routes advertised to a specific neighbor. These are the routes in the adjacent RIB out for the neighbor's outbound update group.

Format `show ip bgp [vrf` *`vrf-name`*`] neighbors ip-address advertised-routes`

Mode Privileged EXEC

Parameter	Description
vrf-name	(Optional) Display routes belonging to communities within a VRF instance.
ip-address	The IP address of a neighbor.

The command output displays the following information.

Parameter	Description
BGP table version	Each time phase 2 of the BGP decision process runs to select new BGP routes, this number is incremented
Status codes	p – The route has been updated in Adj-RIB-Out since the last UPDATE message was sent. Transmission of an UPDATE message is pending.
Network	Destination prefix
Next Hop	The BGP NEXT HOP as advertised to the peer.
Local Pref	The local preference. Local preference is never advertised to external peers.
Metric	The value of the Multi Exit Discriminator, if the MED is advertised to the peer.
Path	The AS path. The AS path does not include the local AS number, which is added to the beginning of the AS path when a route is advertised to an external peer.
NOTE: The value of the ORIGIN attribute follows immediately after the AS Path.	

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip bgp neighbors 172.20.101.100 advertised-routes

BGP table version is 5, local router ID is 20.1.1.1
Status codes: p advertisement pending
Origin codes: i - IGP, e - EGP, ? - incomplete

Originating default network 0.0.0.0

  Version   Network            Next Hop     Metric   Local Pref  Path
  5         172.20.1.0/24  172.20.101.1         10          100 20 10       i
p 5         20.1.1.0/24    172.20.101.1                     100    20       ?
```

NOTE: This output differs slightly from the output in **show ip bgp**. Suppressed routes and non-best routes are not advertised, so these status codes are not relevant here. Advertised routes always have a single next hop, the BGP NEXT HOP advertised to the peer. Local preference is never sent to external peers.

The output indicates whether BGP is configured to originate a default route to this peer (neighbor default-originate).

11.1.0.123 show ip bgp neighbors policy

This command displays the inbound and outbound IPv4 and L2VPN policies configured for a specific peer. The output distinguishes policies that are configured on the peer itself and policies that the peer inherits from a peer template.

Format `show ip bgp [vrf` *`vrf-name`*`] neighbors [{ip-address]} policy`

Mode Privileged EXEC

Parameter	Description
vrf-name	(Optional) Display the names of the communities within a VRF instance.
ip-address	(Optional) Specifies an IPv4 address of a neighbor to which to limit the output.

The command output displays the following information.

Parameter	Description
Neighbor	The peer address of a neighbor.
Addr-Family	The peer address family type.

Parameter	Description
Policy	A neighbor-specific BGP policy.
Template	If the policy is inherited from a peer template, this field lists the template name.

Example: The following shows example CLI display output for the command.

```
(router) #show ip bgp neighbors 192.168.10.2 policy

Neighbor        Addr-family           Policy                      Template
--------------- ----------- ---------------------------------  ---------------
192.168.10.2    IPv4        advertisement-interval 5
                            default-originate if-default-present
                            filter-list 0 in
                            filter-list 0 out
                            next-hop-self disabled
                            prefix-list  in
                            prefix-list  out
                            maximum-prefix 8160
                            remove-private-as send-as-all
                            route-map  in
                            route-map  out
                            route-reflector-client  disabled
                            send-community disabled

192.168.10.2    EVPN        activate
                            maximum-prefix 102400
                            route-reflector-client  disabled
                            send-community disabled
                            send-extended-community disabled
```

11.1.0.124 show ip bgp neighbors {received-routes | routes | rejected-routes}

This command displays the list of IPv4 routes received from a specific neighbor. The list includes either all routes received from the neighbor, received routes that passed inbound policy, or routes rejected by inbound policy. If a VRF instance is specified, the routes information is displayed for the neighbors in the VRF instance.

Format `show ip bgp [vrf` *`vrf-name`*`] neighbors [`*`ip-address`* `{received-routes | routes | rejected-routes}]`

Mode Privileged EXEC

Parameter	Description
vrf-name	(Optional) Display the routes belonging to communities within a VRF instance.
ip-address	(Optional) The IP address of a neighbor.
received-routes	Display all routes received from this neighbor, regardless of if the routes passed inbound policy
routes	Display only routes that passed inbound policy.
rejected-routes	Display only routes rejected by inbound policy.

The command output displays the following information.

Parameter	Description
Network	Destination prefix
Next Hop	The BGP NEXT HOP as advertised by the peer.
Metric	The value of the Multi Exit Discriminator, if a MED is received from the peer.
Local Pref	The local preference received from the peer.
Path	The AS path as received from the peer
Origin	The value of the Origin attribute as received from the peer

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip bgp neighbors 172.20.101.100 received-routes

local router ID is 20.1.1.1
Origin codes: i - IGP, e - EGP, ? - incomplete


Network        Next Hop         Metric   Local Pref  Path  Origin
172.20.1.0/24  172.20.101.1         10          100 20 10       i
20.1.1.0/24    172.20.101.1                     100    20       ?
```

11.1.0.125 show ip bgp route-reflection

This command displays all global configuration related to IPv4 route reflection, including the cluster ID and whether client-to-client route reflection is enabled, and lists all the neighbors that are configured as route reflector clients. If a VRF instance is specified, the routes belonging to communities within a VRF instance are displayed.

If a route reflector client is configured with an outbound route map, the output warns that set statements in the route map are ignored when reflecting routes to this client.

Format `show ip bgp [vrf` *`vrf-name`*`] route-reflection`

Mode Privileged EXEC

Parameter	Description
Cluster ID	The cluster ID used by this router. The value configured with the Section 11.1.0.15, bgp cluster-id command is displayed. If no cluster ID is configured, the local router ID is shown and tagged as default.
Client-to-client Reflection	Displays *Enabled* when this router reflects routes received from its clients to its other clients; otherwise *Disabled* displays.
Clients	A list of this router's internal peers that have been configured as route reflector clients.
Non-client Internal Peers	A list of this router's internal peers that are not configured as route reflector clients. Routes from non-client peers are reflected to clients and vice-versa.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip bgp route-reflection

Cluster ID ..................................... 1.1.1.1 (configured)
Client-to-client Reflection ................... Enabled
Clients: 172.20.1.2, 172.20.3.2, 172.20.5.2
Non-client Internal Peers: 192.168.1.2, 192.162.2.2
Skipping set statements in outbound route map gandolf when reflecting to internal peer 172.20.1.2.
```

11.1.0.126 show ip bgp statistics

This command displays recent decision process history. Phase 1 of the decision process reacts to UPDATE messages received from peers, determining what new routes are accepted and deleting withdrawn routes from the Adj-RIB-In. Phase 2 determines the best path for each destination, updates the BGP route table, and updates the common RIB. Phase 3 is run independently for each outbound update group and determines which routes should be advertised to neighbors in each group. Each entry in the table shows statistics for one phase of the decision process. The table shows the 20 most recent decision process runs, with the most recent information at the end of the table. If a VRF instance is specified, the statistics for the routes belonging to communities within the VRF instance are displayed.

Format `show ip bgp [vrf vrf-name] statistics`

Mode Privileged EXEC

The command displays the following information.

Parameter	Description
Delta T	How long since the decision process was run. hours:minutes:seconds if the elapsed time is less than 24 hours. Otherwise, days:hours.
Phase	Which phase of the decision process was run
Upd Grp	Outbound update group ID. Only applies when phase 3 is run.
GenId	Generation ID of BGP routing table when decision process was run. The generation ID is incremented each time phase 2 of the decision process is run and when there is a change to the status of aggregate addresses.
Reason	The event that triggered the decision process to run
Peer	Phase 1 of the decision process can be triggered for a specific peer when a peer's inbound routing policy changes or the peer is reset. When phase 1 is run for a single peer, the peer's IP address is given.
Duration	How long the decision process took, in milliseconds
Adds	The number of routes added. For phase 1, this is the number of prefixes that pass inbound policy and are added to the Accept-RIB-In. For phase 2, this is the number of routes added to the BGP routing table. For phase 3, this is the number of prefixes added to the update group's Adj-RIB-Out.
Mods	The number of routes modified. Always 0 for phase 1.
Dels	The number of routes deleted. Always 0 for phase 1.

Example: The following shows example CLI display output for the command.

```
(Routing) # show ip bgp statistics

  Delta T  Phase  Upd Grp   GenId          Reason       Peer  Duration  Adds  Mods  Dels
 29:33:49      3        0    2041  Fwd status chng                  34   750     0   500
 29:33:40      2             2042   Accept-RIB-In-                  59   750     0   500
 29:33:28      2             2043   Accept-RIB-In-                  10     0     0   250
 29:23:40      2             2044   Accept-RIB-In-                  32     0     0  1000
 29:13:40      3        1    2044     Phase 2 done                  48   500  2500  1750
 29:02:40      1             2044      Adj-RIB-In+                  21   500     0     0
 29:02:01      3        0    2044     Phase 2 done                  41   750     0  1250
 28:33:40      2             2045     Phase 1 done                       32   500     0
 28:15:00      1             2045      Adj-RIB-In+                    9   250     0     0
 28:14:40      2             2046     Phase 1 done                      16   250     0
```

11.1.0.127 show ip bgp summary

This command displays a summary of BGP configuration and status. If a VRF instance is specified, the configuration and status for the routes in belonging to communities withing the specified VRF instance are displayed.

Format `show ip bgp [vrf vrf-name] summary`
Mode Privileged EXEC

The command displays the following information.

Parameter	Description
IPv4 Routing	Whether IPv4 routing is globally enabled. BGP does not include the IPv4 unicast AFI/SAFI capability in OPEN messages it sends unless routing is globally enabled.
BGP Admin Mode	Whether BGP is globally enabled
BGP Router ID	The configured router ID
Local AS Number	The router's AS number
Traps	Whether BGP traps are enabled.
Maximum Paths	The maximum number of next hops in an external BGP route.
Maximum Paths iBGP	The maximum number of next hops in an internal BGP route.
Default Keep Alive Time	The configured keepalive time used by all peers that have not been configured with a peer-specific keepalive time.
Default Hold Time	The configured hold time used by all peers that have not been configured with a peer-specific hold time.
Number of Network Entries	The number of distinct prefixes in the local RIB
Number of AS Paths	The number of AS paths in the local RIB
Default Metric	The default value for the MED for redistributed routes.
Default Route Advertise	Whether BGP is configured to advertise a default route. Corresponds to the Section 11.1.0.23, default-information originate command.
Redistributing Source	A source of routes that BGP is configured to redistribute.
Metric	The metric configured with the redistribute command.
Match Value	For routes redistributed from OSPF, the types of OSPF routes being redistributed.
Distribute List	The name of the prefix list used to filter redistributed routes, if one is configured with the Section 11.1.0.32, distribute-list prefix outcommand.
Route Map	The name of the route map used to filter redistributed routes.
Dynamic Neighbors	Shows the current number of created dynamic IPv4 BGP neighbors, high water mark and a limit of dynamic IPv4 BGP neighbors that can be created.
Neighbor	The IP address of a neighbor. A neighbor, that is created with BGP dynamic neighbors feature, will be marked with "*".
ASN	The neighbor's ASN
MsgRcvd	The number of BGP messages received from this neighbor
MsgSent	The number of BGP messages sent to this neighbor
State	The adjacency state. One of IDLE, CONNECT, ACTIVE, OPEN SENT, OPEN CNFRM, EST
Up/Down Time	How long the adjacency has been in the ESTABLISHED state, or, if the adjacency is down, how long it has been down. In days:hours:minutes:seconds
Pfx Rcvd	The number of prefixes received from the neighbor

Example: The following shows example CLI display output for the command.

```
(Routing) # show ip bgp summary
```

```
Admin Mode.............................Enable
BGP Router ID..........................172.20.1.1
Local AS Number........................200
Traps..................................Disable
Maximum Paths..........................32
Maximum Paths iBGP.....................16
Default Keep Alive Time................30 sec
Default Hold Time......................90 sec
Number of Network Entries..............20
Number of AS Paths.....................5

Default Metric.............................. Not configured
Default Route Advertise..................... No

Redistributing..............................
Source...................................... ospf
Metric...................................... Not Configured
Match Value................................. 'internal'
Distribute List............................. Not configured

Neighbor      ASN    MsgRcvd  MsgSent      State  Up/Down Time   Pfx Rcvd
100.10.1.1     50         48       92        EST      00:47:30         20
100.20.1.4     20          0        2   OPEN SENT                       0
```

11.1.0.128 show ip bgp template

Use this command to view information about all configured BGP peer templates or for the specified BGP template.

Format `show ip bgp template` *name*

Mode Privileged EXEC

Term	Definition
Name	The name of a BGP peer template
AF	The address family to which the configuration command applies. This field is blank for session parameters, which apply to all address families.
Configuration	Configuration commands that are included in the template.

Example: The following shows example CLI display output for the command.

```
(router) #show ip bgp template

Template Name   AF    Configuration
-------------  ----   ----------------------------
peer-grp1             timers 5 15
                      password rivendell
               IPv4   advertisement-interval 15


peer-grp2      IPv4   prefix-list strider in
               IPv4   maximum-prefix 100
               IPv6   prefix-list gandolf in
               IPv6   maximum-prefix 200

peer-grp3      IPv6   send-community
```

```
peer-grp4              update-source loopback 0
               IPv4    next-hop-self
```

11.1.0.129 show ip bgp traffic

This command reports global BGP message counters for transmitted and received messages along with BGP work queue information. If a VRF instance is specified, the counters belonging to communities within that VRF instance are displayed.

Format `show ip bgp [vrf` *`vrf-name`*`] traffic`

Mode Privileged EXEC

The first table lists the number of BGP messages of each type that this router has sent and received. Following the table is a maximum send and receive UPDATE message rate. These rates report the busiest one-second interval.

The queue statistics table reports information for BGP work queues. Items placed on each of these work queues are as follows:

Term	Description
Events	Includes most timer events and configuration changes.
Keepalive Tx	Includes timer events to send a KEEPALIVE message to a peer.
Dec Proc	Includes events that cause the decision process to be run.
Rx Data	holds incoming BGP messages.
RTO Notifications	Includes best route change and next hop resolution change notifications from the routing table.
MIB Queries	Includes pending SNMP queries for BGP status

Example: The following shows example CLI display output for the command.

```
(router) #show ip bgp traffic
Time Since Counters Cleared: 55223 Seconds
BGP Message Statistics
                Open     Update  Notification   Keepalive    Refresh      Total
Recd:              6         11              0        7888          0       7905
Sent:              8         56              3        8465          0       8532

Max Received UPDATE rate: 1 pps
Max Send UPDATE rate: 5 pps

BGP Queue Statistics
             Current         Max       Drops       Limit
Events             0           2           0         800
Keepalive Tx       0           3           0         128
Dec Proc           0           3           0         133
Rx Data            0           3           0         500
RTO Notifications  0           4           0        1222
MIB Queries        0           0           0           5
```

11.1.0.130 show ip bgp update-group

This command reports the status of outbound update groups and their members. If a VRF instance is specified, the status of the update groups for that VRF instance are displayed.

Format `show ip bgp [vrf vrf-name] update-group [ipv4-address | ipv6-address ]`

Mode Privileged EXEC

Parameter	Description
ipv4-address | ipv6-address	(Optional) If specified, this option restricts the output to the update group containing the peer with the given IPv4 or IPv6 address.

The command displays the following information.

Parameter	Description
Update Group ID	Unique identifier for outbound update group
Peer Type	Whether peers in this update group are internal or external
Minimum Advertisement Interval	The minimum time, in seconds, between sets of UPDATE messages sent to the group
Send Community	If the BGP communities are included in route advertisements to members of the group.
Remove Private ASNs	If BGP removes private ASNs from paths advertised to members of this update group. ■ Replace if BGP replaces private ASNs with the local ASN. ■ Remove if private ASNs are simply removed. ■ Otherwise No.
Route Reflector Client	If peers in this update group are route reflector clients.
Neighbor AS Path Access List Out	The AS path access list used to filter UPDATE messages sent to peers in the update group
Neighbor Prefix List Out	Name of the prefix list used to filter prefixes advertised to the peers in the update group
Members Added	The number of peers added to the group since the group was formed
Members Removed	The number of peers removed from the group
Update Version	The number of times phase 3 of the BGP decision process has run for this group to determine which routes should be advertised to the group
Number of UPDATEs Sent	The number of UPDATE messages that have been sent to this group. Incremented once for each UPDATE regardless of the number of group members
Time Since Last UPDATE	Time since an UPDATE message was last sent to the group. If no UPDATE has been sent to the group, the status is “Never.”
Current Prefixes	The number of prefixes currently advertised to the group
Current Paths	The number of paths currently advertised to the group
Prefixes Advertised	The total number of prefixes advertised to the group since the group was formed
Prefixes Withdrawn	The total number of prefixes included in the Withdrawn Routes field of UPDATE messages sent to the group since the group was formed
UPDATE Send Failures	The number of UPDATE messages that failed to be delivered to all members of the group
Current Members	The IPv4 address of all current members of the group

The update send history table show statistics on as many as the ten most recent executions of the update send process for the update group. Items in the history table are as follows:

Parameter	Description
Version	The update version
Delta T	The amount of time elapsed since the update send process executed. hours::minutes::seconds.
Duration	How long the update send process took, in milliseconds
UPD Built	The number of UPDATE messages built

Parameter	Description
UPD Sent	The number of UPDATE messages successfully transmitted to group members. Normally a copy of each UPDATE message built is sent to each group member.
Paths Sent	The number of paths advertised
Pfxs Adv	The number of prefixes advertised
Pfxs Wd	The number of prefixes withdrawn

Example: The following shows an example of the command displaying information for all update groups.

```
(Routing) # show ip bgp update-group

Update Group ID.............................. 0
Peer Type.................................... External
Minimum Advertisement Interval.............. 30 seconds
Remove Private ASNs.......................... No
Route Reflector Client....................... No
Neighbor AS Path Access List Out............. 1
Neighbor Prefix List Out..................... pfxList1
Members Added................................ 48
Members Removed.............................. 0
Update Version............................... 19
Number of UPDATEs Sent....................... 512
Time Since Last Update....................... 5 hrs 3 min 2 sec
Current Prefixes............................. 5500
Current Paths................................ 22
Prefixes Advertised.......................... 191250
Prefixes Withdrawn........................... 186000
UPDATE Send Failures......................... 0

Current Members:  172.20.1.100, 172.20.2.100

   Version   Delta T Duration UPD Built UPD Sent Paths Sent Pfxs Adv  Pfxs Wd
        10   00:33:49      100         6      288          5     1250      750
        11   00:33:49        0         4      192          3      750      250
        12   00:33:49        0         2       96          1      250     1000
        13   00:33:49        0         2       96          1      250     1018
        14   00:33:49        0         1       48          0        0      482
        15   00:33:49      100         8      384          7     1750      750
        16   00:33:49        0         3      144          2      500      250
        17   00:31:49        0         4      192          3      750      750
        18   00:23:49      100         4      192          3      750     1000
        19   00:03:49      100         6      288          5     1250      500


Update Group ID.............................. 1
Peer Type.................................... Internal
Minimum Advertisement Interval.............. 5 seconds
Neighbor AS Path Access List Out............. none
Neighbor Prefix List Out..................... none
Members Added................................ 3
Members Removed.............................. 0
Update Version............................... 4
Number of UPDATEs Sent....................... 8
Time Since Last UPDATE....................... 3 hrs 13 min 22 sec
Current Prefixes............................. 84
Current Paths................................ 2
```

```
Prefixes Advertised..................... 100
Prefixes Withdrawn...................... 16
UPDATE Send Failures.................... 0

Current Members:  172.24.3.1, 172.25.8.56, 172.28.9.1

Version   Delta T Duration UPD Built UPD Sent Paths Sent Pfxs Adv  Pfxs Wd
     10   00:00:49      100         6      288          5     1250      750
```

11.1.0.131 show ip bgp vpnv4

This command displays the VPNv4 address information from the BGP table. If an optional VRF is specified, the address information pertaining to that VRF is displayed.

Format `show ip bgp vpnv4 {all | rd` *`route-distinguisher`* `| vrf` *`vrf-name`*`} [`*`ip-prefix/length`*`]`

Mode Privileged EXEC

Parameter	Description
all	Displays the complete VPNv4 database.
rd route-distinguisher	Displays NLRI prefixes that match the named route distinguisher.
vrf vrf-name	Displays NLRI prefixes associated with the named VRF instance.
ip-prefix/length	IP address (in dotted decimal format) and the length of the mask (0 to 32). The slash (/) mark must be included.

The command outputs the following information, depending on the selected parameters.

Field	Description
BGP table version	Each time phase 2 of the BGP decision process runs to select new BGP routes, this number is incremented.
Status codes	One of the following: ■ s: The route is aggregated into an aggregate address configured with the summary-only option. ■ *: EFOS never displays invalid routes; so this code is always displayed (to maintain consistency with the industry standard). ■ >: Indicates that BGP has selected this path as the best path to the destination. ■ i: The route is learned from an internal peer.
Route Distinguisher	The RD associated with the VRF.
Network	Destination prefix
Next Hop	The route's BGP next hop.
Metric	BGP metric.
LocPrf	The local preference.
Path	The AS path per route.
Prefix/Prefix Length	The destination prefix and prefix length.
Generation ID	The version of the BGP routing table when this route last changed.
Forwarding	if this BGP route is used for forwarding.
Advertised To Update Groups	The outbound update groups to which this route is advertised.
Local Preference	The local preference, either as received from the peer or as set according to local policy.

Field	Description
AS Path	The AS Path. This form of the command displays AS Paths as long as allowed by **bgp maxas-limit**.
Origin	Value of the ORIGIN attribute.
Metric	Value of the MED attribute, if included.
Type	If the path is received from an internal or external peer.
IGP Cost	The interior gateway cost (e.g., OSPF cost) to the BGP NEXT HOP
Peer (Peer ID)	The IP address of the peer that sent this route, and its router ID.
BGP Next Hop	The BGP NEXT HOP attribute.
Atomic Aggregate	If the ATOMIC AGGEGATE attribute is attached to the path.
Aggregator	The AS number and router ID of the speaker that aggregated the route.
Communities	The BGP communities attached to the path.
Originator	If the ORIGINATOR attribute is attached to the path, the value of this attribute.
Cluster List	If the CLUSTER_LIST attribute is attached to the path, the sequence of cluster IDs in the cluster list.
Extended Community	Route target value associated with the specified route.

Example: The following example shows all available VPNv4 information in a BGP routing table:

```
(Routing) # show ip bgp vpnv4 all

BGP table version is 5, local router ID is 20.1.1.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network            Next Hop     Metric   LocPrf   Path
Route Distinguisher : 1:10 (for VRF red)
*> 172.20.1.0/24    100.10.1.1          10      100   20 10 i
*> 24.95.16.0/24    100.10.1.1          10      100   20 10 i
*> 24.14.8.0/24     100.10.1.1          10      100   20 10 i

Route Distinguisher : 2:20 (for VRF blue)
*> 173.20.1.0/24    120.10.1.1          10      100   20 10 i
*> 25.95.16.0/24    120.10.1.1          10      100   20 10 i
*> 25.14.8.0/24     120.10.1.1          10      100   20 10 i

Route Distinguisher : 3:30 (for VRF yellow)
*> 174.20.1.0/24    130.10.1.1          10      100   20 10 i
*> 26.95.16.0/24    130.10.1.1          10      100   20 10 i
*> 26.14.8.0/24     130.10.1.1          10      100   20 10 i
```

Example: The following example shows VPNv4 routing entries for VRF named *red*:

```
(Routing) # show ip bgp vpnv4 vrf red

BGP table version is 5, local router ID is 20.1.1.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network            Next Hop     Metric   LocPrf   Path
Route Distinguisher : 1:10 (for VRF red)
*> 172.20.1.0/24    100.10.1.1          10      100   20 10 i
*> 24.95.16.0/24    100.10.1.1          10      100   20 10 i
*> 24.14.8.0/24     100.10.1.1          10      100   20 10 i
```

Example: The following example shows the attributes for network 172.20.1.0 that include multi-paths and best path (Use like any of the below formats):

```
(Routing) # show ip bgp vpnv4 vrf red 172.20.1.0 255.255.255.0
(Routing) # show ip bgp vpnv4 vrf red 172.20.1.0/24

Prefix/Prefix Length..................... 1:100:172.20.1.0/24
Generation ID............................ 2056
Forwarding............................... Yes
Advertised to Update Groups.............. 1, 5

Best Path:
Imported from............................ 2:200:100.10.1.1
Local Preference......................... 100
AS Path.................................. 20 10
Origin................................... IGP
Metric................................... 10
Type..................................... External
IGP Cost................................. 30
Peer (Peer ID)........................... 100.10.1.1 (32.4.1.1)
BGP Next Hop............................. 100.10.1.1
Atomic Aggregate......................... Included
Aggregator (AS, Router ID)............... 300, 14.1.1.1
Communities.............................. no-export
Extended Community....................... RT:1:100
                                          RT:2:200
Originator.............................   10.1.1.1

Non-best Paths:
Local Preference......................... 200
AS Path.................................. 18 50 27
Origin................................... Incomplete
Type..................................... External
IGP Cost................................. 10
Peer (Peer ID)........................... 200.1.1.1 (18.24.1.3)
BGP Next Hop............................. 200.1.1.1
Extended Community....................... RT:3:300
```

11.1.0.132 show bgp l2vpn evpn summary

This command displays a summary of BGP configuration and status for L2VPN address family.

Format `show bgp l2vpn evpn summary`

Mode Privileged EXEC

Example:

```
(Routing) #show bgp l2vpn evpn summary

EVPN Control Plane ..................... Enable
BGP Admin Mode ......................... Enable
BGP Operational Mode ................... Enable
BGP Router ID .......................... 2.2.2.3
Local AS Number ........................ 100
Number of Network Entries .............. 10
```

```
Number of AS Paths ............................ 1
Dynamic Neighbors Current/High/Limit .......... 0/0/20
L2VPN EVPN config peers ....................... 1
L2VPN EVPN capable peers ...................... 1
Retain Route-target All ....................... Disable

Neighbor                ASN  MsgRcvd  MsgSent         State   Up/Down Time  Pfx Rcvd
3.3.3.4                 200       10       10            Up    00:00:20      100
```

Field	Description
EVPN Control Plane	Whether EVPN is globally enabled. BGP does not include the L2VPN EVPN AFI/SAFI capability in OPEN messages it sends unless evpn is globally enabled.
BGP Admin Mode	Whether BGP is globally enabled.
BGP Router ID	The configured router ID
Local AS Number	The router's AS number
Number of Network Entries	The number of distrinct L2VPN prefixes in the local RIB
Number of AS Paths	The number of AS paths in the local RIB
Dynamic Neighbors	Shows current number of created dynamic IPv4 BGP neighbors, high water mark and a limit of dynamic IPv4 BGP neighbors that can be created
L2VPN EVPN Config Peers	The number of peers are activated for l2vpn.
L2VPN EVPN Capable peers	The number of peers received L2VPN EVPN AFI/SAFI capability from the neighbors.
Neighbor	The IP address of a neighbor. A neighbor, that is created with BGP dynamic neighbors feature, will be marked with "*".
ASN	The neighbor's ASN
MsgRcvd	The number of BGP messages received from this neighbor
MsgSent	The number of BGP messages sent to this neighbor
State	The adjacency state. One of IDLE, CONNECT, ACTIVE, OPEN SENT, OPEN CNFRM, EST
Up/Down Time	How long the adjacency has been in the ESTABLISHED state, or, if the adjacency is down, how long it has been down. In days:hours:minutes:seconds
Pfx Rcvd	The number of L2VPN prefixes received from the neighbor

11.1.0.133 show bgp l2vpn evpn

To view the EVPN routes in the BGP routing table, use the `show bgp l2vpn evpn` command in Privileged EXEC mode. The output lists both best and non-best paths to each EVPN route. The route-type filter option shows it's specific type EVPN routes. By passing the IP address and prefixLen argument corresponding to the overlay end-host's IP, it displays the best and non-best paths for the end-host along with the Path attributes. This IP address and it's length argument is available only for Type-2 EVPN routes. By passing the specific Rd value, it displays the best and non-best paths for the end-host along with the Path attributes.

Format `show bgp l2vpn evpn [[route-type` *`type-1 - type-5`*`] `*`prefix/len`*` || [rd `*`rd-value`*`]]`

Mode Privileged EXEC

Example:

```
(Routing) #show bgp l2vpn evpn

BGP table version is 0, local router ID is 2.2.2.3
Status Codes: s suppressed, * valid, > best, i - internal, S - stale
Origin Codes: i - IGP, e - EGP, ? - incomplete
EVPN type-1 prefix: [1]:[ESI]:[EthTag]:[Label]
```

```
EVPN type-2 prefix: [2]:[ESI]:[EthTag]:[MAClen]:[MAC]:[IPlen]:[IP]
EVPN type-3 prefix: [3]:[EthTag]:[IPlen]:[OrigIP]
EVPN type-4 prefix: [4]:[ESI]:[IPlen]:[OrigIP]
EVPN type-5 prefix: [5]:[ESI]:[EthTag]:[IPlen]:[IP]:[GatewayIP]


    Network             Next Hop         Metric     LocPref Path
    ------------------- ---------------- ---------- ------- ----
    Route Distinguisher : 192.168.10.2:0
*>  [1]:[0:0x12340]:[0]:[0]
                        192.168.10.2                     100 200 i
*>  [4]:[0:0x0]:[32]:[192.168.10.2]
                        192.168.10.2                     100 200 i
*>  [4]:[0:0x12340]:[32]:[192.168.10.2]
                        192.168.10.2                     100 200 i
    Route Distinguisher : 192.168.10.2:10
*>  [2]:[0:0x0]:[1]:[48]:[00:00:00:01:02:03]:[32]:[11.11.11.1]
                        192.168.10.2                     100 200 i
*>  [3]:[1]:[32]:[192.168.10.2]
                        192.168.10.2                     100 200 i
    Route Distinguisher : 192.168.10.2:131
*>  [3]:[1]:[32]:[192.168.10.2]
                        192.168.10.2                     100 200 i
    Route Distinguisher : 192.168.30.2:0
*>  [4]:[0:0x0]:[32]:[192.168.30.2]
                        192.168.30.2                     100 200 i
```

Field	Description
Network	Destination EVPN route. It is displayed in the respective formats for EVPN type-2 or type-3 prefixes, as mentioned in the header of the command output.
Next Hop	The route's BGP NEXT HOP.
Metric	Multi Exit Descriminator
LocPref	The local preference
Path	The AS path The value of the ORIGIN attribute follows immediately after the AS PATH.

Example:

```
(Routing) #show bgp l2vpn evpn route-type type-2

BGP table version is 7, local router ID is 1.1.1.1
Status Codes: s suppressed, * valid, > best, i - internal, S - stale
Origin Codes: i - IGP, e - EGP, ? - incomplete
EVPN type-1 prefix: [1]:[ESI]:[EthTag]:[Label]
EVPN type-2 prefix: [2]:[ESI]:[EthTag]:[MAClen]:[MAC]:[IPlen]:[IP]
EVPN type-3 prefix: [3]:[EthTag]:[IPlen]:[OrigIP]
EVPN type-4 prefix: [4]:[ESI]:[IPlen]:[OrigIP]
EVPN type-5 prefix: [5]:[ESI]:[EthTag]:[IPlen]:[IP]:[GatewayIP]

    Network             Next Hop         Metric     LocPref Path
    ------------------- ---------------- ---------- ------- ----
    Route Distinguisher : 192.168.10.2:10
*>  [2]:[0:0x0]:[1]:[48]:[00:00:00:01:02:03]:[32]:[11.11.11.1]
                        192.168.10.2                     100 200 i
```

```
(Routing) #show bgp l2vpn evpn route-type 2 11.11.11.1/32

Route Distinguisher ..... 192.168.10.2:10
Route Table Entry .....
[2]:[0:0x0]:[1]:[48]:[00:00:00:01:02:03]:[32]:[11.11.11.1]
Generation ID ..... 1
Forwarding ..... No
Advertised to Update Groups ..... 0 1

Best Path:

Local Preference ..... 100
AS Path ..... 200
Origin ..... IGP
Type ..... External
IGP Cost ..... 0
Peer (Peer ID) ..... 192.168.10.2 (9.5.0.1)
BGP Next Hop ..... 192.168.10.2
Received Labels ..... 16
                      20
Extended Communities ..... RT:192.168.10.2:10

(Routing) #show bgp l2vpn evpn rd 192.168.10.2:10

Route Distinguisher ..... 192.168.10.2:10
Route Table Entry .....
[2]:[0:0x0]:[1]:[48]:[00:00:00:01:02:03]:[32]:[11.11.11.1]
Generation ID ..... 1
Forwarding ..... No
Advertised to Update Groups ..... 0 1

Best Path:

Local Preference ..... 100
AS Path ..... 200
Origin ..... IGP
Type ..... External
IGP Cost ..... 0
Peer (Peer ID) ..... 192.168.10.2 (9.5.0.1)
BGP Next Hop ..... 192.168.10.2
Received Labels ..... 16
                      20
Extended Communities ..... RT:192.168.10.2:10

Generation ID ..... 1
Forwarding ..... No
Advertised to Update Groups ..... None

------------------------------------------------------------------------------

Route Distinguisher ..... 192.168.10.2:10
Route Table Entry ..... [3]:[1]:[32]:[192.168.10.2]
Generation ID ..... 1
Forwarding ..... No
Advertised to Update Groups ..... 0 1

Best Path:
```

```
Local Preference ............................. 100
AS Path ...................................... 200
Origin ....................................... IGP
Type ......................................... External
IGP Cost ..................................... 0
Peer (Peer ID) ............................... 192.168.10.2 (9.5.0.1)
BGP Next Hop ................................. 192.168.10.2
Extended Communities ......................... RT:192.168.10.2:10
```

11.1.0.134 show bgp l2vpn evpn update-group

This command reports the status of L2VPN outbound update groups and their members.

Format `show bgp l2vpn evpn update-group [`*`group-index`* `|` *`peer-address`* `]`

Mode Privileged EXEC

Syntax	Description
group-index	(Optional) If specified, this option restricts the output to a single update group.
peer-address	(Optional) If specified, this option restricts the output to the update group containing the peer with the given IPv4 address.

Example: This command shows information for all update groups:

```
(localhost) #show bgp l2vpn evpn update-group

Update Group ................................. 0
Peer Type .................................... External
Minimum Advertisement Interval ............... 30 seconds
Send Community ............................... Yes
Send Extended Community ...................... Yes
Remove Private ASNs .......................... No
Route Reflector Client ....................... No
Neighbor AS Path Access List Out ............. none
Neighbor Prefix List Out ..................... none
Neighbor Route Map Out ....................... none
Members Added ................................ 2
Members Removed .............................. 0
Update Version ............................... 1
Number of UPDATES Sent ....................... 2
Time Since Last UPDATE ....................... 0 days 15 hrs 10 mins 10 secs
Current Prefixes ............................. 3
Current Paths ................................ 2
Prefixes Advertised .......................... 3
Prefixes Withdrawn ........................... 0
UPDATE Send Failures ......................... 0
Current Members: 192.168.20.2, 192.168.10.2

 Version  Delta T  Duration  UPD Built  UPD Sent  Paths Sent  Pfxs Adv  Pfxs Wd
      1 15:10:10         0          2         4           2         3        0
```

11.1.0.135 show bgp l2vpn evpn statistics

This command displays recent decision process history. Phase 1 of the decision process reacts to UPDATE messages received from peers, determining what new routes are accepted and deleting withdrawn routes from the Adj-RIB-In. Phase 2 determines the best path for each destination, updates the BGP route table, and updates the common RIB. Phase 3 is run independently for each outbound update group and determines which routes should be advertised to neighbors in each group. Each entry in the table shows statistics for one phase of the decision process. The table shows the 20 most recent decision process runs, with the most recent information at the end of the table.

Format `show bgp l2vpn evpn statistics`

Mode Privileged EXEC

Example:

```
(localhost) #show bgp l2vpn evpn statistics

Delta T Phase Upd Grp GenId   Reason          Peer  Duration  Adds  Mods  Dels
15:10:35   1             0  Adj-RIB-In+                0     3     0     0
15:10:33   2             1  Accept-RIB-In+             0     3     0     0
15:10:18   3       0     1  New update grp             1     3     0     0
```

11.1.0.136 show bgp l2vpn evpn route-reflection

This command shows the configuration of the local router as a route reflector. Output and field descriptions are the same as for IPv4 (see Section 11.1.0.125, show ip bgp route-reflection).

Format `show bgp l2vvpn evpn route-reflection`

Mode Privileged EXEC

11.1.0.137 show bgp ipv6

Use the **show bgp ipv6** command in Privileged EXEC mode to display IPv6 routes in the BGP routing table.

Format `show bgp ipv6 [`*`ipv6-prefix`*`|`*`prefix-length`* `[longer-prefixes | shorter-prefixes [`*`length`*`]] | filter-list `*`as-path-list`*`]`

Mode Privileged EXEC

Parameter	Description
ipv6-prefix prefix-length	(Optional) Limits the output to a specific prefix.
longer-prefixes	(Optional) Display the specified prefix and any longer prefixes within the same range.
shorter-prefixes	(Optional) Used with the **ipv6-prefix|prefix-length** option to show routes whose prefix length is shorter than **prefix-length** and, optionally, longer than a specified length. This option may not be given if the **longer-prefixes** option is given.
as-path-list	(Optional) Filter the output to the set of routes that match a given AS Path list. This option may not be given if an **ipv6-prefix|prefix-length** option is given.

The command output displays the following information.

Parameter	Description
BGP table version	Each time phase 2 of the BGP decision process runs to select new BGP routes, this number is incremented
Status codes	■ s – The route is aggregated into an aggregate address configured with the summary-only option ■ * – EFOS BGP never displays invalid routes; so this code is always displayed ■ > – Indicates that BGP has selected this path as the best path to the destination ■ i – If the route is learned from an internal peer
Network	IPv6 destination prefix
Next Hop	The IPv6 route's BGP NEXT HOP
Metric	Multi Exit Discriminator
LocPrf	The local preference
Path	The AS path
Origin	The value of the Origin attribute

Example: The following shows example CLI display output for the command.

```
(R1) # show bgp ipv6
BGP table version is 5, local router ID is 20.1.1.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network               Next Hop     Metric   LocPrf   Path
*> 2001:DB8::/48      3FFE:100::1        10      100   20 10  i
                      3FFE:200::4
*> 2001:DB8:4:5::/64  3FFE:100::1        10      100   20 10  ?
```

11.1.0.138 show bgp ipv6 aggregate-address

This command lists IPv6 aggregate addresses that have been configured and indicates whether each is currently active.

Format `show bgp ipv6 aggregate-address`

Mode Privileged EXEC

Parameter	Description
Prefix/Len	Destination prefix and prefix length.
AS Set	Indicates whether an empty AS path is advertised with the aggregate address (N) or an AS SET is advertised with the set of AS numbers for the paths contributing to the aggregate (Y).
Summary Only	Indicates whether the individual networks are suppressed (Y) or advertised (N).
Active	Indicates whether the aggregate is currently being advertised.

Example: The following shows example CLI display output for the command.

```
(R1) # show bgp ipv6 aggregate-address

Prefix/Len         AS Set    Summary Only    Active
----------------   ------    ------------    ------
2001:DB8::/48           N               Y         Y
3ffe:4000:1::/48        N               Y         Y
```

11.1.0.139 show bgp ipv6 community

This command displays IPv6 routes that belong to a given set of communities. The output format and field descriptions are the same as for the Section 11.1.0.137, show bgp ipv6 command.

Format `show bgp ipv6 community` *`communities`* `[exact-match]`
Mode Privileged EXEC

Parameter	Description
communities	A string of zero or more community values, which may be in either format and may contain the well-known community keywords no-advertise and no-export. The output displays routes that belong to every community specified in the command.
exact-match	(Optional) Only displays routes that are members of those and only those communities specified in the command.

11.1.0.140 show bgp ipv6 community-list

This command displays IPv6 routes that match a community list. The output format and field descriptions are the same as for the Section 11.1.0.137, show bgp ipv6 command.

Format `show bgp ipv6 community-list` *`name`* `[exact-match]`
Mode Privileged EXEC

Parameter	Description
name	A standard community list name.
exact-match	(Optional) Display only routes that are an exact match for the set of communities in the matching community list statement.

11.1.0.141 show bgp ipv6 listen range

This command displays information about BGP listen ranges.

Format `show bgp ipv6 listen range [`*`network/length`*`]`
Mode Privileged EXEC

Parameter	Description
listen range	Displays all listen subnet ranges that have been created.
network / length	Displays information about specified listen range.

Example:

```
(Routing) #show bgp ipv6 listen range

Listen Range ................................. 2001::1/64
Inherited Template ........................... template_2001

  Member                                  ASN       State
  --------------------------------------- ----- -----------
```

```
  2001::10                                65001 OPENCONFIRM
  2001::20                                    0      ACTIVE


Listen Range ................................ 2002::1/64
Inherited Template .......................... template_2002

  Member                                  ASN       State
  --------------------------------------- ----- -----------
```

11.1.0.142 show bgp ipv6 neighbors advertised-routes

This command displays IPv6 routes advertised to a specific neighbor. The format and field descriptions are the same as for the IPv4 command Section 11.1.0.122, show ip bgp neighbors advertised-routes except that the **Network** and **Next Hop** fields show IPv6 addresses and the command displays IPv4 routes advertised to a specific neighbor with RFC5549.

Format `show bgp ipv6 neighbors {`*`ipv4-address`* `|` *`ipv6-address`* `[interface` *`interface-name`*`] |autodetect interface` *`interface-name`*`} advertised-routes`

Mode Privileged EXEC

11.1.0.143 show bgp ipv6 neighbors routes

This command displays a list of IPv6 routes received from a specific neighbor. The list includes either all routes received from the neighbor, received routes that passed inbound policy, or routes rejected by inbound policy. The output and format as the same as for the IPv4 command Section 11.1.0.121, show ip bgp neighbors, except that they list IPv6 routes.

Format `show bgp ipv6 neighbors` *`ipv4-address`* `|` *`ipv6-address`* `{received-routes | routes | rejected-routes}`

Mode Privileged EXEC

11.1.0.144 show bgp ipv6 neighbors policy

This command displays the inbound and outbound IPv6 policies configured for a specific peer. The output distinguishes policies that are configured on the peer itself and policies that the peer inherits from a peer template.

Format `show bgp ipv6 neighbors [`*`ipv4-address`* `|` *`ipv6-address`* `[interface` *`interface-name`*`] | autodetect interface` *`interface-name`* `policy`

Mode Privileged EXEC

```
(Routing) #show bgp ipv6 neighbors fe80::1 interface 0/1 policy


Neighbor        Policy                                              Template
--------------- --------------------------------------------------- ---------------
fe80::1%0/1
                 activate
                 prefix-list jupiter in
                 prefix-list saturn out
                 maximum-prefix 2000
                 send-community
```

11.1.0.145 show bgp ipv6 route-reflection

This command shows the configuration of the local router as a route reflector.

Format `show bgp ipv6 route-reflection`

Mode Privileged EXEC

Parameter	Description
Cluster ID	The cluster ID used by this router. The value configured with the Section 11.1.0.15, bgp cluster-id command is displayed. If no cluster ID is configured, the local router ID is shown and tagged as default.
Client-to-client Reflection	Displays *Enabled* when this router reflects routes received from its clients to its other clients; otherwise *Disabled* displays.
Clients	A list of this router's internal peers that have been configured as route reflector clients.
Non-client Internal Peers	A list of this router's internal peers that are not configured as route reflector clients. Routes from non-client peers are reflected to clients and vice-versa.

Example: The following shows example CLI display output for the command.

```
(Routing) #show bgp ipv6 route-reflection

Cluster ID ..................................... 0.0.0.0 (default)
Client-to-client Reflection ................... Enabled
Clients:
Non-client Internal Peers:
```

11.1.0.146 show bgp ipv6 neighbors

This command displays a list of IPv6 routes received from a specific neighbor. The list includes either all routes received from the neighbor, received routes that passed inbound policy, or routes rejected by inbound policy. The output and format as the same as for the IPv4 command Section 11.1.0.121, show ip bgp neighbors, except:

- IPv6 routes are listed
- If the peer address ("Remote Address") is a link local address, the next line of output indicates the scope of the address.
- No "IPv4 Outbound Update Group" is listed.
- No IPv4 prefix statistics are shown.
- RFC 5549 Support is displayed only if the BGP neighbor is peered over IPv6 network.
- If the peer is configured as "autodetect", the "Remote Address" shows detected IPv6 address or "Unresolved" in case if the peer is not detected by the autodetect feature.
- Autodetect status" is displayed only if the peer is configured as "autodetect". The field shows one of the following statuses: "Peer is detected", "Peer is not detected" or "Multiple peers are detected".

Format `show bgp ipv6 neighbors [`*`ipv4-address`* `|` *`ipv6-address`* `[interface` *`interface-name`*`] | autodetect interface` *`interface-name`* `{received-routes | routes | rejected-routes}`

Mode Privileged EXEC

```
(Routing) # show bgp ipv6 neighbors fe80::2

Description: spine 1 router 1

Remote Address ............................... fe80::2
```

```
Autodetect status ............................. Peer is detected
Interface...................................... 0/1
Remote AS ..................................... 100
Peer ID ....................................... 14.3.0.1
Peer Admin Status ............................. START
Peer State .................................... ESTABLISHED
Peer Type ..................................... DYNAMIC
Listen Range .................................. 2001::1/64
Local Port .................................... 179
Remote Port ................................... 58265
Connection Retry Interval ..................... 120 sec
Neighbor Capabilities ......................... None
IPv4 Unicast Support .......................... None
IPv6 Unicast Support .......................... Both
Graceful Restart Support....................... Enabled
Graceful Restart Helper Support................ Enabled
RFC 5549 Support .............................. Enable
Update Source.................................. None
Local Interface Address ....................... fe80::2
Configured Hold Time .......................... 90 sec
Configured Keep Alive Time..................... 30 sec
Negotiated Hold Time .......................... 30 sec
Keep Alive Time ............................... 10 sec
MD5 Password................................... password

Last Error (Sent).............................. Hold Timer Expired
Last SubError.................................. None
Time Since Last Error.......................... 0 day 0 hr 4 min 27 sec
Established Transitions ....................... 1
Established Time .............................. 0 day 0 hr 4 min 25 sec
Time Since Last Update ........................ 0 day 0 hr 4 min 24 sec
IPv6 Outbound Update Group..................... 7


             Open   Update   Keepalive   Notification   Refresh   Total
Msgs Sent       1        0          10              0         0      11
Msgs Rcvd       1        1          11              0         0      12

Received UPDATE Queue Size:  0 bytes. High: 355. Limit 196096. Drops 0.

IPv6 Prefix Statistics:
                          Inbound       Outbound
Prefixes Advertised             1              0
Prefixes Withdrawn              0              0
Prefixes Current                1              0
Prefixes Accepted1 N/A
Prefixes Rejected               1            N/A
Max NLRI per Update             1              0
Min NLRI per Update             1              0
```

11.1.0.147 show bgp ipv6 statistics

This command shows statistics for the IPv6 decision process. Output and field descriptions are the same as for the IPv4 command Section 11.1.0.126, show ip bgp statistics.

Format `show bgp ipv6 statistics`

Mode Privileged EXEC

11.1.0.148 show bgp ipv6 summary

This command displays a summary of BGP IPv6 configuration and status. The output and field descriptions are the same as for the Section 11.1.0.127, show ip bgp summary command, except that **Number of Network Entries**, **Number of AS Paths**, and **Pfx Rcvd** all count IPv6 rather than IPv4 routing information. The command lists all adjacencies that are configured to carry IPv6 routes.

Format `show bgp ipv6 summary`

Mode Privileged EXEC

11.1.0.149 show bgp ipv6 update-group

This command reports the status of IPv6 outbound update groups and their numbers. Output and format are the same as for Section 11.1.0.130, show ip bgp update-group.

Format `show bgp ipv6 update-group [`*`group-index`* `|` *`ipv4-address`* `|` *`ipv6-address`* `[interface` *`interface-name`*`] autodetect interface` *`interface-name`*

Mode Privileged EXEC

Parameter	Description
group-index	(Optional) If specified, this option restricts the output to a single update group.
ipv4-address	The IPv4 address of a peer enabled for the exchange of IPv6 prefixes. If specified, this option restricts the output to the update group containing the peer with the given address.
ipv6-address	The IPv6 address of a peer. If the peer address is a link local address, the interface that defines the scope of the address must also be given. If a peer address is specified, this option restricts the output to the update group containing the peer with the given address.
autodetect interface	The routing interface on which the neighbor's link local IPv6 address is auto detected.

11.1.0.150 snapshot bgp

Use the snapshot bgp command in Support mode to dump a set of BGP debug information to capture the current state of BGP.

Format `snapshot bgp`

Mode Support mode

11.2 BGP Routing Policy Commands

Exterior routing protocols like BGP use industry-standard routing policy to filter and modify routing information exchanged with peers. BGP makes use of the following routing policy constructs:

- AS Path Access Lists
- BGP Community Lists

Use the Routing Policy commands to configure routing policies such as:

- Matching on an AS Path
- Modifying the AS Path
- Setting the local preference
- Setting the route metric
- Setting an IPv6 next hop
- Setting or matching on a BGP community

11.2.0.1 ip as-path access-list

To create an AS path access list, use the **ip as-path access-list** command in Global Configuration mode. An AS path access list filters BGP routes on the AS path attribute of a BGP route. The AS path attribute is a list of the autonomous system numbers along the path to the destination. An AS path access list is an ordered sequence of statements. Each statement specifies a regular expression and a permit or deny action. If the regular expression matches the AS path of the route expressed as an ASCII string, the route is considered a match and the statement's action is taken. An AS path list has an implicit deny statement at the end. If a path does not match any of the statements in an AS path list, the action is considered to be deny.

Once you have created an AS path list, you cannot delete an individual statement. If you want to remove an individual statement, you must delete the AS path list and recreate it without the statement to be deleted.

Statements are applied in the order in which they are created. New statements are added to the end of the list. The statement with the first matching regular expression is applied.

EFOS allows configuration of up to 128 AS path access lists, with up to 64 statements each.

To enter the question mark within a regular expression, you must first enter **CTRL-V** to prevent the CLI from interpreting the question mark as a request for help.

Table 16, AS Path Regular Expression Syntax lists AS path list regular expression syntax.

Default No AS path lists are configured by default. There are no default values for any of the parameters of this command.

Format `ip as-path access-list` *`as-path-list-number`* `{permit|deny}` *`regexp`*

Mode Global Configuration

Parameter	Description
as-path-list-number	A number from 1 to 500 uniquely identifying the list. All AS path access list commands with the same *as-path-list-number* are considered part of the same list.
permit	(Optional) Permit routes whose AS Path attribute matches the regular expression.
deny	(Optional) Deny routes whose AS Path attribute matches the regular expression.

Parameter	Description
regexp	A regular expression used to match the AS path attribute of a BGP path where the AS path is treated as an ASCII string.

Table 16: AS Path Regular Expression Syntax

Special Character	Symbol	Behavior
asterisk	*	Matches zero or more sequences of the pattern.
brackets	[]	Designates a range of single-character patterns.
caret	^	Matches the beginning of the input string.
dollar sign	$	Matches the end of the input string.
hyphen	–	Separates the end points of a range.
period	.	Matches any single character, including white space.
plus sign	–	Matches 1 or more sequences of the pattern.
question mark	?	Matches 0 or 1 occurrences of the pattern.
underscore	_	Matches a comma (,), left brace ({), right brace (}), left parenthesis, right parenthesis, the beginning of the input string, the end of the input string, or a space.

Example: In the following example, the router is configured to reject routes received from neighbor 172.20.1.1 with an AS path that indicates the route originates in, or passes through, AS 100.

```
(Routing)(Config)# ip as-path access-list 1 deny _100_
(Routing)(Config)# ip as-path access-list 1 deny ^100$
(Routing)(Config)# router bgp 1
(Routing)(Config-router)# neighbor 172.20.1.1 remote-as 200
(Routing)(Config-router)# neighbor 172.20.1.1 filter-list 1 in
```

11.2.0.1.1 no ip as-path access-list

To delete an AS path access list, use the **no** form of this command.

Format `no ip as-path access-list` *`as-path-list-number`*
Mode Global Configuration

11.2.0.2 ip bgp-community new-format

To display BGP standard communities in AA:NN format, use the **ip bgp-community new-format** command in Global Configuration mode. RFC 1997 specifies that the first two bytes of a community number are considered to be an autonomous system number. The new format displays a community number as the ASN followed by a 16-bit AS-specific number.

Default Standard communities are displayed in AA:NN format.
Format `ip bgp-community new-format`
Mode Global Configuration

11.2.0.2.1 no ip bgp-community new-format

To display BGP standard communities as 32-bit integers, use the **no** form of this command.

Format `no ip bgp-community new-format`
Mode Global Configuration

11.2.0.3 ip community-list

To create or configure a BGP community list, use the **ip community-list** command in Global Configuration mode. A community list statement with no community values is considered a match for all routes, regardless of their community membership. So the statement **ip community-list bullseye permit** is a *permit all* statement.

A community number may be entered in either format, as a 32-bit integer or a pair of 16-bit integers separated by a colon, regardless of whether the Section 11.2.0.2, ip bgp-community new-format command is active. Up to 16 communities, including the well-known communities, can be listed in a single command. Up to 32 statements may be configured with a given community list name. Up to 128 unique community list names may be configured.

Default No community lists are configured by default.
Format `ip community-list standard` ***`list-name`*** `{permit | deny} [`***`community-number`***`] [no-advertise] [no-export]`
Mode Global Configuration

Parameter	Description
standard list-name	Identifies a named standard community list. The name may contain up to 32 characters.
permit	Indicates that matching routes are permitted.
deny	Indicates that matching routes are denied.
community-number	From zero to 16 community numbers formatted as a 32-bit integers or in AA:NN format, where AA is a 2-byte autonomous system number and NN is a 16 bit integer. The range is 1 to 4,294,967,295 (any 32-bit integer other than 0). Communities are separated by spaces.
no-advertise	The well-known standard community, NO_ADVERTISE (0xFFFFFF02).
no-export	The well-known standard community, NO_EXPORT, (0xFFFFFF01).

11.2.0.3.1 no ip community-list

To delete a community list, use the **no** form of the command.

Format `no ip community-list standard` ***`list-name`***
Mode Global Configuration

11.2.0.4 ip prefix-list

To create a prefix list or add a prefix list entry, use the ip prefix-list command in Global Configuration mode. Prefix lists allow matching of route prefixes with those specified in the prefix list. Each prefix list includes of a sequence of prefix list entries ordered by their sequence numbers. A router sequentially examines each prefix list entry to determine if the route's prefix matches that of the entry. An empty or nonexistent prefix list permits all prefixes. An implicit deny is assume if a given prefix does not match any entries of a prefix list. Once a match or deny occurs the router does not go through the rest of the list. A prefix list may be used within a route map to match a route's prefix using the Section 11.2.0.9, match ip address command.

Up to 128 prefix lists may be configured. The maximum number of statements allowed in prefix list is 64.

Default No prefix lists are configured by default. When neither the **ge** nor the **le** option is configured, the destination prefix must match the network/length exactly. If the **ge** option is configured without the **le** option, any prefix with a network mask greater than or equal to the **ge** value is considered a match. Similarly, if the **le** option is configured without the **ge** option, a prefix with a network mask less than or equal to the **le** value is considered a match.

Format `ip prefix-list list-name {[seq number] {permit | deny} network/length [ge length] [le length] | renumber renumber-interval first-statement-number}`

Mode Global Configuration

Parameter	Description
list-name	The text name of the prefix list. Up to 32 characters.
seq number	(Optional) The sequence number for this prefix list statement. Prefix list statements are ordered from lowest sequence number to highest and applied in that order. If you do not specify a sequence number, the system will automatically select a sequence number five larger than the last sequence number in the list. Two statements may not be configured with the same sequence number. The value ranges from 1 to 4,294,967,294.
permit	Permit routes whose destination prefix matches the statement.
deny	Deny routes whose destination prefix matches the statement.
network/length	Specifies the match criteria for routes being compared to the prefix list statement. The network can be any valid IP prefix. The length is any IPv4 prefix length from 0 to 32.
ge length	(Optional) If this option is configured, then a prefix is only considered a match if its network mask length is greater than or equal to this value. This value must be longer than the network length and less than or equal to 32.
le length	(Optional) If this option is configured, then a prefix is only considered a match if its network mask length is less than or equal to this value. This value must be longer than the **ge** length and less than or equal to 32.
renumber	(Optional) Provides the option to renumber the sequence numbers of the IP prefix list statements with a given interval starting from a particular sequence number. The valid range for *renumber-interval* is 1–100, and the valid range for *first-statement-number* is 1–1000.

Example: The following example configures a prefix list that allows routes with one of two specific destination prefixes, 172.20.0.0/16 and 192.168.1.0/24:

```
(Routing)(config)# ip prefix-list apple seq 10 permit 172.20.0.0/16
(Routing)(config)# ip prefix-list apple seq 20 permit 192.168.10/24
```

Example: The following example disallows only the default route.

```
(Routing)(config)# ip prefix-list orange deny 0.0.0.0/0
(Routing)(config)# ip prefix-list orange permit 0.0.0.0/0 ge 1
```

11.2.0.4.1 no ip prefix-list

To delete a prefix list or a statement in a prefix list, use the **no** form of this command. The command **no ip prefix-list list-name** deletes the entire prefix list. To remove an individual statement from a prefix list, you must specify the statement exactly, with all its options.

Format `no ip prefix-list list-name [seq number] {permit | deny} network/length [ge length] [le length]`

Mode Global Configuration

11.2.0.5 ip prefix-list description

To apply a text description to a prefix list, use the **ip prefix-list description** command in Global Configuration mode.

Default No description is configured by default.

Format `ip prefix-list` *`list-name`* `description` *`text`*

Mode Global Configuration

Parameter	Description
list-name	The text name of the prefix list.
description text	Text description of the prefix list. Up to 80 characters.

11.2.0.5.1 no ip prefix-list description

To remove the text description, use the **no** form of this command.

Format `no ip prefix-list` *`list-name`* `description`

Mode Global Configuration

11.2.0.6 ipv6 prefix-list

Use this command to create IPv6 prefix lists. An IPv6 prefix list can contain only ipv6 addresses. Prefix lists allow matching of route prefixes with those specified in the prefix list. Each prefix list includes of a sequence of prefix list entries ordered by their sequence numbers. A router sequentially examines each prefix list entry to determine if the route's prefix matches that of the entry. For IPv6 routes, only IPv6 prefix lists are matched. An empty or nonexistent prefix list permits all prefixes. An implicit deny is assumed if a given prefix does not match any entries of a prefix list. Once a match or deny occurs the router does not go through the rest of the list. An IPv6 prefix list may be used within a route map to match a route's prefix using the `match ipv6 address` command. A route map may contain both IPv4 and IPv4 prefix lists. If a route being matched is an IPv6 route, only the IPv6 prefix lists are matched.

Up to 128 prefix lists may be configured. The maximum number of statements allowed in prefix list is 64. These numbers indicate only IPv6 prefix lists. IPv4 prefix lists may be configured in appropriate numbers independently.

Default No prefix lists are configured by default. When neither the **ge** nor the **le** option is configured, the destination prefix must match the network/length exactly. If the **ge** option is configured without the **le** option, any prefix with a network mask greater than or equal to the **ge** value is considered a match. Similarly, if the **le** option is configured without the **ge** option, a prefix with a network mask less than or equal to the **le** value is considered a match.

Format `ipv6 prefix-list` *`list-name`* `[seq` *`seq-number`*`] { {permit/deny}` *`ipv6-prefix/prefix-length`* `[ge` *`ge-value`*`] [le` *`le-value`*`] | description` *`text`* `| renumber` *`renumber-interval first-statement-number`*`}`

Mode Global Configuration

Parameter	Description
list-name	The text name of the prefix list. Up to 32 characters.

Parameter	Description
seq number	(Optional) The sequence number for this prefix list statement. Prefix list statements are ordered from lowest sequence number to highest and applied in that order. If you do not specify a sequence number, the system will automatically select a sequence number five larger than the last sequence number in the list. Two statements may not be configured with the same sequence number. The value ranges from 1 to 4,294,967,294.
permit	Permit routes whose destination prefix matches the statement.
deny	Deny routes whose destination prefix matches the statement.
ipv6-prefix/prefix-length	Specifies the match criteria for routes being compared to the prefix list statement. The ipv6-prefix can be any valid IPv6 prefix where the address is specified in hexadecimal using 16-bit values between colons. The prefix-length is the The length of the IPv6 prefix, given as a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
ge length	(Optional) If this option is configured, specifies a prefix length greater than or equal to the ipv6-prefix/prefix-length. It is the lowest value of a range of the length.
le length	(Optional) If this option is configured, specifies a prefix length less than or equal to the **ipv6-**prefix/prefix-length. It is the highest value of a range of the length.
Description	A description of the prefix list. It can be up to 80 characters in length.
renumber	(Optional) Provides the option to renumber the sequence numbers of the IPv6 prefix list statements with a given interval starting from a particular sequence number.

Example: The following example configures a prefix list that allows routes with one of two specific destination prefixes, `2001::/64 and 5F00::/48`:

```
(R1)(config)# ipv6 prefix-list apple seq 10 permit 2001::/64
(R1)(config)# ipv6 prefix-list apple seq 20 permit 5F00::/48
```

11.2.0.6.1 no ipv6 prefix-list

Use this command to deletes either the entire prefix list or an individual statement from a prefix list.

Format `ipv6 prefix-list` *`list-name`*
Mode Global Configuration

NOTE: The description must be removed using the `no ip prefix-list description` before using this command to delete an IPv6 Prefix List.

11.2.0.7 match as-path

This route map match term matches BGP autonomous system paths against an AS path access list. If you enter a new **match as-path** term in a route map statement that already has a **match as-path** term, the AS path list numbers in the new term are added to the existing match term, up to the maximum number of lists in a term. A route is considered a match if it matches any one or more of the AS path access lists the match term refers to.

Format `match as-path` *`as-path-list-number`*
Mode Route Map Configuration

Parameter	Description
as-path-list-number	An integer from 1 to 500 identifying the AS path access list to use as match criteria.

11.2.0.7.1 no match as-path

This command deletes the match as-path term that matches BGP autonomous system paths against an AS path access list.

Format `no match as-path` *`as-path-list-number`*
Mode Route Map Configuration

11.2.0.8 match community

To configure a route map to match based on a BGP community list, use the **match community** command in Route Map Configuration mode. If the community list returns a **permit** action, the route is considered a match. If the match statement refers to a community list that is not configured, no routes are considered to match the statement.

Format `match community` *`community-list`* `[`*`community-list...`*`] [exact-match]`
Mode Route Map Configuration

Parameter	Description
community-list	The name of a standard community list. Up to eight names may be included in a single match term.
exact-match	(Optional) When this option is given, a route is only considered a match if the set of communities on the route is an exact match for the set of communities in one of the statements in the community list.

11.2.0.8.1 no match community

To delete a match term from a route map, use the **no** form of this command. The command **no match community list exact-match** removes the match statement from the route map. (It does not simply remove the exact-match option.) The command **no match community** removes the match term and all its community lists.

Format `no match community` *`community-list`* `[`*`community-list...`*`] [exact-match]`
Mode Route Map Configuration

11.2.0.9 match ip address

To configure a route map to match based on a destination prefix, use the **match ip address** command in Route Map Configuration mode. If you specify multiple prefix lists in one statement, then a match occurs if a prefix matches any one of the prefix lists. If you configure a match ip address statement within a route map section that already has a match ip address statement, the new prefix lists are added to the existing set of prefix lists, and a match occurs if any prefix list in the combined set matches the prefix.

Default No match criteria are defined by default.
Format `match ip address prefix-list` *`prefix-list-name`* `[`*`prefix-list-name...`*`]`
Mode Route Map Configuration

Parameter	Description
prefix-list-name	The name of a prefix list used to identify the set of matching routes. Up to eight prefix lists may be specified.

11.2.0.9.1 no match ip address

To delete a match statement from a route map, use the **no** form of this command.

Format `no match ip address [prefix-list` *`prefix-list-name`* `[`*`prefix-list-name...`*`]]`
Mode Route Map Configuration

11.2.0.10 set as-path

To prepend one or more AS numbers to the AS path in a BGP route, use the set as-path command in Route Map Configuration mode. This command is normally used to insert one or more instances of the local AS number at the beginning of the AS_PATH attribute of a BGP route. Doing so increases the AS path length of the route. The AS path length has a strong influence on BGP route selection. Changing the AS path length can influence route selection on the local router or on routers to which the route is advertised.

When prepending an inbound route, if the first segment in the AS_PATH of the received route is an AS_SEQUENCE, *as-path-string* is inserted at the beginning of the sequence. If the first segment is an AS_SET, *as-path-string* is added as a new segment with type AS_SEQUENCE at the beginning of the AS path. When prepending an outbound route to an external peer, *as-path-string* follows the local AS number, which is always the first ASN.

Format `set as-path prepend` *`as-path-string`*
Mode Route Map Configuration

Parameter	Description
as-path-string	A list of AS path numbers to insert at the beginning of the AS_PATH attribute of matching BGP routes. To prepend more than one AS number, separate the ASNs with a space and enclose the string in quotes. Up to ten AS numbers may be prepended.

Example: The following example prepends three instances an external peer's AS number to paths received from that peer, making routes learned from this peer less likely to be chosen as the best path.

```
(Routing)# config
(Routing)# route-map ppAsPath
(Routing)# set as-path prepend "2 2 2"
(Routing)# exit
(Routing)# router bgp 1
(Routing)# neighbor 172.20.1.2 remote-as 2
(Routing)# neighbor 172.20.1.2 route-map ppAsPath in
```

11.2.0.10.1 no set as-path

To remove a set command from a route map, use the **no** form of this command.

Format `no set as-path prepend` *`as-path-string`*
Mode Route Map Configuration

11.2.0.11 set comm-list delete

To remove BGP communities from an inbound or outbound UPDATE message, use the **set comm-list delete** command in Route Map Configuration mode. A route map with this **set** command can be used to remove selected communities from inbound and outbound routes. When a community list is applied to a route for this purpose, each of the route's communities is submitted to the community list one at a time. Communities permitted by the list are removed from the route. Because communities are processed individually, a community list used to remove communities should not include the exact-match option on statements with multiple communities. Such statements can never match an individual community.

When a route map statement includes both **set** community and **set comm-list delete** terms, the **set comm-list delete** term is processed first, and then the **set** community term (meaning that, communities are first removed, and then communities are added).

Format `set comm-list` *`community-list-name`* `delete`
Mode Route Map Configuration

Parameter	Description
community-list-name	A standard community list name.

11.2.0.11.1 no set comm-list

To delete the set command from a route map, use the **no** form of this command.

Format `no set comm-list`
Mode Route Map Configuration

11.2.0.12 set community

To modify the communities attribute of matching routes, use the **set community** command in Route Map Configuration mode. The **set community** command can be used to assign communities to routes originated through BGP's network and redistribute commands, and to set communities on routes received from a specific neighbor or advertised to a specific neighbor. It can also be used to remove all communities from a route.To remove a subset of the communities on a route, use the command Section 11.2.0.11, set comm-list delete.

Format `set community {`*`community-number`* `[additive] | none}`
Mode Route Map Configuration

Parameter	Description
community-number	One to sixteen community numbers, either as a 32-bit integers or in AA:NN format. Communities are separated by spaces. The well-known communities **no advertise** and **no-export** are also accepted.
additive	(Optional) Communities are added to those already attached to the route.
none	(Optional) Removes all communities from matching routes.

11.2.0.12.1 no set community

To remove a set term from a route map, use the **no** form of this command.

Format `no set community`
Mode Route Map Configuration

11.2.0.13 set local-preference

To set the local preference of specific BGP routes, use the **set local-preference** command in Route Map Configuration mode. The local preference is the first attribute used to compare BGP routes. Setting the local preference can influence which route BGP selects as the best route. When used in conjunction with a Section 11.2.0.7, match as-path or Section 11.2.0.9, match ip address command, this command can be used to prefer routes that transit certain ASs or to make the local router a more preferred exit point to certain destinations.

Format `set local-preference` *`value`*
Mode Route Map Configuration

Parameter	Description
value	A local preference value, from 0 to 4,294,967,295 (any 32-bit integer).

11.2.0.13.1 no set local-preference

To remove a set command from a route map, use the **no** form of this command.

Format `no set local-preference` *`value`*
Mode Route Map Configuration

11.2.0.14 set metric (BGP)

To set the metric of a route, use the **set metric** command in Route Map Configuration mode. This command sets the Multi Exit Discriminator (MED) when used in a BGP context. When there are multiple peering points between two autonomous systems (AS), setting the MED on routes advertised by one router can influence the other AS to send traffic through a specific peer.

Format `set metric` *`value`*
Mode Route Map Configuration

Parameter	Description
value	A metric value, from 0 to 4,294,967,295 (any 32-bit integer).

11.2.0.14.1 no set metric (BGP)

To remove a **set** command from a route map, use the **no** form of this command.

Format `no set metric` *`value`*
Mode Route Map Configuration

11.2.0.15 set ipv6 next-hop (BGP)

To set the IPv6 next hop of a route, use the **set ipv6 next-hop** command in Route Map Configuration mode. When used in a route map applied to UPDATE messages received from a neighbor, the command sets the next hop address for matching IPv6 routes received from the neighbor.

When used in a route map applied to UPDATE messages sent to a neighbor, the command sets the next hop address for matching IPv6 routes sent to the neighbor. If the address is a link local address, the address is assumed to be on the interface where the UPDATE is sent or received. If the command specifies a global IPv6 address, the address is not required to be on a local subnet.

Format set ipv6 next-hop *ipv6-address*

Mode Route Map Configuration

Parameter	Description
ipv6-address	The IPv6 address set as the Network Address of Next Hop field in the MP_NLRI attribute of an UPDATE message.

11.2.0.15.1 no set ipv6 next-hop (BGP)

To remove a **set** command from a route map, use the **no** form of this command.

Format no set ipv6 next-hop

Mode Route Map Configuration

11.2.0.16 show ip as-path-access-list

This command displays the contents of AS path access lists.

Format show ip as-path-access-list [*as-path-list-number*]

Mode Privileged EXEC

Parameter	Description
as-path-list-number	(Optional) When an AS path list number is specified, the output is limited to the single AS path list specified. The number is an integer from 1 to 500.

Example: The following shows example CLI display output for the command.

```
(Routing)# show ip as-path-access-list

AS path access list 1
   deny _100_
   deny ^100$

AS path access list 2
   deny _200_
   deny ^200$
```

11.2.0.17 show ip community-list

This command displays community lists. The format of community values is dictated by the Section 11.2.0.2, ip bgp-community new-format command.

Format show ip community-list [*community-list-name*]

Mode Privileged EXEC

Parameter	Description
community-list-name	(Optional) A standard community list name. This option limits the output to a single list.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip community-list

Standard community list buzz
     permit 100:200
     permit 100:300
     permit 100:400
Standard community list woody
    permit 200:1
    permit 200:2
    permit 200:3
```

11.2.0.18 clear ip community-list

This command clears community lists.

Format clear ip community-list [*community-list-name*]

Mode Privileged EXEC

Parameter	Description
community-list-name	(Optional) A community list name.

11.2.0.19 show ip prefix-list

This command displays configuration and status for a prefix list.

Format `show ip prefix-list [detail | summary] prefix-list-name [network/length] [seq sequence-number] [longer] [first-match]`

Mode Privileged EXEC

Parameter	Description
detail | summary	(Optional) Displays detailed or summarized information about all prefix lists.
prefix-list-name	(Optional) The name of a specific prefix list.
network/length	(Optional) The network number and length (in bits) of the network mask.
seq	(Optional) Applies the sequence number to the prefix list entry.

Parameter	Description
sequence-number	(Optional) The sequence number of the prefix list entry.
longer	(Optional) Displays all entries of a prefix list that are more specific than the given network/length.
first-match	(Optional) Displays the entry of a prefix list that matches the given network/length.

Acceptable forms of this command are as follows:

```
show ip prefix-list prefix-list-name network/length first-match
show ip prefix-list prefix-list-name network/length longer
show ip prefix-list prefix-list-name network/length
show ip prefix-list prefix-list-name seq sequence-number
show ip prefix-list prefix-list-name
show ip prefix-list summary
show ip prefix-list summary prefix-list-name
show ip prefix-list detail
show ip prefix-list detail prefix-list-name
```

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip prefix-list fred

ip prefix-list fred:
   count: 3, range entries: 3, sequences: 5 - 15, refcount: 0
   seq 5 permit 10.10.1.1/20 ge 22
   seq 10 permit 10.10.1.2/20 le 30
   seq 15 permit 10.10.1.2/20 ge 29 le 30
```

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip prefix-list summary fred

ip prefix-list fred:
   count: 3, range entries: 3, sequences: 5 - 15, refcount: 0
```

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip prefix-list detail fred

ip prefix-list fred:
   count: 3, range entries: 3, sequences: 5 - 15, refcount: 0
   seq 5 permit 10.10.1.1/20 ge 22 (hitcount: 0)
   seq 10 permit 10.10.1.2/20 le 30 (hitcount: 0)
   seq 15 permit 10.10.1.2/20 ge 29 le 30 (hitcount: 0)
```

11.2.0.20 clear ip prefix-list

To reset IP prefix-list counters, use the **clear ip prefix-list** command in Privileged EXEC mode. This command is used to clear prefix-list hit counters. The hit count is a value indicating the number of matches to a specific prefix list entry.

Format `clear ip prefix-list [[prefix-list-name] [network/length]]`

Mode Privileged EXEC

Parameter	Description
prefix-list-name	(Optional) Name of the prefix list from which the hit count is to be cleared.
network/length	(Optional) Network number and length (in bits) of the network mask. If this option is specified, hit counters are only cleared for the matching statement.

Example: The following shows an example of the command.

```
(Routing) # clear ip prefix-list orange 20.0.0.0/8
```

11.2.0.21 show ipv6 prefix-list

This command displays configuration and status for a selected prefix list.

Format `show ipv6 prefix-list [detail | summary] listname [ipv6-prefix/prefix-length] [seq 1-4294967294] [longer] [first-match]`

Mode Privileged EXEC

Parameter	Description
detail | summary	(Optional) Displays detailed or summarized information about all prefix lists.
list-name	(Optional) The name of a specific prefix list.
ipv6-prefix/prefix-length	(Optional) The network number and length (in bits) of the network mask.
seq	(Optional) Applies the sequence number to the prefix list entry.
sequence-number	(Optional) The sequence number of the prefix list entry.
longer	(Optional) Displays all entries of a prefix list that are more specific than the given network/length.
first-match	(Optional) Displays the entry of a prefix list that matches the given network/length.

Acceptable forms of this command are as follows:

```
show ipv6 prefix-list listname ipv6-prefix/prefix-length first-match
show ipv6 prefix-list listname ipv6-prefix/prefix-length longer
show ipv6 prefix-list listname ipv6-prefix/prefix-length
show ipv6 prefix-list listname seq sequence-number
show ipv6 prefix-list listname
show ipv6 prefix-list summary
show ipv6 prefix-list summary prefix-list-name
show ipv6 prefix-list detail
show ipv6 prefix-list detail prefix-list-name
```

The command outputs the following information.

Parameter	Description
count	Number of entries in the prefix list.
range entries	Number of entries that match the input range.
ref count	Number of entries referencing the given prefix list.
seq	Sequence number of the entry in the list.
permit/deny	The action to take.
sequences	Range of sequence numbers for the entries in the list
hit count	Number of matches for the prefix entry

Example: The following shows example CLI display output for the command.

```
(Switch) #show ipv6 prefix-list apple
ipv6 prefix-list apple:
count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
seq 5 deny 5F00::/8 le 128
seq 10 deny ::/0
seq 15 deny ::/1
```

```
seq 20 deny ::/2
seq 25 deny ::/3 ge 4
       seq 30 permit ::/0 le 128

(Switch) #show ipv6 prefix-list summary apple
ipv6 prefix-list apple:
count: 6, range entries: 3, sequences: 5 - 30, refcount: 31

(Switch) #show ipv6 prefix-list detail apple
ipv6 prefix-list apple:
count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
seq 5 deny 5F00::/8 le 128 (hit count: 0, refcount: 1)
seq 10 deny ::/0 (hit count: 0, refcount: 1)
seq 15 deny ::/1 (hit count: 0, refcount: 1)
seq 20 deny ::/2 (hit count: 0, refcount: 1)
seq 25 deny ::/3 ge 4 (hit count: 0, refcount: 1)
       seq 30 permit ::/0 le 128 (hit count: 240664, refcount: 0)
```

11.2.0.22 clear ipv6 prefix-list

Use this command to reset and clear IPv6 prefix-list hit counters. The hit count is a value indicating the number of matches to a specific prefix list entry.

Format clear ipv6 prefix-list [*prefix-list-name*] [ipv6-prefix/*prefix-length*]

Mode Privileged EXEC

Parameter	Description
list-name	(Optional) Name of the prefix list from which the hit count is to be cleared.
ipv6-prefix/prefix-length	(Optional) IPv6 prefix number and length (in bits) of the network mask. If this option is specified, hit counters are only cleared for the matching statement.

Chapter 12: Quality of Service Commands

This chapter describes the Quality of Service (QoS) commands available in the EFOS CLI.

NOTE: The commands in this chapter are in one of two functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.

12.1 Class of Service Commands

This section describes the commands you use to configure and view Class of Service (CoS) settings for the switch. The commands in this section allow you to control the priority and transmission rate of traffic.

NOTE: Commands you issue in the Interface Config mode only affect a single interface. Commands you issue in the Global Config mode affect all interfaces.

12.1.0.1 classofservice dot1p-mapping

This command maps an 802.1p priority to an internal traffic class. The `userpriority` values can range from 0-7. The `trafficclass` values range from 0-6, although the actual number of available traffic classes depends on the platform.

Format `classofservice dot1p-mapping` *`userpriority trafficclass`*

Modes
- Global Config
- Interface Config

12.1.0.1.1 no classofservice dot1p-mapping

This command maps each 802.1p priority to its default internal traffic class value.

Format `no classofservice dot1p-mapping`

Modes
- Global Config
- Interface Config

12.1.0.2 classofservice ip-dscp-mapping

This command maps an IP DSCP value to an internal traffic class. The `ipdscp` value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

The `trafficclass` values can range from 0-6, although the actual number of available traffic classes depends on the platform.

Format `classofservice ip-dscp-mapping` *`ipdscp trafficclass`*

Mode Global Config

12.1.0.2.1 no classofservice ip-dscp-mapping

This command maps each IP DSCP value to its default internal traffic class value.

Format `no classofservice ip-dscp-mapping`

Mode Global Config

12.1.0.3 classofservice trust

This command sets the class of service trust mode of an interface or range of interfaces. You can set the mode to trust one of the Dot1p (802.1p), IP DSCP, or IP Precedence packet markings. You can also set the interface mode to untrusted. If you configure an interface to use Dot1p, the mode does not appear in the output of the `show running config` command because Dot1p is the default.

NOTE: The `classofservice trust dot1p` command will not be supported in future releases of the software because Dot1p is the default value. Use the `no classofservice trust` command to set the mode to the default value.

Default dot1p

Format `classofservice trust {dot1p | ip-dscp | untrusted}`

Modes
- Global Config
- Interface Config

12.1.0.3.1 no classofservice trust

This command sets the interface mode to the default value.

Format `no classofservice trust`

Modes
- Global Config
- Interface Config

12.1.0.4 cos-queue min-bandwidth

Format `no classofservice trust`

Modes
- Global Config
- Interface Config

This command specifies the minimum transmission bandwidth guarantee for each interface queue on an interface, a range of interfaces, or all interfaces. The total number of queues supported per interface is platform specific. A value from 0-100 (percentage of link rate) must be specified for each supported queue, with 0 indicating no guaranteed minimum bandwidth. The sum of all values entered must not exceed 100.

Format `cos-queue min-bandwidth` *`bw-0 bw-1 … bw-n`*

Modes
- Global Config
- Interface Config

12.1.0.4.1 no cos-queue min-bandwidth

This command restores the default for each queue's minimum bandwidth value.

Format `no cos-queue min-bandwidth`

Modes
- Global Config
- Interface Config

12.1.0.5 cos-queue random-detect

This command activates weighted random early discard (WRED) for each specified queue on the interface. Specific WRED parameters are configured using the `random-detect queue-parms` and the `random-detect exponential-weighting-constant` commands.

Format `cos-queue random-detect` *`queue-id-1`* `[`*`queue-id-2 … queue-id-n`*`]`

Modes
- Global Config
- Interface Config

When specified in Interface Config mode, this command affects a single interface only, whereas in Global Config mode, it applies to all interfaces.

At least one, but no more than *n* queue-id values are specified with this command. Duplicate queue-id values are ignored. Each queue-id value ranges from 0 to (*n*–1), where n is the total number of queues supported per interface. The number *n* = 7 and corresponds to the number of supported queues (traffic classes).

12.1.0.5.1 no cos-queue random-detect

Use this command to disable WRED, thereby restoring the default tail drop operation for the specified queues on the interface.

Format `no cos-queue random-detect` *`queue-id-1`* `[`*`queue-id-2 … queue-id-n`*`]`

Modes
- Global Config
- Interface Config

12.1.0.6 cos-queue strict

This command activates the strict priority scheduler mode for each specified queue for an interface queue on an interface, a range of interfaces, or all interfaces.

Format `cos-queue strict` *`queue-id-1 [queue-id-2 … queue-id-n]`*

Modes
- Global Config
- Interface Config

12.1.0.6.1 no cos-queue strict

This command restores the default weighted scheduler mode for each specified queue.

Format `no cos-queue strict` *`queue-id-1`* `[`*`queue-id-2 … queue-id-n`*`]`

Modes
- Global Config
- Interface Config

12.1.0.7 random-detect

This command is used to enable WRED for the interface as a whole, and is only available when per-queue WRED activation control is not supported by the device Specific WRED parameters are configured using the `random-detect queue-parms` and the `random-detect exponential-weighting-constant` commands.

Format `random-detect`

Modes
- Global Config
- Interface Config

When specified in Interface Config mode, this command affects a single interface only, whereas in Global Config mode, it applies to all interfaces. The Interface Config mode command is only available on platforms that support independent per-port class of service queue configuration.

12.1.0.7.1 no random-detect

Use this command to disable WRED, thereby restoring the default tail drop operation for all queues on the interface.

Format `no random-detect`

Modes
- Global Config
- Interface Config

12.1.0.8 random-detect exponential weighting-constant

This command is used to configure the WRED decay exponent for a CoS queue interface.

Format `random-detect exponential-weighting-constant` *`1-TBD`*

Modes
- Global Config
- Interface Config

12.1.0.8.1 no random-detect exponential-weighting-constant

Use this command to set the WRED decay exponent back to the default.

Format `no random-detect exponential-weighting-constant`

Modes
- Global Config
- Interface Config

12.1.0.9 random-detect queue-parms

This command is used to configure WRED parameters for each drop precedence level supported by a queue. It is used only when per-COS queue configuration is enabled (using the `cos-queue random-detect` command).

Format
`random-detect queue-parms` *`queue-id`* `[`*`queue-id`*`] ...` `[units {KB|percentage}] min-thresh` *`minthresh-green minthresh-yellow minthresh-red minthresh-nontcp`* `max-thresh` *`max-thresh-green max-thresh-yellow max-thresh-red maxthresh-nontcp`* `drop-prob-scale` *`drop-scale-green drop-scale-yellow drop-scale-red drop-scale-nontcp`* `[ ecn ]`
`no random-detect queue-parms` *`queue-id`* `[`*`queue-id`*`] ...`

Modes
- Global Config
- Interface Config

Each parameter is specified for each possible drop precedence (*color* of TCP traffic). The last precedence applies to all non-TCP traffic. For example, in a 3-color system, four of each parameter specified: green TCP, yellow TCP, red TCP, and non-TCP, respectively.

Parameter	Definition
queue-id	The internal class of service queue. Range 0 to 6. This is the internal CoS queue number, which is not the same as the CoS or DSCP value received in the packet. Use the `show classofservice dot1p-mapping` command to display the CoS value to CoS queue mapping.
units	Minimum and maximum threshold values can be configured in KB or percentage.
min-thresh	The minimum congestion threshold (in terms of percentage of queue depth) at which to begin dropping or ECN marking packets at 1/8th of the configured drop probability. At or below the minimum threshold, no packets are dropped. The range between the minimum and maximum thresholds is divided equally into 8 increasing levels of drop probability.
max-thresh	The maximum congestion threshold to end dropping at the configured maximum drop probability and to begin dropping at 100%.
drop-probability	The maximum drop probability. Range 0-100. This is the drop probability for a packet when the maximum threshold is reached. Above the maximum threshold, 100% of matching packets are dropped.
ecn	Enable ECN marking on the selected CoS queues. When EC N is enabled, packets not marked as ECN capable are dropped when selected for discard by WRED.

Default Configuration

The default WRED thresholds are listed below. By default WRED is not enabled for any CoS queue and ECN is not enabled for any CoS queue. By default, minimum and maximum threshold units are percentage. The thresholds for each color and CoS queue are configured independently and may overlap.

Usage Guidelines for ECN-Capable Systems

ECN capability is an end-to-end feedback mechanism. Both ends of the TCP connection must participate. When ECN is enabled, packets marked as ECN-capable and exceeding the upper WRED threshold are marked CE and are not dropped. In cases of extreme congestion, ECN-capable packets may be dropped.

Use the `show interfaces traffic` command to see color aware drops, ECN Tx counts, and congestion levels.

ECN capability can be enabled in Windows Server 2008 and later releases using the following command:

```
netsh interface tcp set global ecncapability=enabled
```

Examples

Example: The following example configures simple meter and a trTCM meter.

```
! Define a class-map so that all traffic will be in the set of traffic  cos-any
class-map match-all cos-any ipv4
match any
exit
! Define a class-map such that all traffic with a Cos value of 1
! will be in the set of traffic cos1.
! We will use this as a conform color class map. Conform-color class
! maps must be one of cos, secondary cos,
```

```
! dscp, or ip precedence.
class-map match-all cos1 ipv4
match cos 1
exit
! Define a class-map such that all ipv4 traffic with a Cos value of 0
! will be in the set of traffic cos0.
! We will use this as a conform color class map. Conform-color class
! maps must be one of cos, secondary cos,  dscp, or ip precedence.
class-map match-all cos0 ipv4
match cos 0
exit
! Define a class-map such that all TCP will be in the set of traffic TCP.
! We will use this as a base color class for metering traffic.
class-map match-all tcp ipv4
match protocol tcp
exit
!
! Define a policy-map to include packets matching class cos-any (IPv4).
! Ingress IPv4 traffic arriving at a port  participating this policy will
! be assigned red or green coloring based on the metering.
!
policy-map simple-policy in
class cos-any
!
! Create a simple policer in color blind mode. Packets below the committed information
! rate (CIR) or committed burst size (CBS) are assigned drop precedence green.
! Packets that exceed the CIR (in Kbps) or CBS (in Kbytes) are colored red.
! Both the conform and violate actions are set to transmit as WRED is
! used to drop packets when congested.
!
police-simple 10000000 64 conform-action transmit violate-action transmit
exit
exit
!
! Define a policy-map in color aware mode matching class cos-any (IPv4).
! Ingress IPv4 traffic arriving at a port participating in this policy will be
! assigned green, yellow or red coloring based on the meter.
!
policy-map two-rate-policy in
class tcp
!
! Create a two-rate policer per RFC 2698. The CIR value is 800 Kbps and
! the CBS is set to 96 Kbytes.  The PIR is set to 950 Kbps and the PBS is
! set to 128 Kbytes. Color-aware processing is enabled via the  conform-color
! command, i.e. any packets not in cos 0 or 1 are pre-colored red. Packets in
! cos 0 are pre-colored yellow. Packets in cos 1 are pre-colored green.
! Pre-coloring gives greater bandwidth to CoS 1 as they are initially
! subject to the CIR/CBS limits. Packets in CoS 0 are subject to the PIR limits.
! Based on the CIR/CBD, the PIR/PBS, and the conform, exceed, and
! violate actions specified below:
!
! TCP packets with rates less than or equal to the CIR/CBS in class cos1
! are conforming to the rate (green).
! These packets will be dropped randomly at an increasing rate between 0-3%
! when the outgoing interface is congested between 80 and 100%.
!
! TCP packets with rates above the CIR/CBS and less than or equal to
! PIR/PBS in either class cos1 or class cos2  are policed as exceeding the
```

```
! CIR (yellow). These packets will be dropped randomly at an increasing rate
! between 0-5% when the outgoing interface is congested between 70 and 100%.

! TCP packets with rates higher than the PIR/PBS or which belong to neither
! class cos1 or class cos2 are  violating the rate (red). These packets will be
! dropped randomly at an increasing rate between 0-10% when the outgoing
! interface is congested between 50 and 100%.
!
! Non TCP packets in CoS queue 0 or 1 will be dropped randomly at an increasing
! rate between 0-15% when the outgoing interface is congested between 50 and 100%.
!
police-two-rate 800 96 950 128 conform-action transmit exceed-action transmit violate-action transmit
conform-color cos1 exceed-color cos0
exit
exit
!
!Enable WRED drop on traffic classes 0 and 1
!
cos-queue random-detect 0 1
!
! Set the exponential-weighting-constant. The exponential weighting constant smooths
! the result of the average queue depth calculation by the function:
!   average depth = (previous queue depth * (1-1/2^n)) + (current queue depth * 1/2^n).
! Because the instantaneous queue depth fluctuates rapidly, larger values will cause
! the average queue depth value to respond to changes more slowly than smaller values.
! The average depth is used in calcuating the amount of congestion on a queue.
!
random-detect exponential-weighting-constant 4
!
! Configure the queue parameters for traffic class 0 and 1. We set the minimum threshold and maximum
! thresholds to 80-100% for green traffic, 70-100% for yellow traffic and 50-100% for red traffic.
! Non-TCP traffic drops in the 50-100% congestion range. Green traffic is dropped
! at a very low rate to slowly close the TCP window. Yellow and red traffic
! are dropped more aggresively.
!
random-detect queue-parms 0 1 min-thresh 80 70 50 50 max-thresh 100 100 100 100 drop-prob-scale  3 5
10 15
!
! Assign the color policies to ports. The metering policies are applied on ingress ports.
!
interface 0/22
service-policy in simple-policy
exit
interface 0/23
service-policy in two-rate-policy
exit
```

Example: The following example enables WRED discard for non-color aware traffic. Since a color-aware policer is not enabled, the traffic is treated as if it were colored green. This means that only the green TCP and non-TCP WRED thresholds are active.

```
!
! Configure the thresholds for TCP traffic on COS queue 1. The other thresholds are kept at their
default values.
! The minimum threshold of 50% and maximum threshold of 100% with
! a drop probability of 2% are a good starting point for tuning the WRED
! parameters for a particular network.
```

```
!
random-detect queue-parms 1 min-thresh 50 30 20 100 max-thresh 100 90 80 100 drop-prob-scale  2 10 10 10
!
! Enable WRED on cos-queue 1 (the default cos queue).
!
cos-queue random-detect 1
```

Example: This example globally configures the switch to utilize ECN marking of packets queued for egress on CoS queues 0 and 1 using the DCTCP threshold as it appears in "DCTCP: Efficient Packet Transport for the Commoditized Data Center."

The first threshold parameter configures Congestion Enabled TCP packets in CoS queues 0 and 1 that exceed the WRED threshold given below (13%) to be marked as Congestion Experienced in conjunction with the first ECN parameter. TCP packets without ECN capability bits are dropped according to the normal WRED processing. Packets on other CoS queues are handled in the standard manner, i.e. tail dropped when insufficient buffer is available. Yellow and red packet configuration (second and third threshold parameters) is kept at the defaults as no metering to reclassify packets from green to yellow or red is present. The last threshold parameter configures non-TCP packets in CoS queues 0 and 1 to be processed with the WRED defaults. The ecn keyword configures CoS queues 0 and 1 for ECN marking. The weighting constant is set to 0 in the second line of the configuration as described in the DCTCP paper cited above. Finally, CoS queues 0 and 1 are configured for WRED as shown in the last line of the configuration.

```
console(config)#random-detect queue-parms 0 1 min-thresh 13 30 20 100 max-thresh 13 90 80 drop-prob-
scale 100 10 10 10 ecn
console(config)#random-detect exponential-weighting-constant 0
console(config)#cos-queue random-detect 0 1
```

Example: Enable WRED and ECN on queues 0 and 1, enable WRED on queues 2 and 3.

```
random-detect queue-parms 0 1 min-thresh 13 30 20 100 max-thresh 13 90 80 drop-prob-scale 100 10 10
10 ecn
random-detect queue-parms 2 3 min-thresh 13 30 20 100 max-thresh 13 90 80 drop-prob-scale 100 10 10 10
cos-queue random-detect 0 1 2 3
```

Example: Set the WRED parameters to their default values on queues 0 and 1

```
no random-detect queue-parms 0 1
```

12.1.0.9.1 no random-detect queue-parms

Use this command to set the WRED configuration back to the default.

Format `no random-detect queue-parms` *`queue-id`* `[`*`queue-id`*`]...`

Modes
- Global Config
- Interface Config

12.1.0.10 traffic-shape

This command specifies the maximum transmission bandwidth limit for the interface as a whole. You can also specify this value for a range of interfaces or all interfaces. Also known as rate shaping, traffic shaping has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded.

Format `traffic-shape` *`bw`*

Modes
- Global Config
- Interface Config

12.1.0.10.1 no traffic-shape

This command restores the interface shaping rate to the default value.

Format `no traffic-shape`

Modes
- Global Config
- Interface Config

12.1.0.11 show classofservice dot1p-mapping

This command displays the current Dot1p (802.1p) priority mapping to internal traffic classes for a specific interface. The *slot/port* parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the 802.1p mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Format `show classofservice dot1p-mapping [slot/port]`

Mode Privileged EXEC

The following information is repeated for each user priority.

Parameter	Definition
User Priority	The 802.1p user priority value.
Traffic Class	The traffic class internal queue identifier to which the user priority value is mapped.

12.1.0.12 show classofservice ip-precedence-mapping

This command displays the current IP Precedence mapping to internal traffic classes for a specific interface. The *slot/port* parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the IP Precedence mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Format `show classofservice ip-precedence-mapping [slot/port]`

Mode Privileged EXEC

The following information is repeated for each user priority.

Parameter	Definition
IP Precedence	The IP Precedence value.
Traffic Class	The traffic class internal queue identifier to which the IP Precedence value is mapped.

12.1.0.13 show classofservice ip-dscp-mapping

This command displays the current IP DSCP mapping to internal traffic classes for the global configuration settings.

Format `show classofservice ip-dscp-mapping`
Mode Privileged EXEC

The following information is repeated for each user priority.

Parameter	Definition
IP DSCP	The IP DSCP value.
Traffic Class	The traffic class internal queue identifier to which the IP DSCP value is mapped.

12.1.0.14 show classofservice trust

This command displays the current trust mode setting for a specific interface. The *slot/port* parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If you specify an interface, the command displays the port trust mode of the interface. If you do not specify an interface, the command displays the most recent global configuration settings.

Format `show classofservice trust [slot/port]`
Mode Privileged EXEC

Parameter	Definition
Non-IP Traffic Class	The traffic class used for non-IP traffic. This is only displayed when the COS trust mode is set to trust IP Precedence or IP DSCP (on platforms that support IP DSCP).
Untrusted Traffic Class	The traffic class used for all untrusted traffic. This is only displayed when the COS trust mode is set to 'untrusted'.

12.1.0.15 show interfaces cos-queue

This command displays the class-of-service queue configuration for the specified interface. The *slot/port* parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the class-of-service queue configuration of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Format `show interfaces cos-queue [slot/port]`
Mode Privileged EXEC

Parameter	Definition
Queue Id	An interface supports n queues numbered 0 to (n-1). The specific n value is platform dependent.
Minimum Bandwidth	The minimum transmission bandwidth guarantee for the queue, expressed as a percentage. A value of 0 means bandwidth is not guaranteed and the queue operates using best-effort. This is a configured value.
Scheduler Type	Indicates whether this queue is scheduled for transmission using a strict priority or a weighted scheme. This is a configured value.
Queue Management Type	The queue depth management technique used for this queue (tail drop).

If you specify the interface, the command also displays the following information.

Parameter	Definition
Interface	The *slot/port* of the interface. If displaying the global configuration, this output line is replaced with a Global Config indication.
Interface Shaping Rate	The maximum transmission bandwidth limit for the interface as a whole. It is independent of any per-queue maximum bandwidth value(s) in effect for the interface. This is a configured value.

12.1.0.16 show interfaces random-detect

This command displays the global WRED settings for each CoS queue. If you specify the slot/port, the command displays the WRED settings for each CoS queue on the specified interface. Valid interfaces include physical ports and port channels. ECN capability is also displayed.

The per CoS queue display for an interface displays the threshold, drop probability, and ECN capability per color in the order, green, yellow, red, and non-TCP.

Format `show interfaces random-detect [slot/port]`

Mode Privileged EXEC

Parameter	Definition
Queue ID	An interface supports n queues numbered 0 to (n-1). The n value is platform dependent.
WRED Minimum Threshold	The configured minimum threshold the queue depth (as a percentage) where WRED starts marking and dropping traffic.
WRED Maximum Threshold	The configured maximum threshold is the queue depth (as a percentage) above which WRED marks / drops all traffic.
WRED Drop Probability	The configured percentage probability that WRED will mark/drop a packet, when the queue depth is at the maximum threshold. (The drop probability increases linearly from 0 just before the minimum threshold, to this value at the maximum threshold, then goes to 100% for larger queue depths).
ECN	Identifies whether ECN is enabled.

Example: This example shows ECN enabled on CoS queues 0 and 1 with a minimum threshold of 40% for green colored packets, 30% for yellow colored packets, 20% for red colored packets and 100% for non-TCP packets.

```
(switch)#show interfaces random-detect

Global Configuration

Queue ID..................................... 0
Threshold Units.............................. Percentage
WRED Minimum Threshold
  Precedence level 0......................... 40
  Precedence level 1......................... 30
  Precedence level 2......................... 20
  Precedence level 3......................... 99
WRED Drop Probability
  Precedence level 0......................... 10
  Precedence level 1......................... 10
  Precedence level 2......................... 10
  Precedence level 3......................... 10
ECN Enabled.................................. No
```

```
Queue ID..................................... 1
Threshold Units.............................. Percentage
WRED Minimum Threshold
  Precedence level 0......................... 40
  Precedence level 1......................... 30
  Precedence level 2......................... 20
  Precedence level 3......................... 99
WRED Drop Probability
  Precedence level 0......................... 10
  Precedence level 1......................... 10
  Precedence level 2......................... 10
  Precedence level 3......................... 10
ECN Enabled.................................. No
```

12.2 Differentiated Services Commands

This section describes the commands you use to configure QOS Differentiated Services (DiffServ).

You configure DiffServ in several stages by specifying three DiffServ components:

1. Class
   a. Creating and deleting classes.
   b. Defining match criteria for a class.
2. Policy
   a. Creating and deleting policies
   b. Associating classes with a policy
   c. Defining policy statements for a policy/class combination
3. Service
   a. Adding and removing a policy to/from an inbound interface

The DiffServ class defines the packet filtering criteria. The attributes of a DiffServ policy define the way the switch processes packets. You can define policy attributes on a per-class instance basis. The switch applies these attributes when a match occurs.

Packet processing begins when the switch tests the match criteria for a packet. The switch applies a policy to a packet when it finds a class match within that policy.

The following rules apply when you create a DiffServ class:

- Each class can contain a maximum of one referenced (nested) class
- Class definitions do not support hierarchical service policies

A given class definition can contain a maximum of one reference to another class. You can combine the reference with other match criteria. The referenced class is truly a reference and not a copy since additions to a referenced class affect all classes that reference it. Changes to any class definition currently referenced by any other class must result in valid class definitions for all derived classes, otherwise the switch rejects the change. You can remove a class reference from a class definition.

The only way to remove an individual match criterion from an existing class definition is to delete the class and recreate it.

NOTE: The mark possibilities for policing include CoS, IP DSCP, and IP Precedence. While the latter two are only meaningful for IP packet types, CoS marking is allowed for both IP and non-IP packets, since it updates the 802.1p user priority field contained in the VLAN tag of the layer 2 packet header.

12.2.0.1 diffserv

This command sets the DiffServ operational mode to active. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, DiffServ services are activated.

Format	`diffserv`
Mode	Global Config

12.2.0.1.1 no diffserv

This command sets the DiffServ operational mode to inactive. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, DiffServ services are activated.

Format `no diffserv`

Mode Global Config

12.3 DiffServ Class Commands

Use the DiffServ class commands to define traffic classification. To classify traffic, you specify Behavior Aggregate (BA), based on DSCP and Multi-Field (MF) classes of traffic (name, match criteria)

This set of commands consists of class creation/deletion and matching, with the class match commands specifying Layer 3, Layer 2, and general match criteria. The class match criteria are also known as class rules, with a class definition consisting of one or more rules to identify the traffic that belongs to the class.

NOTE: Once you create a class match criterion for a class, you cannot change or delete the criterion. To change or delete a class match criterion, you must delete and recreate the entire class.

The CLI command root is `class-map`.

12.3.0.1 class-map

This command defines a DiffServ class of type match-all or match-any. When used without any match condition, this command enters the class-map mode. The `class-map-name` is a case sensitive alphanumeric string from 1 to 31 characters uniquely identifying an existing DiffServ class.

For the `match-all` argument, a given packet needs to match all the rules configured in class-map to get classified as the configured class-map.

For the `match-any` argument, a given packet can match at least one of the rules configured in the class-map to get classified as the configured class-map.

NOTE: The class-map-name 'default' is reserved and must not be used.

This command may be used without specifying a class type to enter the Class-Map Config mode for an existing DiffServ class.

NOTE: Note the following:

- The optional keywords `[{ipv4 | ipv6}]` specify the Layer 3 protocol for this class. If not specified, this parameter defaults to ipv4. This maintains backward compatibility for configurations defined on systems before IPv6 match items were supported. You can configure the protocol type using the `match protocol protocol-type` command in the Class-map config mode.The optional keyword `appiq` creates a new DiffServ appiq class. Regular expressions found in the traffic patterns in layer 7 applications can be matched to the App-IQ class using a `match signature` command.
- The CLI mode is changed to Class-Map Config when this command is successfully executed.

Format `class-map {match-all | match-any} class-map-name [{appiq | ipv4 | ipv6}]`

Mode Global Config

Parameter	Definition
match-all	For the match-all argument, a given packet needs to match all the rules configured in class-map to get classified as the configured class-map.
match-any	For the match-any argument, a given packet can match at least one of the rules configured in the class-map to get classified as the configured class-map.
class-map-name	A case sensitive alphanumeric string from 1 to 31 characters uniquely identifying a DiffServ class.

Example: This example shows configuring a new class-map with the class-map name *test-class-map*.

```
(Switching) (Config)#class-map match-all test-class-map
(Switching) (Config-classmap)#
(Switching) (Config-classmap)#exit

(Switching) (Config)#class-map ?

<class-map-name>         Enter an existing DiffServ class name to enter the
                         class-map config mode.
match-all                Specify class type as all.
match-any                Specify class type as any.
rename                   Rename a DiffServ Class.

(Switching) (Config)#class-map match-all test-class-map-1
(Switching) (Config-classmap)# match ip dscp 36
(Switching) (Config-classmap)# match protocol ip
(Switching) (Config-classmap)# exit

(Switching) (Config)#class-map match-any test-class-map-2
(Switching) (Config-classmap)# match ip dscp 36
(Switching) (Config-classmap)# match protocol ipv6
(Switching) (Config-classmap)# exit

(Switching) (Config)#class-map match-any test-class-map-3
(Switching) (Config-classmap)# match access-group test-access-list-3
(Switching) (Config-classmap)# exit
```

12.3.0.1.1 no class-map

This command eliminates an existing DiffServ class. The *class-map-name* is the name of an existing DiffServ class. (The class name **default** is reserved and is not allowed here.) This command may be issued at any time; if the class is currently referenced by one or more policies or by any other class, the delete action fails.

Format `no class-map` *class-map-name*
Mode Global Config

12.3.0.2 class-map rename

This command changes the name of a DiffServ class. The `class-map-name` is the name of an existing DiffServ class. The `new-class-map-name` parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the class.

Default none
Format `class-map rename` *class-map-name new-class-map-name*
Mode Global Config

12.3.0.3 match access-group

This command configures for the specified class a match condition based on the configured IPv4 access-list number. The value for *acl-number* is a valid standard or extended ACL in the range from 1 to 199.

The `no` form does not exist for this command.

Format `match access-group` *`acl-number`*
Mode Class-Map Config

12.3.0.4 match access-group name

This command configures for the specified class a match condition based on the name of the configured access-list. The value for *`acl-name`* is in the range from 1 to 199.

The following notes apply to this command:

- Class-maps containing access-list as match criteria may only be applied to ingress policies.
- The action (mirror, redirect, time-range, etc) clauses in the access-lists referenced by a policy are ignored for the purpose of policy application. The access-lists are used for matching the traffic only.
- The `no` form does not exist for this command.
- IPv4, IPv6, and MAC ACLs can be configured as match criteria using this command.

Format `match access-group name` *`acl-name`*
Mode Class-Map Config

12.3.0.5 match any

This command adds to the specified class definition a match condition whereby all packets are considered to belong to the class. Use the [not] option to negate the match condition.

Default none
Format `match [not] any`
Mode Class-Map Config

12.3.0.6 match class-map

This command adds to the specified class definition the set of match conditions defined for another class. The `refclassname` is the name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

Default `none`
Format `match class-map` *`refclassname`*
Mode Class-Map Config

NOTE: Note the following:

- The parameters refclassname and class-map-name can not be the same.
- Only one other class may be referenced by a class.
- Any attempts to delete the refclassname class while the class is still referenced by any class-map-name fails.
- The combined match criteria of class-map-name and refclassname must be an allowed combination based on the class type.
- Any subsequent changes to the refclassname class match criteria must maintain this validity, or the change attempt fails.
- The total number of class rules formed by the complete reference class chain (including both predecessor and successor classes) must not exceed a platform-specific maximum. In some cases, each removal of a refclass

rule reduces the maximum number of available rules in the class definition by one.

12.3.0.6.1 no match class-map

This command removes from the specified class definition the set of match conditions defined for another class. The `refclassname` is the name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

Format `no match class-map` *`refclassname`*
Mode Class-Map Config

12.3.0.7 match cos

This command adds to the specified class definition a match condition for the Class of Service value (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). The value may be from 0 to 7. Use the [not] option to negate the match condition.

Default none
Format `match [not] cos` *`0-7`*
Mode Class-Map Config

12.3.0.8 match secondary-cos

This command adds to the specified class definition a match condition for the secondary Class of Service value (the inner 802.1Q tag of a double VLAN tagged packet). The value may be from 0 to 7. Use the [not] option to negate the match condition.

NOTE: This command is supported on the following platforms:

- BCM56314
- BCM56504
- BCM56214
- BCM56224

Default none
Format `match [not] secondary-cos` *`0-7`*
Mode Class-Map Config

12.3.0.9 match destination-address mac

This command adds to the specified class definition a match condition based on the destination MAC address of a packet. The *`macaddr`* parameter is any layer 2 MAC address formatted as six, two-digit hexadecimal numbers separated by colons (e.g., 00:11:22:dd:ee:ff). The *`macmask`* parameter is a layer 2 MAC address bit mask, which need not be contiguous, and is formatted as six, two-digit hexadecimal numbers separated by colons (e.g., ff:07:23:ff:fe:dc). Use the [not] option to negate the match condition.

Default none
Format `match [not] destination-address mac` *`macaddr macmask`*

Mode Class-Map Config

12.3.0.10 match dstip

This command adds to the specified class definition a match condition based on the destination IP address of a packet. The `ipaddr` parameter specifies an IP address. The `ipmask` parameter specifies an IP address bit mask and must consist of a contiguous set of leading 1 bits. Use the [not] option to negate the match condition.

Default none
Format `match [not] dstip` *`ipaddr ipmask`*
Mode Class-Map Config

12.3.0.11 match dstip6

This command adds to the specified class definition a match condition based on the destination IPv6 address of a packet. Use the [not] option to negate the match condition.

Default none
Format `match [not] dstip6` *`destination-ipv6-prefix/prefix-length`*
Mode Ipv6-Class-Map Config

12.3.0.12 match dstl4port

This command adds to the specified class definition a match condition based on the destination layer 4 port of a packet using a single keyword or numeric notation. To specify the match condition as a single keyword, the value for `portkey` is one of the supported port name keywords. The currently supported `portkey` values are: domain, echo, ftp, ftpdata, smtp, snmp, telnet, tftp, www. Each of these translates into its equivalent port number. To specify the match condition using a numeric notation, one layer 4 port number is required. The port number is an integer from 0 to 65535. Use the [not] option to negate the match condition.

Default none
Format `match [not] dstl4port {`*`portkey | 0-65535`*`}`
Mode Class-Map Config

12.3.0.13 match ethertype

This command adds to the specified class definition a match condition based on the value of the ethertype. The `ethertype` value is specified as one of the following keywords: `appletalk`, `arp`, `ibmsna`, `ipv4`, `ipx`, `mplsmcast`, `mplsucast`, `netbios`, `novell`, `pppoe`, `rarp` or as a custom EtherType value in the range of 0x0600-0xFFFF. Use the [not] option to negate the match condition.

Format `match [not] ethertype {`*`keyword | custom 0x0600-0xFFFF`*`}`
Mode Class-Map Config

12.3.0.14 match exp

This command configures for the specified class a match condition based on the MPLS-TP EXP (Traffic Class field) value. The *`exp-value`* parameter is the MPLS-TP traffic class field value, which has a possible range of 0 to 7.

Format `match exp` *exp-value*
Mode Class-Map Config

12.3.0.14.1 no match exp

This command removes the MPLS-TP EXP match statement from the class-map.

Format `no match exp` *exp-value*
Mode Class-Map Config

12.3.0.15 match ip dscp

This command adds to the specified class definition a match condition based on the value of the IP DiffServ Code Point (DSCP) field in a packet, which is defined as the high-order six bits of the Service Type octet in the IP header (the low-order two bits are not checked).

The `dscpval` value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef. Use the [not] option to negate the match condition.

NOTE: The ip dscp, ip precedence, and ip tos match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

Default none
Format `match ip dscp` *dscpval*
Mode Class-Map Config

12.3.0.16 match ip precedence

This command adds to the specified class definition a match condition based on the value of the IP Precedence field in a packet, which is defined as the high-order three bits of the Service Type octet in the IP header (the low-order five bits are not checked). The precedence value is an integer from 0 to 7. Use the [not] option to negate the match condition.

NOTE: The IP DSCP, IP Precedence, and IP ToS match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

Default none
Format `match [not] ip precedence` *0-7*
Mode Class-Map Config

12.3.0.17 match ip tos

This command adds to the specified class definition a match condition based on the value of the IP TOS field in a packet, which is defined as all eight bits of the Service Type octet in the IP header. The value of `tosbits` is a two-digit hexadecimal number from 00 to ff. The value of `tosmask` is a two-digit hexadecimal number from 00 to ff. The `tosmask` denotes the bit positions in `tosbits` that are used for comparison against the IP TOS field in a packet. For example, to check for an IP TOS value having bits 7 and 5 set and bit 1 clear, where bit 7 is most significant, use a `tosbits` value of a0 (hex) and a `tosmask` of a2 (hex). Use the [not] option to negate the match condition.

NOTE: Note the following:

- The IP DSCP, IP Precedence, and I ToS match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.
- This “free form” version of the IP DSCP/Precedence/TOS match specification gives the user complete control when specifying which bits of the IP Service Type field are checked.

Default none

Format `match [not] ip tos` *`tosbits tosmask`*

Mode Class-Map Config

12.3.0.18 match ip6flowlbl

Use this command to enter an IPv6 flow label value. Use the [not] option to negate the match condition.

Default none

Format `match [not] ip6flowlbl label` *`0-1048575`*

Mode IPv6-Class-Map Config

12.3.0.19 match protocol

This command converts an IPv4 class-map to either an IPv6 class-map (if the argument is *ipv6*) or non-IP class-map (if the argument is *none*.

Format `match protocol` *`none|ipv6`*

Mode Class-Map Config

NOTE: The `no` form does not exist for this command.

12.3.0.20 match protocol

This command adds to the specified class definition a match condition based on the protocol type using a single keyword notation or a numeric value notation.

To specify the match condition using a single keyword, use one of the following: `icmp`, `igmp`, `ip`, `tcp`, `udp`, `ipv6`, `gre`, and `icmpv6`.

To specify the match condition using a numeric value notation, the protocol number is a standard value assigned by IANA and is interpreted as an integer from 0 to 255. Use the [not] option to negate the match condition.

NOTE: This command does not validate the protocol number value against the current list defined by IANA.

Default none

Format `match [not] protocol {`*`0-255`* `| { icmp | igmp | ip | tcp | udp | ipv6 | gre | icmpv6} | none}`

Mode Class-Map Config

Example: This example shows the process of configuring the protocol type `tcp` for a give class-map `test-class-map`

```
(switch) (Config)#class-map match-all test-class-map
(switch) (Config-classmap)# match protocol tcp
```

12.3.0.21 match source-address mac

This command adds to the specified class definition a match condition based on the source MAC address of a packet. The *address* parameter is any layer 2 MAC address formatted as six, two-digit hexadecimal numbers separated by colons (e.g., 00:11:22:dd:ee:ff). The *macmask* parameter is a layer 2 MAC address bit mask, which may not be contiguous, and is formatted as six, two-digit hexadecimal numbers separated by colons (e.g., ff:07:23:ff:fe:dc). Use the [not] option to negate the match condition.

Default none

Format `match [not] source-address mac` *address macmask*

Mode Class-Map Config

12.3.0.22 match srcip

This command adds to the specified class definition a match condition based on the source IP address of a packet. The `ipaddr` parameter specifies an IP address. The `ipmask` parameter specifies an IP address bit mask and must consist of a contiguous set of leading 1 bits. Use the [not] option to negate the match condition.

Default none

Format `match [not] srcip` *ipaddr ipmask*

Mode Class-Map Config

12.3.0.23 match srcip6

This command adds to the specified class definition a match condition based on the source IP address of a packet. Use the [not] option to negate the match condition.

Default none

Format `match [not] srcip6` *source-ipv6-prefix/prefix-length*

Mode Ipv6-Class-Map Config

12.3.0.24 match srcl4port

This command adds to the specified class definition a match condition based on the source layer 4 port of a packet using a single keyword or numeric notation. To specify the match condition as a single keyword notation, the value for `portkey` is one of the supported port name keywords (listed below). The currently supported `portkey` values are: domain, echo, ftp, ftpdata, smtp, snmp, telnet, tftp, www. Each of these translates into its equivalent port number, which is used as both the start and end of a port range.

To specify the match condition as a numeric value, one layer 4 port number is required. The port number is an integer from 0 to 65535. Use the [not] option to negate the match condition.

Default none

Format `match not srcl4port {`*portkey* | *0-65535*`}`

Mode Class-Map Config

12.3.0.25 match src port

This command adds a match condition for a range of layer source 4 ports. If an interface receives traffic that is within the configured range of layer 4 source ports, then only the `appiq` class is in effect. *portvalue* specifies a single source port.

Default	none
Format	`match src port {`*`portstart-portend`* `|` *`portvalue`*`}`
Mode	Class-Map Config

12.3.0.26 match vlan

This command adds to the specified class definition a match condition based on the value of the layer 2 VLAN Identifier field (the only tag in a single tagged packet or the first or outer tag of a double VLAN tagged packet). The VLAN ID is an integer from 0 to 4095. Use the [not] option to negate the match condition.

Default	none
Format	`match [not] vlan` *`0-4095`*
Mode	Class-Map Config

12.3.0.27 match secondary-vlan

This command adds to the specified class definition a match condition based on the value of the layer 2 secondary VLAN Identifier field (the inner 802.1Q tag of a double VLAN tagged packet). The secondary VLAN ID is an integer from 0 to 4095. Use the [not] option to negate the match condition.

Default	none
Format	`match [not] secondary-vlan` *`0-4095`*
Mode	Class-Map Config

12.4 DiffServ Policy Commands

Use the DiffServ policy commands to specify traffic conditioning actions, such as policing and marking, to apply to traffic classes

Use the policy commands to associate a traffic class that you define by using the class command set with one or more QoS policy attributes. Assign the class/policy association to an interface to form a service. Specify the policy name when you create the policy.

Each traffic class defines a particular treatment for packets that match the class definition. You can associate multiple traffic classes with a single policy. When a packet satisfies the conditions of more than one class, preference is based on the order in which you add the classes to the policy. The first class you add has the highest precedence.

This set of commands consists of policy creation/deletion, class addition/removal, and individual policy attributes.

NOTE: The only way to remove an individual policy attribute from a class instance within a policy is to remove the class instance and readd it to the policy. The values associated with an existing policy attribute can be changed without removing the class instance.

The CLI command root is `policy-map`.

12.4.0.1 assign-queue

This command modifies the queue id to which the associated traffic stream is assigned. The `queueid` is an integer from 0 to `n`-1, where `n` is the number of egress queues supported by the device.

Format	`assign-queue` *`queueid`*
Mode	Policy-Class-Map Config
Incompatibilities	Drop

12.4.0.2 drop

This command specifies that all packets for the associated traffic stream are to be dropped at ingress.

Format	`drop`
Mode	Policy-Class-Map Config
Incompatibilities	Assign Queue, Mark (all forms), Mirror, Police, Redirect

12.4.0.3 mirror

This command specifies that all incoming packets for the associated traffic stream are copied to a specific egress interface (physical port or LAG).

Format	`mirror` *`slot/port`*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Redirect

12.4.0.4 redirect

This command specifies that all incoming packets for the associated traffic stream are redirected to a specific egress interface (physical port or port-channel).

Format	`redirect` *`slot/port`*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mirror

12.4.0.5 conform-color

Use this command to enable color-aware traffic policing and define the conform-color class map. Used in conjunction with the police command where the fields for the conform level are specified. The *`class-map-name`* parameter is the name of an existing DiffServ class map.

NOTE: This command may only be used after specifying a police command for the policy-class instance.

Format	`conform-color` *`class-map-name`*
Mode	Policy-Class-Map Config

12.4.0.6 class

This command creates an instance of a class definition within the specified policy for the purpose of defining treatment of the traffic class through subsequent policy attribute statements. The `classname` is the name of an existing DiffServ class.

NOTE: Note the following:

- This command causes the specified policy to create a reference to the class definition.
- The CLI mode is changed to Policy-Class-Map Config when this command is successfully executed.

Format	`class` *`classname`*
Mode	Policy-Map Config

12.4.0.6.1 no class

This command deletes the instance of a particular class and its defined treatment from the specified policy. `classname` is the names of an existing DiffServ class.

NOTE: This command removes the reference to the class definition for the specified policy.

Format	`no class` *`classname`*
Mode	Policy-Map Config

12.4.0.7 mark cos

This command marks all packets for the associated traffic stream with the specified class of service (CoS) value in the priority field of the 802.1p header (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). If the packet does not already contain this header, one is inserted. The CoS value is an integer from 0 to 7.

Default	1

Format	`mark-cos` *`0-7`*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark IP DSCP, IP Precedence, Police

12.4.0.8 mark secondary-cos

This command marks all packets for the associated traffic stream with the specified secondary class of service (CoS) value in the priority field of the 802.1p header (the secondary or inner 802.1Q tag of a double VLAN tagged packet). If the packet does not already contain this header, one is inserted. The CoS value is an integer from 0 to 7.

Format	`mark secondary-cos` *`0-7`*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark IP DSCP, IP Precedence, Police

12.4.0.9 mark cos-as-sec-cos

This command marks outer VLAN tag priority bits of all packets as the inner VLAN tag priority, marking Cos as Secondary CoS. This essentially means that the inner VLAN tag CoS is copied to the outer VLAN tag CoS.

Format	mark-cos-as-sec-cos
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark IP DSCP, IP Precedence, Police

Example: The following shows an example of the command.

```
(Routing) (Config-policy-classmap)#mark cos-as-sec-cos
```

12.4.0.10 mark exp

This command configures diffserv policy-map to mark all the packets of the associated traffic stream with the specified MPLS-TP EXP (Traffic Class field) value. The *`exp-value`* parameter is the MPLS-TP traffic class field value and has a possible range of 0 to 7.

Format	`mark exp` *`exp-value`*
Mode	Policy-Class-Map Config

12.4.0.10.1 no mark exp

This command removes the MPLS-TP EXP mark statement from the DiffServ policy-map.

Format	`no mark exp`
Mode	Policy-Class-Map Config

12.4.0.11 mark ip-dscp

This command marks all packets for the associated traffic stream with the specified IP DSCP value.

The `dscpval` value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

Format	`mark ip-dscp` *`dscpval`*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark CoS, Mark IP Precedence, Police

12.4.0.12 mark ip-precedence

This command marks all packets for the associated traffic stream with the specified IP Precedence value. The IP Precedence value is an integer from 0 to 7.

Format	`mark ip-precedence` *`0-7`*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark CoS, Mark IP Precedence, Police
Policy Type	In

12.4.0.13 police-simple

This command is used to establish the traffic policing style for the specified class. The simple form of the **police** command uses a single data rate and burst size, resulting in two outcomes: conform and violate. The conforming data rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The conforming burst size is specified in kilobytes (KB) and is an integer from 1 to 128.

For each outcome, the only possible actions are drop, set-cos-as-sec-cos, set-cos-transmit, set-sec-cos-transmit, set-dscp-transmit, set-prec-transmit, or transmit. In this simple form of the **police** command, the conform action defaults to transmit and the violate action defaults to drop. These actions can be set with this command once the style has been configured.

For set-dscp-transmit, a `dscpval` value is required and is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

For set-prec-transmit, an IP Precedence value is required and is specified as an integer from 0-7.

For set-cos-transmit an 802.1p priority value is required and is specified as an integer from 0-7.

Format	`police-simple {`*`1-4294967295 1-128`* `conform-action {drop | set-cos-as-sec-cos | set-cos-transmit` *`0-7`* `| set-sec-cos-transmit` *`0-7`* `| set-prec-transmit` *`0-7`* `| set-dscp-transmit` *`0-63`* `| transmit} [violate-action {drop | set-cos-as-sec-cos | set-cos-transmit` *`0-7`* `| set-sec-cos-transmit` *`0-7`* `| set-prec-transmit` *`0-7`* `| set-dscp-transmit` *`0-63`* `| transmit}]}`
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark (all forms)

Example: The following shows an example of the command.

```
(Routing) (Config-policy-classmap)#police-simple 1 128 conform-action transmit violate-action drop
```

12.4.0.14 police-single-rate

This command is the single-rate form of the **police** command and is used to establish the traffic policing style for the specified class. For each outcome, the only possible actions are drop, set-cos-as-sec-cost, set-cos-transmit, set-sec-cos-transmit, set-dscp-transmit, set-prec-transmit, or transmit. In this single-rate form of the **police** command, the conform action defaults to send, the exceed action defaults to drop, and the violate action defaults to drop. These actions can be set with this command once the style has been configured.

Format `police-single-rate {`*`1-4294967295 1-128 1-128`* `conform-action {drop | set-cos-as-sec-cos | set-cos-transmit` *`0-7`* `| set-sec-cos-transmit` *`0-7`* `| set-prec-transmit` *`0-7`* `| set-dscp-transmit` *`0-63`* `| transmit} exceed-action {drop | set-cos-as-sec-cos | set-cos-transmit` *`0-7`* `| set-sec-cos-transmit` *`0-7`* `| set-prec-transmit` *`0-7`* `| set-dscp-transmit` *`0-63`* `| transmit} [violate-action {drop | set-cos-as-sec-cos-transmit | set-cos-transmit` *`0-7`* `| set-sec-cos-transmit` *`0-7`* `| set-prec-transmit` *`0-7`* `| set-dscp-transmit` *`0-63`* `| transmit}]}`

Mode Policy-Class-Map Config

12.4.0.15 police-two-rate

This command is the two-rate form of the **police** command and is used to establish the traffic policing style for the specified class. For each outcome, the only possible actions are drop, set-cos-as-sec-cos, set-cos-transmit, set-sec-cos-transmit, set-dscp-transmit, set-prec-transmit, or transmit. In this two-rate form of the **police** command, the conform action defaults to send, the exceed action defaults to drop, and the violate action defaults to drop. These actions can be set with this command once the style has been configured.

Format `police-two-rate {`*`1-4294967295 1-4294967295 1-128 1-128`* `conform-action {drop | set-cos-as-sec-cos | set-cos-transmit` *`0-7`* `| set-sec-cos-transmit` *`0-7`* `| set-prec-transmit` *`0-7`* `| set-dscp-transmit` *`0-63`* `| transmit} exceed-action {drop | set-cos-as-sec-cos | set-cos-transmit` *`0-7`* `| set-sec-cos-transmit` *`0-7`* `| set-prec-transmit` *`0-7`* `| set-dscp-transmit` *`0-63`* `| transmit} [violate-action {drop | set-cos-as-sec-cos | set-cos-transmit` *`0-7`* `| set-sec-cos-transmit` *`0-7`* `| set-prec-transmit` *`0-7`* `| set-dscp-transmit` *`0-63`* `| transmit}]}`

Mode Policy-Class-Map Config

12.4.0.16 policy-map

This command establishes a new DiffServ policy. The `policyname` parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy. The type of policy is specific to the inbound traffic direction as indicated by the in parameter.

NOTE: The CLI mode is changed to Policy-Map Config when this command is successfully executed.

Format `policy-map` *`policyname`* `in`

Mode Global Config

12.4.0.16.1 no policy-map

This command eliminates an existing DiffServ policy. The `policyname` parameter is the name of an existing DiffServ policy. This command may be issued at any time. If the policy is currently referenced by one or more interface service attachments, this delete attempt fails.

Format `no policy-map` *`policyname`*
Mode Global Config

12.4.0.17 policy-map rename

This command changes the name of a DiffServ policy. The `policyname` is the name of an existing DiffServ class. The `newpolicyname` parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy.

Format `policy-map rename` *`policyname newpolicyname`*
Mode Global Config

12.5 DiffServ Service Commands

Use the DiffServ service commands to assign a DiffServ traffic conditioning policy, which you specified by using the policy commands, to an interface in the incoming direction

The service commands attach a defined policy to a directional interface. You can assign only one policy at any one time to an interface in the inbound direction. DiffServ is not used in the outbound direction.

This set of commands consists of service addition/removal.

The CLI command root is `service-policy`.

12.5.0.1 service-policy

This command attaches a policy to an interface in the inbound direction. The `policyname` parameter is the name of an existing DiffServ policy. This command causes a service to create a reference to the policy.

NOTE: Note the following:

- This command effectively enables DiffServ on an interface in the inbound direction. There is no separate interface administrative 'mode' command for DiffServ.
- This command fails if any attributes within the policy definition exceed the capabilities of the interface. Once a policy is successfully attached to an interface, any attempt to change the policy definition, that would result in a violation of the interface capabilities, causes the policy change attempt to fail.

Format `service-policy in` *`policymapname`*

Modes
- Global Config
- Interface Config

NOTE: Each interface can have one policy attached.

12.5.0.1.1 no service-policy

This command detaches a policy from an interface in the inbound direction. The `policyname` parameter is the name of an existing DiffServ policy.

NOTE: This command causes a service to remove its reference to the policy. This command effectively disables DiffServ on an interface in the inbound direction. There is no separate interface administrative 'mode' command for DiffServ.

Format `no service-policy in` *`policymapname`*

Modes
- Global Config
- Interface Config

12.6 DiffServ Show Commands

Use the DiffServ show commands to display configuration and status information for classes, policies, and services. You can display DiffServ information in summary or detailed formats. The status information is only shown when the DiffServ administrative mode is enabled.

12.6.0.1 show class-map

This command displays all configuration information for the specified class. The `class-map-name` is the name of an existing DiffServ class.

Format `show class-map` *`class-map-name`*
Mode Privileged EXEC

If the class-name is specified the following fields are displayed:

Parameter	Definition
Class Map Name	A case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying a DiffServ class.
Class Type	A class type of all means every match criterion defined for the class is evaluated simultaneously and must all be true to indicate a class match.
Match Rule Count	Number of match rules configured for the class-map.
Match Criteria	The Match Criteria fields are only displayed if they have been configured. Not all platforms support all match criteria values. They are displayed in the order entered by the user. The fields are evaluated in accordance with the class type. The possible Match Criteria fields are: Destination IP Address, Destination Layer 4 Port, Destination MAC Address, Ethertype, Source MAC Address, VLAN, Class of Service, Every, IP DSCP, IP Precedence, IP TOS, Protocol Keyword, Reference Class, Source IP Address, and Source Layer 4 Port.
Values	The values of the Match Criteria.

If you do not specify the Class Name, this command displays a list of all defined DiffServ classes. The following fields are displayed:

Parameter	Definition
Class Name	The name of this class. (Note that the order in which classes are displayed is not necessarily the same order in which they were created.)
Class Type	A class type of all means every match criterion defined for the class is evaluated simultaneously and must all be true to indicate a class match.
ACL ID or Ref Class Name	The name of an existing DiffServ class whose match conditions are being referenced by the specified class definition or access-group name/ID.

12.6.0.2 show diffserv

This command displays the DiffServ General Status Group information, which includes the current administrative mode setting as well as the current and maximum number of rows in each of the main DiffServ private MIB tables. This command takes no options.

Format `show diffserv`
Mode Privileged EXEC

Parameter	Definition
DiffServ Admin mode	The current value of the DiffServ administrative mode.
Class Table Size	The current number of entries (rows) in the Class Table.
Class Table Max	The maximum allowed entries (rows) for the Class Table.
Class Rule Table Size	The current number of entries (rows) in the Class Rule Table.
Class Rule Table Max	The maximum allowed entries (rows) for the Class Rule Table.
Policy Table Size	The current number of entries (rows) in the Policy Table.
Policy Table Max	The maximum allowed entries (rows) for the Policy Table.
Policy Instance Table Size	Current number of entries (rows) in the Policy Instance Table.
Policy Instance Table Max	Maximum allowed entries (rows) for the Policy Instance Table.
Policy Attribute Table Size	Current number of entries (rows) in the Policy Attribute Table.
Policy Attribute Table Max	Maximum allowed entries (rows) for the Policy Attribute Table.
Service Table Size	The current number of entries (rows) in the Service Table.
Service Table Max	The maximum allowed entries (rows) for the Service Table.

12.6.0.3 show policy-map

This command displays all configuration information for the specified policy. The `policyname` is the name of an existing DiffServ policy.

Format `show policy-map` *`[policyname]`*
Mode Privileged EXEC

If the Policy Name is specified the following fields are displayed:

Parameter	Definition
Policy Name	The name of this policy.
Policy Type	The policy type (only inbound policy definitions are supported for this platform.)

The following information is repeated for each class associated with this policy (only those policy attributes actually configured are displayed):

Parameter	Definition
Assign Queue	Directs traffic stream to the specified QoS queue. This allows a traffic classifier to specify which one of the supported hardware queues are used for handling packets belonging to the class.
Class Name	The name of this class.
Committed Burst Size (KB)	The committed burst size, used in simple policing.
Committed Rate (Kbps)	The committed rate, used in simple policing.
Conform Action	The current setting for the action taken on a packet considered to conform to the policing parameters. This is not displayed if policing is not in use for the class under this policy.
Conform Color Mode	The current setting for the color mode. Policing uses either color blind or color aware mode. Color blind mode ignores the coloration (marking) of the incoming packet. Color aware mode takes into consideration the current packet marking when determining the policing outcome.
Conform COS	The CoS mark value if the conform action is set-cos-transmit.
Conform DSCP Value	The DSCP mark value if the conform action is set-dscp-transmit.

Parameter	Definition
Conform IP Precedence Value	The IP Precedence mark value if the conform action is set-prec-transmit.
Drop	Drop a packet upon arrival. This is useful for emulating access control list operation using DiffServ, especially when DiffServ and ACL cannot co-exist on the same interface.
Exceed Action	The action taken on traffic that exceeds settings that the network administrator specifies.
Exceed Color Mode	The current setting for the color of exceeding traffic that the user may optionally specify.
Mark CoS	The class of service value that is set in the 802.1p header of inbound packets. This is not displayed if the mark cos was not specified.
Mark CoS as Secondary CoS	The secondary 802.1p priority value (second/inner VLAN tag. Same as CoS (802.1p) marking, but the dot1p value used for remarking is picked from the dot1p value in the secondary (i.e. inner) tag of a double-tagged packet.
Mark IP DSCP	The mark/remark value used as the DSCP for traffic matching this class. This is not displayed if mark ip description is not specified.
Mark IP Precedence	The mark/remark value used as the IP Precedence for traffic matching this class. This is not displayed if mark ip precedence is not specified.
Mirror	Copies a classified traffic stream to a specified egress port (physical port or LAG). This can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment. This field does not display on Broadcom 5630x platforms.
Non-Conform Action	The current setting for the action taken on a packet considered to not conform to the policing parameters. This is not displayed if policing not in use for the class under this policy.
Non-Conform COS	The CoS mark value if the non-conform action is set-cos-transmit.
Non-Conform DSCP Value	The DSCP mark value if the non-conform action is set-dscp-transmit.
Non-Conform IP Precedence Value	The IP Precedence mark value if the non-conform action is set-prec-transmit.
Peak Rate	Guarantees a committed rate for transmission, but also transmits excess traffic bursts up to a user-specified peak rate, with the understanding that a downstream network element (such as the next hop's policer) might drop this excess traffic. Traffic is held in queue until it is transmitted or dropped (per type of queue depth management.) Peak rate shaping can be configured for the outgoing transmission stream for an AF (Assured Forwarding) traffic class (although average rate shaping could also be used.)
Peak Burst Size	(PBS). The network administrator can set the PBS as a means to limit the damage expedited forwarding traffic could inflict on other traffic (e.g., a token bucket rate limiter) Traffic that exceeds this limit is discarded.
Policing Style	The style of policing, if any, used (simple).
Redirect	Forces a classified traffic stream to a specified egress port (physical port or LAG). This can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment. This field does not display on Broadcom 5630x platforms.

If the Policy Name is not specified this command displays a list of all defined DiffServ policies. The following fields are displayed:

Parameter	Definition
Policy Name	The name of this policy. (The order in which the policies are displayed is not necessarily the same order in which they were created.)
Policy Type	The policy type (Only inbound is supported).
Class Members	List of all class names associated with this policy.

Example: The following shows example CLI display output including the mark-cos-as-sec-cos option specified in the policy action.

```
(Routing) #show policy-map p1
Policy Name..................................... p1
Policy Type..................................... In
Class Name...................................... c1
Mark CoS as Secondary CoS...................... Yes
```

Example: The following shows example CLI display output including the mark-cos-as-sec-cos action used in the policing (simple-police, police-single-rate, police two-rate) command.

```
(Routing) #show policy-map p2
Policy Name..................... p2
Policy Type..................... In
Class Name...................... c2
Policing Style.................. Police Two Rate
Committed Rate.................. 1
Committed Burst Size............ 1
Peak Rate....................... 1
Peak Burst Size................. 1
Conform Action.................. Mark CoS as Secondary CoS
Exceed Action................... Mark CoS as Secondary CoS
Non-Conform Action.............. Mark CoS as Secondary CoS
Conform Color Mode.............. Blind
Exceed Color Mode............... Blind
```

12.6.0.4 show diffserv service

This command displays policy service information for the specified interface and direction. The *slot/port* parameter specifies a valid *slot/port* number for the system.

Format `show diffserv service` *slot/port* `in`

Mode Privileged EXEC

Parameter	Definition
DiffServ Admin Mode	The current setting of the DiffServ administrative mode. An attached policy is only in effect on an interface while DiffServ is in an enabled mode.
Interface	*slot/port*
Direction	The traffic direction of this interface service.
Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface in the indicated direction.
Policy Details	Attached policy details, whose content is identical to that described for the show policy-map `policymapname` command (content not repeated here for brevity).

12.6.0.5 show diffserv service brief

This command displays all interfaces in the system to which a DiffServ policy has been attached. The inbound direction parameter is optional.

Format `show diffserv service brief [in]`

Mode Privileged EXEC

Parameter	Definition
DiffServ Mode	The current setting of the DiffServ administrative mode. An attached policy is only active on an interface while DiffServ is in an enabled mode.

The following information is repeated for interface and direction (only those interfaces configured with an attached policy are shown):

Parameter	Definition
Interface	*slot/port*
Direction	The traffic direction of this interface service.
OperStatus	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface in the indicated direction.

12.6.0.6 show policy-map interface

This command displays policy-oriented statistics information for the specified interface and direction. The *slot/port* parameter specifies a valid interface for the system.

NOTE: This command is only allowed while the DiffServ administrative mode is enabled.

Format `show policy-map interface {slot/port | lag lag-id} [in]`

Mode Privileged EXEC

Parameter	Definition
Interface	*The port or LAG associated with the policy.*
Direction	The traffic direction of this interface service.
Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface in the indicated direction.

The following information is repeated for each class instance within this policy:

Parameter	Definition
Class Name	The name of this class instance.
In Discarded Packets	A count of the packets discarded for this class instance for any reason due to DiffServ treatment of the traffic class.

12.6.0.7 show service-policy

This command displays a summary of policy-oriented statistics information for all interfaces in the specified direction.

Format `show service-policy [in | out]`

Mode Privileged EXEC

The following information is repeated for each interface and direction (only those interfaces configured with an attached policy are shown):

Parameter	Definition
Interface	*The interface associated with the service policy.*
Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface.

12.7 MAC Access Control List Commands

This section describes the commands you use to configure MAC Access Control List (ACL) settings. MAC ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to MAC ACLs:

- The maximum number of ACLs you can create is hardware dependent. The limit applies to all ACLs, regardless of type.
- The system supports only Ethernet II frame types.
- The maximum number of rules per MAC ACL is hardware dependent.
- For the Broadcom 5630x platform, if you configure an IP ACL on an interface, you cannot configure a MAC ACL on the same interface.

NOTE: EFOS supports ACL counters for MAC, IPv4, and IPv6 access lists. For information about how to enable the counters, see Section 12.8.0.2, access-list counters enable.

12.7.0.1 mac access-list extended

This command creates a MAC Access Control List (ACL) identified by `name`, consisting of classification fields defined for the Layer 2 header of an Ethernet frame. The `name` parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.

If a MAC ACL by this name already exists, this command enters Mac-Access-List config mode to allow updating the existing MAC ACL.

NOTE: The CLI mode changes to Mac-Access-List Config mode when you successfully execute this command.

Format	`mac access-list extended` *`name`*
Mode	Global Config

12.7.0.1.1 no mac access-list extended

This command deletes a MAC ACL identified by `name` from the system.

Format	`no mac access-list extended` *`name`*
Mode	Global Config

12.7.0.2 mac access-list extended rename

This command changes the name of a MAC Access Control List (ACL). The `name` parameter is the name of an existing MAC ACL. The `newname` parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.

This command fails if a MAC ACL by the name `newname` already exists.

Format	`mac access-list extended rename` *`name newname`*
Mode	Global Config

12.7.0.3 mac access-list resequence

Use this command to renumber the sequence numbers of the entries for specified MAC access list with the given increment value starting from a particular sequence number. The command is used to edit the sequence numbers of ACL rules in the ACL and change the order in which entries are applied. This command is not saved in startup configuration and is not displayed in running configuration.

NOTE: If the generated sequence number exceeds the maximum sequence number, the ACL rule creation fails and an informational message is displayed.

Default 10

Format `mac access-list resequence {name| id } starting-sequence-number increment`

Mode Global Config

Parameter	Description
starting-sequence-number	The sequence number from which to start. The range is 1–2147483647. The default is 10.
increment	The amount to increment. The range is 1–2147483647. The default is 10.

12.7.0.4 {deny | permit} (MAC ACL)

This command creates a new rule for the current MAC access list. A rule may either deny or permit traffic according to the specified classification fields. At a minimum, the source and destination MAC value must be specified, each of which may be substituted using the keyword any to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

Format `[sequence-number] {deny|permit} {srcmac | any} {dstmac | any} [ethertypekey | 0x0600-0xFFFF] [vlan {eq 0-4095}] [cos 0-7] [[log] [time-range time-range-name] [assign-queue queue-id]] [{mirror | redirect} slot/port][rate-limit rate burst-size] [sflow-remote-agent]`

Mode Mac-Access-List Config

NOTE: Note the following:

- An implicit **deny all** MAC rule always terminates the access list.
- For BCM5630x and BCM5650x based systems, assign-queue, redirect, and mirror attributes are configurable for a deny rule, but they have no operational effect.

The *sequence-number* specifies the sequence number for the ACL rule. The sequence number is specified by the user or is generated by device.

If a sequence number is not specified for the rule, a sequence number that is 10 greater than the last sequence number in ACL is used and this rule is placed in the end of the list. If this is the first ACL rule in the given ACL, a sequence number of 10 is assigned. If the calculated sequence number exceeds the maximum sequence number value, the ACL rule creation fails. A rule cannot be created that duplicates an already existing one and a rule cannot be configured with a sequence number that is already used for another rule.

For example, if user adds new ACL rule to ACL without specifying a sequence number, it is placed at the bottom of the list. By changing the sequence number, the user can move the ACL rule to a different position in the ACL.

The Ethertype may be specified as either a keyword or a four-digit hexadecimal value from 0x0600-0xFFFF. The currently supported *ethertypekey* values are: appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast, mplsucast, netbios, novell, pppoe, rarp. Each of these translates into its equivalent Ethertype value(s).

Table 17: Ethertype Keyword and 4-digit Hexadecimal Value

Ethertype Keyword	Corresponding Value
appletalk	0x809B
arp	0x0806
ibmsna	0x80D5
ipv4	0x0800
ipv6	0x86DD
ipx	0x8037
mplsmcast	0x8848
mplsucast	0x8847
netbios	0x8191
novell	0x8137, 0x8138
pppoe	0x8863, 0x8864
rarp	0x8035

The `vlan` and `cos` parameters refer to the VLAN identifier and 802.1p user priority fields, respectively, of the VLAN tag. For packets containing a double VLAN tag, this is the first (or outer) tag.

The `time-range` parameter allows imposing time limitation on the MAC ACL rule as defined by the parameter *time-range-name*. If a time range with the specified name does not exist and the MAC ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the MAC ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see Section 12.11, Time Range Commands for Time-Based ACLs.

The `assign-queue` parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed *queue-id* value is 0-(n-1), where n is the number of user configurable queues available for the hardware platform. The *assign-queue* parameter is valid only for a `permit` rule.

For the Broadcom 5650x platform, the *mirror* parameter allows the traffic matching this rule to be copied to the specified *slot/port*, while the redirect parameter allows the traffic matching this rule to be forwarded to the specified *slot/port*. The *assign-queue* and *redirect* parameters are only valid for a `permit` rule.

NOTE: Note the following:

- The *mirror* and *redirect* parameters are not available on the Broadcom 5630x platform.
- The special command form `{deny | permit} any any` is used to match all Ethernet layer 2 packets, and is the equivalent of the IP access list “match every” rule.

The **permit** command’s optional attribute `rate-limit` allows you to permit only the allowed rate of traffic as per the configured rate in Kb/s, and burst-size in kilobytes.

The `sflow-remote-agent` parameter configures the sFlow sampling action. This action, if configured, copies the packet matching the rule to the remote sFlow agent.

Example: The following shows an example of the command.

```
(Routing) (Config)#mac access-list extended mac1
(Routing) (Config-mac-access-list)#permit 00:00:00:00:aa:bb ff:ff:ff:ff:00:00 any rate-limit 32 16
(Routing) (Config-mac-access-list)#exit
```

12.7.0.4.1 no *sequence-number*

Use this command to remove the ACL rule with the specified sequence number from the ACL.

Format `no` *`sequence-number`*

Mode MAC-Access-List Config

12.7.0.5 mac access-group

This command either attaches a specific MAC Access Control List (ACL) identified by `name` to an interface or range of interfaces, or associates it with a VLAN ID, in a given direction. The `name` parameter must be the name of an existing MAC ACL.

An optional sequence number may be specified to indicate the order of this mac access list relative to other mac access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified mac access list replaces the currently attached mac access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

This command specified in 'Interface Config' mode only affects a single interface, whereas the 'Global Config' mode setting is applied to all interfaces. The VLAN keyword is only valid in the 'Global Config' mode. The 'Interface Config' mode command is only available on platforms that support independent per-port class of service queue configuration.

An optional *control-plane* is specified to apply the MAC ACL on CPU port. The control packets like BPDU are also dropped because of the implicit deny all rule added to the end of the list. To overcome this, permit rules must be added to allow the control packets.

NOTE: Note the following:

- The keyword *control-plane* is only available in Global Config mode.
- The availability of the `out` option is platform-dependent.

Format `mac access-group` *`name`* `{{`*`control-plane`*`|in|out} vlan` *`vlan-id`* `{in|out}} [sequence` *`1-4294967295`*`]`

Modes
- Global Config
- Interface Config

12.7.0.5.1 no mac access-group

This command removes a MAC ACL identified by `name` from the interface in a given direction.

Format `no mac access-group` *`name`* `{{`*`control-plane`*`|in|out} vlan` *`vlan-id`* `{in|out}}`

Modes
- Global Config
- Interface Config

12.7.0.6 remark

This command adds a new comment to the ACL rule.

Use the remark keyword to add comments (remarks) to ACL rule entries belonging to an IPv4, IPv6, MAC, or ARP ACL. Up to L7_ACL_MAX_RULES_PER_LIST*10 remarks per ACL and up to 10 remarks per ACL rule can be configured. Also, up to L7_ACL_MAX_RULES*2 remarks for all QOS ACLs(IPv4/IPv6/MAC) for device can be configured. The total length of the remark cannot exceed 100 characters. A remark can contain characters in the range A-Z, a-z, 0-9, and special characters like space, hyphen, underscore. Remarks are associated to the ACL rule that is immediately created after the remarks are created. If the ACL rule is removed, the associated remarks are also deleted. Remarks are shown only in `show running-config` and are not displayed in `show ip access-lists`.

Remarks can only be added before creating the rule. If a user creates up to 10 remarks, each of them is linked to the next created rule.

Default None

Format `remark` *`comment`*

Mode
- IPv4-Access-List Config
- IPv6-Access-List-Config
- MAC-Access-List Config
- ARP-Access-List Config

Example:

```
(Config)#arp access-list new
(Config-arp-access-list)#remark "test1"
(Config-arp-access-list)#permit ip host 1.1.1.1 mac host 00:01:02:03:04:05
(Config-arp-access-list)#remark "test1"
(Config-arp-access-list)#remark "test2"
(Config-arp-access-list)#remark "test3"
(Config-arp-access-list)#permit ip host 1.1.1.2 mac host 00:03:04:05:06:07
(Config-arp-access-list)#permit ip host 2.1.1.2 mac host 00:03:04:05:06:08
(Config-arp-access-list)#remark "test4"
(Config-arp-access-list)#remark "test5"
(Config-arp-access-list)#permit ip host 2.1.1.3 mac host 00:03:04:05:06:01
```

12.7.0.6.1 no remark

Use this command to remove a remark from an ACL access-list.

When the first occurrence of the remark in ACL is found, the remark is deleted. Repeated execution of this command with the same remark removes the remark from the next ACL rule that has the remark associated with it (if there is any rule configured with the same remark). If there are no more rules with this remark, an error message is displayed

If there is no such remark associated with any rule and such remark is among not associated remarks, it is removed.

Default None

Format `no remark` *`comment`*

Mode
- IPv4-Access-List Config
- IPv6-Access-List-Config
- MAC-Access-List Config
- ARP-Access-List Config

12.7.0.7 show mac access-lists

This command displays summary information for all Mac Access lists and ACL rule hit count of packets matching the configured ACL rule within an ACL. This counter value rolls-over on reaching the maximum value. There is a dedicated counter for each ACL rule. ACL counters do not interact with PBR counters.

For ACL with multiple rules, once a match occurs at any one specific rule, counters associated with this rule only get incremented (for example, consider an ACL with three rules, after matching rule two, counters for rule three would not be incremented).

For ACL counters, If an ACL rule is configured without RATE-LIMIT, the counter value is count of forwarded/discarded packets. (For example: For a burst of 100 packets, the Counter value is 100).

If the ACL rule is configured with RATE LIMIT, the counter value is the MATCHED packet count. If the sent traffic rate exceeds the configured limit, the counters still display matched packet count (despite getting dropped beyond the configured limit since match criteria is met) which would equal the sent rate. For example, if rate limit is set to 10 kbps and ‘matching’ traffic is sent at 100 kbps, counters reflect a 100 kbps value. If the sent traffic rate is less than the configured limit, counters display only the matched packet count. Either way, only the matched packet count is reflected in the counters, irrespective of whether they get dropped or forwarded. ACL counters do not interact with diffserv policies.

Use the access list name to display detailed information of a specific MAC ACL.

NOTE: The command output varies based on the match criteria configured within the rules of an ACL.

Format `show mac access-lists` *`[name]`*

Mode Privileged EXEC

Term	Definition
ACL Name	The user-configured name of the ACL.
ACL Counters	Identifies whether the ACL counters are enabled or disabled.
Interface(s)	The inbound or outbound interfaces to which the ACL is applied.
Sequence Number	The ordered rule number identifier defined within the MAC ACL.
Action	The action associated with each rule. The possible values are Permit or Deny.
Source MAC Address	The source MAC address for this rule.
Source MAC Mask	The source MAC mask for this rule.
Destination MAC Address	The destination MAC address for this rule.
Ethertype	The Ethertype keyword or custom value for this rule.
VLAN ID	The VLAN identifier value or range for this rule.
COS	The COS (802.1p) value for this rule.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	On Broadcom 5650x platforms, the unit/slot/port to which packets matching this rule are copied.
Redirect Interface	On Broadcom 5650x platforms, the *`slot/port`* to which packets matching this rule are forwarded.
sFlow Remote Agent	Indicates whether the sFlow sampling action is configured. This action, if configured, copies the packet matching the rule to the remote sFlow agent.
Time Range Name	Displays the name of the time-range if the MAC ACL rule has referenced a time range.
Rule Status	Status (Active/Inactive) of the MAC ACL rule.
Committed Rate	The committed rate defined by the rate-limit attribute.

Term	Definition
Committed Burst Size	The committed burst size defined by the rate-limit attribute.
ACL Hit Count	The ACL rule hit count of packets matching the configured ACL rule within an ACL.

Example: The following shows example CLI display output for the command.

```
(Routing) #show mac access-lists mac1

ACL Counters: Enabled
ACL Name: mac1

Outbound Interface(s): control-plane

Sequence Number: 10
Action.............................permit
Source MAC Address.................. 00:00:00:00:AA:BB
Source MAC Mask.....................FF:FF:FF:FF:00:00
Committed Rate......................32
Committed Burst Size................16
ACL hit count ......................0

Sequence Number: 25
Action.............................permit
Source MAC Address.................. 00:00:00:00:AA:BB
Source MAC Mask.....................FF:FF:FF:FF:00:00
Destination MAC Address............ 01:80:C2:00:00:00
Destination MAC Mask................00:00:00:FF:FF:FF
Ethertype...........................ipv6
VLAN................................36
CoS Value...........................7
Assign Queue........................4
Redirect Interface..................0/34
sflow-remote-agent..................TRUE
Committed Rate......................32
Committed Burst Size................16
ACL hit count ......................0
```

12.8 IP Access Control List Commands

This section describes the commands you use to configure IP Access Control List (ACL) settings. IP ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to IP ACLs:

- EFOS software does not support IP ACL configuration for IP packet fragments.
- The maximum number of ACLs you can create is hardware dependent. The limit applies to all ACLs, regardless of type.
- The maximum number of rules per IP ACL is hardware dependent.
- On Broadcom 5630x platforms, if you configure a MAC ACL on an interface, you cannot configure an IP ACL on the same interface.
- Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address, and has zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has (0's) in a bit position that must be checked. A **1** in a bit position of the ACL mask indicates the corresponding bit can be ignored.

12.8.0.1 access-list

This command creates an IP Access Control List (ACL) that is identified by the access list number, which is 1-99 for standard ACLs or 100-199 for extended ACLs. Table 18, ACL Command Parameters describes the parameters for the `access-list` command.

IP Standard ACL:

Format `access-list` ***1-99*** `{remark` ***comment***`} | {[`***sequence-number***`]} [rule` ***1-1023***`] {deny | permit} {every | ***srcip srcmask*** } [log] [time-range` ***time-range-name***`][assign-queue` ***queue-id***`] [{mirror | redirect} slot/port] [redirectExtAgent` ***agent-id***`] [rate-limit` ***rate burst-size***`]`

Mode Global Config

IP Extended ACL:

Format `access-list` ***100-199*** `{remark` ***comment***`} | {[`***sequence-number***`]} [rule` ***1-1023***`]{deny | permit } {every | {{eigrp| gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp |` ***0–255*** `} {`***srcip*** `srcmask|any|host` ***srcip***`}[range {`***portkey***`|`***startport***`} {`***portkey***`|`***endport***`} {eq|neq|lt|gt} {`***portkey***`|`***0-65535***`}{`***dstip dstmask***`|any|host` ***dstip***`}[{range {`***portkey***`|`***startport***`} {`***portkey***`|`***endport***`} | {eq | neq | lt | gt} {`***portkey*** `|` ***0-65535***`} ] [flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]] [icmp-type` ***icmp-type*** `[icmp-code` ***icmp-code***`] | icmp-message` ***icmp-message***`] [igmp-type` ***igmp-type***`] [fragments] [precedence` ***precedence*** `| tos` ***tos*** `[ tosmask] | dscp` ***dscp***`]}} [time-range` ***time-range-name***`] [log] [assign-queue` ***queue-id***`] [{mirror | redirect}` ***slot/port***`] [rate-limit` ***rate burst-size***`] [sflow-remote-agent]`

Mode Global Config

NOTE: IPv4 extended ACLs have the following limitations for egress ACLs:

- Match on port ranges is not supported.
- The rate-limit command is not supported.

Table 18: ACL Command Parameters

Parameter	Description
`remark` *`comment`*	Use the remark keyword to add a comment (remark) to an IP standard or IP extended ACL. The remarks make the ACL easier to understand and scan. Each remark is limited to 100 characters. A remark can consist of characters in the range A-Z, a-z, 0-9, and special characters: space, hyphen, underscore. Remarks are displayed only in show running configuration. One remark per rule can be added for IP standard or IP extended ACL. User can remove only remarks that are not associated with a rule. Remarks associated with a rule are removed when the rule is removed
`sequence-number`	Specifies a sequence number for the ACL rule. Every rule receives a sequence number. A sequence number is specified by the user or is generated by the device. If a sequence number is not specified for the rule, a sequence number that is 10 greater than the last sequence number in the ACL is used and this rule is located in the end of the list. If this is the first ACL rule in the given ACL, a sequence number of 10 is assigned. If the calculated sequence number exceeds the maximum sequence number value, the ACL rule creation fails. It is not allowed to create a rule that duplicates an already existing one and a rule cannot be configured with a sequence number that is already used for another rule. For example, if user adds new ACL rule to ACL without specifying a sequence number, it is placed at the bottom of the list. By changing the sequence number, user can move the ACL rule to a different position in the ACL.
`1-99` `or` *`100-199`*	Range 1 to 99 is the access list number for an IP standard ACL. Range 100 to 199 is the access list number for an IP extended ACL.
`[rule` *`1-1023`*`]`	Specifies the IP access list rule.
`{deny | permit}`	Specifies whether the IP ACL rule permits or denies an action. **NOTE:** For 5630x and 5650x-based systems, assign-queue, redirect, and mirror attributes are configurable for a deny rule, but they have no operational effect.
`every`	Match every packet.
`{eigrp | gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp |` *`0-255`*`}`	Specifies the protocol to filter for an extended IP ACL rule.
`srcip srcmask``|any|host` *`scrip`*	Specifies a source IP address and source netmask for match condition of the IP ACL rule. Specifying any specifies *srcip* as 0.0.0.0 and *srcmask* as 255.255.255.255. Specifying host *A.B.C.D* specifies *srcip* as A.B.C.D and *srcmask* as 0.0.0.0.

Table 18: ACL Command Parameters (Continued)

Parameter	Description
{{range{portkey|startport}{portkey|endport}|{eq|neq|lt|gt} {*portkey* | *0-65535*}*]*	**NOTE:** This option is available only if the protocol is TCP or UDP. Specifies the source layer 4 port match condition for the IP ACL rule. You can use the port number, which ranges from 0-65535, or you specify the *portkey*, which can be one of the following keywords: ■ For TCP: *bgp*, *domain*, *echo*, *ftp*, *ftp-data*, *http*, *smtp*, *telnet*, *www*, *pop2*, *pop3*. ■ For UDP: *domain, echo, ntp, rip, snmp, tftp*, *time*, and *who*. For both TCP and UDP, each of these keywords translates into its equivalent port number, which is used as both the start and end of a port range. If *range* is specified, the IP ACL rule matches only if the layer 4 port number falls within the specified portrange. The *startport* and *endport* parameters identify the first and last ports that are part of the port range. They have values from 0 to 65535. The ending port must have a value equal or greater than the starting port. The starting port, ending port, and all ports in between will be part of the layer 4 port range. When *eq* is specified, the IP ACL rule matches only if the layer 4 port number is equal to the specified port number or portkey. When *lt* is specified, IP ACL rule matches if the layer 4 port number is less than the specified port number or portkey. It is equivalent to specifying the range as 0 to <specified port number – 1>. When *gt* is specified, the IP ACL rule matches if the layer 4 port number is greater than the specified port number or portkey. It is equivalent to specifying the range as <specified port number + 1> to 65535. When *neq* is specified, IP ACL rule matches only if the layer 4 port number is not equal to the specified port number or portkey. Two rules are added in the hardware one with range equal to 0 to <specified port number _- 1> and one with range equal to <<specified port number _+ 1 to 65535>> **Note:** Port number matches only apply to unfragmented or first fragments.
dstip dstmask|any|host *dstip*	Specifies a destination IP address and netmask for match condition of the IP ACL rule. Specifying any implies specifying *dstip* as 0.0.0.0 and *dstmask* as 255.255.255.255. Specifying host A.B.C.D implies *dstip* as A.B.C.D and *dstmask* as 0.0.0.0.
[precedence *precedence* | tos *tos* [*tosmask*] | dscp *dscp*]	Specifies the TOS for an IP ACL rule depending on a match of precedence or DSCP values using the parameters *dscp, precedence*, *tos/tosmask*. **NOTE:** *tosmask* is an optional parameter.
flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]	**NOTE:** This option is available only if the protocol is tcp. Specifies that the IP ACL rule matches on the TCP flags. When +<tcpflagname> is specified, a match occurs if the specified <tcpflagname> flag is set in the TCP header. When -<tcpflagname> is specified, a match occurs if the specified <tcpflagname> flag is *NOT* set in the TCP header. When established is specified, a match occurs if the specified RST or ACK bits are set in the TCP header. Two rules are installed in the hardware when the established option is specified.

Table 18: ACL Command Parameters (Continued)

Parameter	Description
`[icmp-type` *`icmp-type`* `[icmp-code` *`icmp-code`*`] | icmp-message` *`icmp-message`*`]`	**NOTE:** This option is available only if the protocol is icmp. Specifies a match condition for ICMP packets. When *icmp-type* is specified, the IP ACL rule matches on the specified ICMP message type, a number from 0 to 255. When *icmp-code* is specified, the IP ACL rule matches on the specified ICMP message code, a number from 0 to 255. Specifying *icmp-message* implies that both *icmp-type* and *icmp-code* are specified. The following icmp-messages are supported: *echo*, *echo-reply*, *host-redirect*, *mobile-redirect*, *net-redirect*, *net-unreachable*, *redirect*, *packet-too-big*, *port-unreachable*, *source-quench*, *router-solicitation*, *router-advertisement*, *time-exceeded*, *ttl-exceeded* and *unreachable*.
`igmp-type` *`igmp-type`*	This option is available only if the protocol is igmp. When *igmp-type* is specified, the IP ACL rule matches on the specified IGMP message type, a number from 0 to 255.
`fragments`	Specifies that the IP ACL rule matches on fragmented IP packets.
`[log]`	Specifies that this rule is to be logged.
`[time-range` *`time-range-name`*`]`	Allows imposing time limitation on the ACL rule as defined by the parameter *time-range-name*. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see Section 12.11, Time Range Commands for Time-Based ACLs.
`[assign-queue` *`queue-id`*`]`	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned.
`[{mirror | redirect}` *`slot/port`*`]`	For Broadcom 5650x platforms, specifies the mirror or redirect interface which is the *`slot/port`* to which packets matching this rule are copied or forwarded, respectively. The *`mirror`* and *`redirect`* parameters are not available on the Broadcom 5630x platform.
`[rate-limit` *`rate burst-size`*`]`	Specifies the allowed rate of traffic as per the configured rate in Kb/s, and burst-size in kilobytes.
`[sflow-remote-agent]`	Configures the sFlow sampling action. This action, if configured, copies the packet matching the rule to the remote sFlow agent.

12.8.0.1.1 no access-list

This command deletes an IP ACL that is identified by the parameter `accesslistnumber` from the system. The range for `accesslistnumber` 1-99 for standard access lists and 100-199 for extended access lists.

Format `no access-list` *`accesslistnumber`* `[rule` *`1-1023`*`]`

Mode Global Config

12.8.0.2 access-list counters enable

Use this command to enable ACL counters for IPv4, IPv6 and MAC access lists.

Default	Enabled
Format	`access-list` *`counters enable`*
Mode	Global Config

12.8.0.2.1 no access-list counters enable

Use this command to disable ACL counters for IPv4, IPv6 and MAC access lists.

Format	`no access-list` *`counters enable`*
Mode	Global Config

12.8.0.3 ip access-list

This command creates an extended IP Access Control List (ACL) identified by *name*, consisting of classification fields defined for the IP header of an IPv4 frame. The *name* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.

If an IP ACL by this name already exists, this command enters IPv4-Access_List config mode to allow updating the existing IP ACL.

NOTE: The CLI mode changes to IPv4-Access-List Config mode when you successfully execute this command.

Format	`ip access-list` *`name`*
Mode	Global Config

12.8.0.3.1 no ip access-list

This command deletes the IP ACL identified by name from the system.

Format	`no ip access-list` *`name`*
Mode	Global Config

12.8.0.4 ip access-list rename

This command changes the name of an IP Access Control List (ACL). The *name* parameter is the names of an existing IP ACL. The `newname` parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.

This command fails is an IP ACL by the name `newname` already exists.

Format	`ip access-list rename` *`name newname`*
Mode	Global Config

12.8.0.5 ip access-list resequence

Use this command to renumber the sequence numbers of the entries for specified IP access list with the given increment value starting from a particular sequence number. The command is used to edit the sequence numbers of ACL rules in the ACL and change the order in which entries are applied. This command is not saved in startup configuration and is not displayed in running configuration.

NOTE: If the generated sequence number exceeds the maximum sequence number, the ACL rule creation fails and an informational message is displayed.

Default 10

Format `ip access-list resequence {name| id } starting-sequence-number increment`

Mode Global Config

Parameter	Description
starting-sequence-number	The sequence number from which to start. The range is 1–2147483647. The default is 10.
increment	The amount to increment. The range is 1–2147483647. The default is 10.

12.8.0.6 {deny | permit} (IP ACL)

This command creates a new rule for the current IP access list. A rule may either deny or permit traffic according to the specified classification fields. At a minimum, either the every keyword or the protocol, source address, and destination address values must be specified. The source and destination IP address fields may be specified using the keyword `any` to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

Format `[sequence-number] {deny | permit} {every | {{eigrp | gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp | 0-255} {srcip srcmask | any | host srcip} [{range {portkey | startport} {portkey | endport} | {eq | neq | lt | gt} {portkey | 0-65535}] {dstip dstmask | any | host dstip} [{range {portkey | startport} {portkey | endport} | {eq | neq | lt | gt} {portkey | 0-65535}] [flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]] [icmp-type icmp-type [icmp-code icmp-code] | icmp-message icmp-message] [igmp-type igmp-type] [fragments] [precedence precedence | tos tos [tosmask] | dscp dscp] | [ttl eq 0-255]}} [time-range time-range-name] [log] [assign-queue queue-id] [{mirror | redirect} slot/port] [rate-limit rate burst-size] [sflow-remote-agent]`

Mode Ipv4-Access-List Config

NOTE: Note the following:

- An implicit **deny all** IP rule always terminates the access list.
- For BCM5630x-based systems, the *mirror* and *redirect* parameters are not available.
- For BCM5650x-based systems, the *mirror* parameter allows the traffic matching this rule to be copied to the specified *slot/port*, while the redirect parameter allows the traffic matching this rule to be forwarded to the specified *slot/port*. The *assign-queue* and *redirect* parameters are only valid for a `permit` rule.
- For IPv4, the following are not supported for egress ACLs: a match on port ranges, the rate-limit command.

The `time-range` parameter allows imposing time limitation on the IP ACL rule as defined by the specified time range. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see Section 12.11, Time Range Commands for Time-Based ACLs.

The `assign-queue` parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed *`queue-id`* value is 0-(n-1), where n is the number of user configurable queues available for the hardware platform. The *`assign-queue`* parameter is valid only for a `permit` rule.

The **permit** command's optional attribute **rate-limit** allows you to permit only the allowed rate of traffic as per the configured rate in kbps, and burst-size in kbytes.

Parameter	Description
sequence-number	The *sequence-number* specifies the sequence number for the ACL rule. The sequence number is specified by the user or is generated by device. If a sequence number is not specified for the rule, a sequence number that is 10 greater than the last sequence number in ACL is used and this rule is placed at the end of the list. If this is the first ACL rule in the given ACL, a sequence number of 10 is assigned. If the calculated sequence number exceeds the maximum sequence number value, the ACL rule creation fails. A rule cannot be created that duplicates an already existing one and a rule cannot be configured with a sequence number that is already used for another rule. For example, if user adds new ACL rule to ACL without specifying a sequence number, it is placed at the bottom of the list. By changing the sequence number, the user can move the ACL rule to a different position in the ACL.
{deny | permit}	Specifies whether the IP ACL rule permits or denies the matching traffic.
Every	Match every packet.
{`eigrp` | `gre` | `icmp` | `igmp` | `ip` | `ipinip` | `ospf` | `pim` | `tcp` | `udp` | *`0 -255`*}	Specifies the protocol to match for the IP ACL rule.
srcip srcmask | any | host *srcip*	Specifies a source IP address and source netmask to match for the IP ACL rule. Specifying "any" implies specifying *srcip* as "0.0.0.0" and *srcmask* as "255.255.255.255". Specifying "host A.B.C.D" implies *srcip* as "A.B.C.D" and *srcmask* as "0.0.0.0".

Parameter	Description
[{range {*portkey* | *startport*} {*portkey* | *endport*} | {eq | neq | lt | gt} {*portkey* | *0-65535*}]	**NOTE:** This option is available only if the protocol is tcp or udp. Specifies the layer 4 port match condition for the IP ACL rule. Port number can be used, which ranges from 0-65535, or the portkey, which can be one of the following keywords: ■ For tcp protocol: bgp, domain, echo, ftp, ftp-data, http, smtp, telnet, www, pop2, pop3 ■ For udp protocol: domain, echo, ntp, rip, snmp, tftp, time, who Each of these keywords translates into its equivalent port number. When range is specified, the IP ACL rule matches only if the layer 4 port number falls within the specified port range. The startport and endport parameters identify the first and last ports that are part of the port range. They have values from 0 to 65535. The ending port must have a value equal to or greater than the starting port. The starting port, ending port, and all ports in between will be part of the layer 4 port range. When eq is specified, IP ACL rule matches only if the layer 4 port number is equal to the specified port number or portkey. When lt is specified, IP ACL rule matches if the layer 4 port number is less than the specified port number or portkey. It is equivalent to specifying the range as 0 to <specified port number – 1>. When gt is specified, IP ACL rule matches if the layer 4 port number is greater than the specified port number or portkey. It is equivalent to specifying the range as <specified port number + 1> to 65535. When neq is specified, IP ACL rule matches only if the layer 4 port number is not equal to the specified port number or port key. Two rules are added in the hardware one with range equal to 0 to <specified port number _- 1> and one with range equal to <<specified port number _+ 1 to 65535>>. **NOTE:** Port number matches only apply to unfragmented or first fragments.
dstip dstmask | any | host *dstip*	Specifies a destination IP address and netmask for match condition of the IP ACL rule. Specifying any implies specifying dstip as 0.0.0.0 and dstmask as 255.255.255.255. Specifying host A.B.C.D implies dstip as A.B.C.D and dstmask as 0.0.0.0.
[precedence *precedence* | tos *tos* [*tosmask*] | dscp *dscp*]	Specifies the TOS for an IP ACL rule depending on a match of precedence or DSCP values using the parameters *dscp, precedence*, *tos/tosmask.* tosmask is an optional parameter.
flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]	Specifies that the IP ACL rule matches on the tcp flags. When +<tcpflagname> is specified, a match occurs if specified <tcpflagname> flag is set in the TCP header. When -<tcpflagname> is specified, a match occurs if specified <tcpflagname> flag is NOT set in the TCP header. When established is specified, a match occurs if either the specified RST or ACK bits are set in the TCP header. Two rules are installed in hardware to when the established option is specified. This option is available only if protocol is tcp.

Parameter	Description
[icmp-type *icmp-type* [icmp-code *icmp-code*] | icmp-message *icmp-message*]	**NOTE:** This option is available only if the protocol is ICMP. Specifies a match condition for ICMP packets. When *icmp-type* is specified, IP ACL rule matches on the specified ICMP message type, a number from 0 to 255. When *icmp-code* is specified, IP ACL rule matches on the specified ICMP message code, a number from 0 to 255. Specifying *icmp-message* implies both *icmp-type* and *icmp-code* are specified. The following icmp-messages are supported: echo, echo-reply, host-redirect, mobile-redirect, net-redirect, net-unreachable, redirect, packet-too-big, port-unreachable, source-quench, router-solicitation, router-advertisement, time-exceeded, ttl-exceeded and unreachable. The ICMP message is decoded into corresponding ICMP type and ICMP code within that ICMP type.
igmp-type *igmp-type*	**NOTE:** This option is visible only if the protocol is IGMP. When *igmp-type* is specified, the IP ACL rule matches on the specified IGMP message type, a number from 0 to 255.
fragments	Specifies that IP ACL rule matches on fragmented IP packets.
`ttl eq`	Specifies that the IP ACL rule matches on packets with the specified Time To Live (TTL) value.
log	Specifies that this rule is to be logged.
time-range *time-range-name*	Allows imposing a time limitation on the ACL rule as defined by the parameter time-range-name. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, the ACL rule is applied immediately. If a time range with specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive.
assign-queue *queue-id*	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned.
{mirror | redirect} *unit/slot/ port*	Specifies the mirror or redirect interface which is the unit/slot/port to which packets matching this rule are copied or forwarded, respectively.
rate-limit *rate burst-size*	Specifies the allowed rate of traffic as per the configured rate in Kb/s, and burst-size in kilobytes.
sflow-remote-agent	Configures the sFlow sampling action. This action, if configured, copies the packet matching the rule to the remote sFlow agent.

12.8.0.6.1 no *sequence-number*

Use this command to remove the ACL rule with the specified sequence number from the ACL.

Format `no sequence-number`

Mode Ipv4-Access-List Config

12.8.0.7 ip access-group

This command either attaches a specific IP ACL identified by `accesslistnumber` to an interface (including VLAN routing interfaces), range of interfaces, or all interfaces; or associates it with a VLAN ID in a given direction. The parameter `name` is the name of the Access Control List.

An optional sequence number may be specified to indicate the order of this IP access list relative to other IP access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached IP access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

An optional *control-plane* is specified to apply the ACL on CPU port. The IPv4 control packets like RADIUS and TACACS+ are also dropped because of the implicit **deny all** rule added at the end of the list. To overcome this, permit rules must be added to allow the IPv4 control packets.

NOTE: Note the following:

- The keyword *control-plane* is only available in Global Config mode.
- The `out` option may or may not be available, depending on the platform.

Default none

Format `ip access-group {`*`accesslistnumber`*`|`*`name`*`} {{`*`control-plane`*`|`*`in`*`|`*`out`*`}|vlan `*`vlan-id`*` {in|out}} [sequence `*`1-4294967295`*`]`

Modes
- Interface Config
- Global Config

12.8.0.7.1 no ip access-group

This command removes a specified IP ACL from an interface.

Default none

Format `no ip access-group {`*`accesslistnumber`*`|`*`name`*`} {{`*`control-plane`*`|`*`in`*`|`*`out`*`}|vlan `*`vlan-id`* `{in|out}}`

Mode
- Interface Config
- Global Config

12.8.0.8 acl-trapflags

This command enables the ACL trap mode.

Default disabled

Format `acl-trapflags`

Mode Global Config

12.8.0.8.1 no acl-trapflags

This command disables the ACL trap mode.

Format `no acl-trapflags`

Mode Global Config

12.8.0.9 show ip access-lists

Use this command to view summary information about all IP ACLs configured on the switch. To view more detailed information about a specific access list, specify the ACL number or name that is used to identify the IP ACL. For ACL with multiple rules, once a match occurs at any one specific rule, counters associated with this rule only get incremented for example, consider an ACL with three rules, after matching rule two, counters for rule three would not be incremented).

For ACL counters, if an ACL rule is configured without RATE-LIMIT, the counter value is count of forwarded/discarded packets (for example: If burst of 100 packets sent from IXIA, the Counter value is 100).

If an ACL rule is configured with RATE LIMIT, the counter value will be the MATCHED packet count. If the sent traffic rate exceeds the configured limit, counters will still display matched packet count (despite getting dropped beyond the configured limit since match criteria is met) that would equal the sent rate. For example, if rate limit is set to 10 kbps and 'matching' traffic is sent at 100 Kb/s, counters would reflect 100 Kb/s value. If the sent traffic rate is less than the configured limit, counters would display only matched packet count. Either way, only matched packet count is reflected in the counters, irrespective of whether they get dropped or forwarded. ACL counters do not interact with DiffServ policies.

Format `show ip access-lists [`*`accesslistnumber`* `|` *`name`*`]`

Mode Privileged EXEC

Parameter	Definition
ACL Counters	Shows whether ACL counters are enabled or disabled.
Current number of ACLs	The number of ACLs of any type currently configured on the system.
Maximum number of ACLs	The maximum number of ACLs of any type that can be configured on the system.
ACL ID/Name	Identifies the configured ACL number or name.
Rules	Identifies the number of rules configured for the ACL.
Direction	Shows whether the ACL is applied to traffic coming into the interface (ingress) or leaving the interface (egress).
Interface(s)	Identifies the interface(s) to which the ACL is applied (ACL interface bindings).
VLAN(s)	Identifies the VLANs to which the ACL is applied (ACL VLAN bindings).
redirectExtAgent	Indicates whether matching flow packets are allowed to be sent to external applications running alongside EFOS on a control CPU. agent-id is a unique identifier for the external receive client application. agent-id is an integer in the range 1 to 100. The `redirectExtAgent` action is mutually exclusive with the `redirect` and `mirror` actions.

If you specify an IP ACL number or name, the following information displays:

NOTE: Only the access list fields that you configure are displayed.

Parameter	Definition
ACL ID	The user-configured ACL identifier.
ACL Counters	Identifies whether the ACL counters are enabled or disabled.
Interface(s)	The inbound or outbound interfaces to which the ACL is applied.
Sequence Number	The number identifier for each rule that is defined for the IP ACL.
Action	The action associated with each rule. The possible values are Permit or Deny.
Match All	Indicates whether this access list applies to every packet. Possible values are True or False.
Protocol	The protocol to filter for this rule.

Parameter	Definition
Source IP Address	The source IP address for this rule.
Source IP Mask	The source IP Mask for this rule.
Source L4 Port Keyword	The source port for this rule.
Destination IP Address	The destination IP address for this rule.
Destination IP Mask	The destination IP Mask for this rule.
Destination L4 Port Keyword	The destination port for this rule.
IP DSCP	The value specified for IP DSCP.
IP Precedence	The value specified IP Precedence.
IP TOS	The value specified for IP TOS.
Fragments	Specifies whether the IP ACL rule matches on fragmented IP packets is enabled.
sFlow Remote Agent	Indicates whether the sFlow sampling action is configured. This action, if configured, copies the packet matching the rule to the remote sFlow agent.
TTL Field Value	The value specified for the TTL.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	The slot/port to which packets matching this rule are copied.
Redirect Interface	The slot/port to which packets matching this rule are forwarded.
Time Range Name	Displays the name of the time-range if the IP ACL rule has referenced a time range.
redirectExtAgent	Indicates whether matching flow packets are allowed to be sent to external applications running alongside EFOS on a control CPU. agent-id is a unique identifier for the external receive client application. agent-id is an integer in the range 1 to 100. The `redirectExtAgent` action is mutually exclusive with the `redirect` and `mirror` actions.
Committed Rate	The committed rate defined by the rate-limit attribute.
Committed Burst Size	The committed burst size defined by the rate-limit attribute.
Rule Status	Status (Active/Inactive) of the IP ACL rule.
ACL Hit Count	The ACL rule hit count of packets matching the configured ACL rule within an ACL.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ip access-lists ip1

ACL Name: ip1
ACL Counters: Enabled
Inbound Interface(s): 0/30


Sequence Number: 1
Action..................................... permit
Match All.................................. FALSE
Protocol................................... 1(icmp)
ICMP Type.....................................3(Destination Unreachable)
Starting Source L4 port.....................80
Ending Source L4 port.......................85
Starting Destination L4 port................180
Ending Destination L4 port..................185
ICMP Code...................................0
Fragments...................................FALSE
sflow-remote- agent........................ TRUE
Committed Rate............................. 32
Committed Burst Size....................... 16
```

```
ACL hit count ..................................0
```

12.8.0.10 show access-lists

This command displays IP ACLs, IPv6 ACLs, and MAC access control lists information for a designated interface and direction. Use the **control-plane** keyword to display the ACLs applied on the CPU port.

Format `show access-lists interface {{slot/port | lag lag-id} in|out | control-plane}`

Mode Privileged EXEC

Parameter	Definition
ACL Type	Type of access list (IP, IPv6 or MAC).
ACL ID	Access List name for a MAC or IPv6 access list or the numeric identifier for an IP access list.
Sequence Number	An optional sequence number may be specified to indicate the order of this access list relative to other access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not specified by the user, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used. Valid range is (1 to 4294967295).
in|out	■ in – Display Access List information for a particular interface and the in direction. ■ out – Display Access List information for a particular interface and the out direction.

12.8.0.11 show access-lists vlan

This command displays Access List information for a particular VLAN ID.

Format `show access-lists vlan vlan-id {in | out}`

Mode Privileged EXEC

Parameter	Description
vlan-id	A VLAN ID.
in|out	■ in – Display Access List information for a particular VLAN ID and the in direction. ■ out – Display Access List information for a particular VLAN ID and the out direction.

12.9 IPv6 Access Control List Commands

This section describes the commands you use to configure IPv6 Access Control List (ACL) settings. IPv6 ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to IPv6 ACLs:

- The maximum number of ACLs you create is 100, regardless of type.
- The system supports only Ethernet II frame types.
- The maximum number of rules per IPv6 ACL is hardware dependent.

NOTE: EFOS supports ACL counters for MAC, IPv4, and IPv6 access lists. For information about how to enable the counters, see Section 12.8.0.2, access-list counters enable.

12.9.0.1 ipv6 access-list

This command creates an IPv6 Access Control List (ACL) identified by *name*, consisting of classification fields defined for the IP header of an IPv6 frame. The *name* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IPv6 access list.

If an IPv6 ACL by this name already exists, this command enters IPv6-Access-List config mode to allow updating the existing IPv6 ACL.

NOTE: The CLI mode changes to IPv6-Access-List Config mode when you successfully execute this command.

Format	`ipv6 access-list` *name*
Mode	Global Config

12.9.0.1.1 no ipv6 access-list

This command deletes the IPv6 ACL identified by *name* from the system.

Format	`no ipv6 access-list` *name*
Mode	Global Config

12.9.0.2 ipv6 access-list rename

This command changes the name of an IPv6 ACL. The *name* parameter is the name of an existing IPv6 ACL. The *newname* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IPv6 access list.

This command fails is an IPv6 ACL by the name *newname* already exists.

Format	`ipv6 access-list rename` *name newname*
Mode	Global Config

12.9.0.3 ipv6 access-list resequence

Use this command to renumber the sequence numbers of the entries for specified IPv6 access list with the given increment value starting from a particular sequence number. The command is used to edit the sequence numbers of ACL rules in the ACL and change the order in which entries are applied. This command is not saved in startup configuration and is not displayed in running configuration.

NOTE: If the generated sequence number exceeds the maximum sequence number, the ACL rule creation fails and an informational message is displayed.

Default 10

Format `ipv6 access-list resequence {name| id } starting-sequence-number increment`

Mode Global Config

Parameter	Description
starting-sequence-number	The sequence number from which to start. The range is 1–2147483647. The default is 10.
increment	The amount to increment. The range is 1–2147483647. The default is 10.

12.9.0.4 {deny | permit} (IPv6)

This command creates a new rule for the current IPv6 access list. A rule may either deny or permit traffic according to the specified classification fields. At a minimum, either the *every* keyword or the protocol, source address, and destination address values must be specified. The source and destination IPv6 address fields may be specified using the keyword *any* to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

Format `{deny | permit} {every | {{icmpv6 | ipv6 | tcp | udp | 0-255} {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [{range {portkey | startport} {portkey | endport} | {eq | neq | lt | gt} {portkey | 0-65535}] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address} [{range {portkey | startport} {portkey | endport} | {eq | neq | lt | gt} {portkey | 0-65535}] [flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]] [flow-label value] [icmp-type icmp-type [icmp-code icmp-code] | icmp-message icmp-message] [routing] [fragments] [sequence sequence-number] [dscp dscp]}} [log] [assign-queue queue-id] [{mirror | redirect} slot/port] [rate-limit rate burst-size] [sflow-remote-agent]`

Mode IPv6-Access-List Config

NOTE: An implicit **deny all IPv6** rule always terminates the access list.

The `time-range` parameter allows imposing time limitation on the IPv6 ACL rule as defined by the parameter *time-range-name*. If a time range with the specified name does not exist and the IPv6 ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the IPv6 ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive. For information about configuring time ranges, see Section 12.11, Time Range Commands for Time-Based ACLs.

The assign-queue parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed *queue-id* value is 0-(n-1), where *n* is the number of user configurable queues available for the hardware platform. The *assign-queue* parameter is valid only for a permit rule.

For the Broadcom 5650x platform, the *mirror* parameter allows the traffic matching this rule to be copied to the specified *slot/port*, while the redirect parameter allows the traffic matching this rule to be forwarded to the specified *slot/port*. The *assign-queue* and *redirect* parameters are only valid for a `permit` rule.

NOTE: The *mirror* and *redirect* parameters are not available on the Broadcom 5630x platform.

The **permit** command's optional attribute **rate-limit** allows you to permit only the allowed rate of traffic as per the configured rate in kbps, and burst-size in kbytes.

IPv6 ACLs have the following limitations:

- Port ranges are not supported for egress IPv6 ACLs.
- For the BCM5684X and BCM5685x platforms, The IPv6 ACL routing keyword is not supported when an IPv6 address is specified.
- For the BCM5684X, BCM5685x, and BCM5644X platforms, the IPv6 ACL fragment keyword matches only on the first two IPv6 extension headers for the fragment header (next header code 44). If the fragment header appears in the third or subsequent header, it is not matched.
- For platforms other than the BCM5684X, BCM5685x, and BCM5644X, the IPv6 ACL fragment keyword matches only on the first IPv6 extension header (next header code 44). If the fragment header appears in the second or subsequent header, it is not matched.
- For platforms other than the BCM5644X, the IPv6 ACL routing keyword matches only on the first IPv6 extension header (next header code 43). If the fragment header appears in the second or subsequent header, it is not matched.
- The rate-limit command is not supported for egress IPv6 ACLs.

Parameter	Description
`{deny | permit}`	Specifies whether the IPv6 ACL rule permits or denies the matching traffic.
`Every`	Specifies to match every packet.
{*protocolkey* | *number*}	Specifies the protocol to match for the IPv6 ACL rule. The current list is: *icmpv6*, *ipv6*, *tcp*, and *udp.*
source-ipv6-prefix/prefix-length | any | *host source-ipv6-address*	Specifies a source IPv6 source address and prefix length to match for the IPv6 ACL rule. Specifying any implies specifying "::/0 " Specifying *host source-ipv6-address* implies matching the specified IPv6 address. This *source-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Parameter	Description
[{range {*portkey* | *startport*} {*portkey* | *endport*} | {eq | neq | lt | gt} {*portkey* | *0-65535*}]	**NOTE:** This option is available only if the protocol is TCP or UDP. Specifies the layer 4 port match condition for the IPv6 ACL rule. A port number can be used, in the range 0-65535, or the *portkey*, which can be one of the following keywords: ■ For TCP: *bgp*, *domain*, *echo*, *ftp*, *ftp-data*, *http*, *smtp*, *telnet*, *www*, *pop2*, *pop3* ■ For UDP: *domain*, *echo*, *ntp*, *rip*, *snmp*, *tftp*, *time*, *who*. Each of these keywords translates into its equivalent port number. When range is specified, IPv6 ACL rule matches only if the layer 4 port number falls within the specified portrange. The *startport* and *endport* parameters identify the first and last ports that are part of the port range. They have values from 0 to 65535. The ending port must have a value equal or greater than the starting port. The starting port, ending port, and all ports in between are part of the layer 4 port range. When eq is specified, IPv6 ACL rule matches only if the layer 4 port number is equal to the specified port number or portkey. When lt is specified, IPv6 ACL rule matches if the layer 4 port number is less than the specified port number or portkey. It is equivalent to specifying the range as 0 to <specified port number – 1>. When gt is specified, IPv6 ACL rule matches if the layer 4 port number is greater than the specified port number or portkey. It is equivalent to specifying the range as <specified port number + 1> to 65535. When neq is specified, IPv6 ACL rule matches only if the layer 4 port number is not equal to the specified port number or portkey. Two rules are added in the hardware one with range equal to 0 to <specified port number - 1> and one with range equal to <<specified port number + 1 to 65535>>
destination-ipv6-prefix/prefix-length | any | *host destination-ipv6-address*	Specifies a destination IPv6 source address and prefix length to match for the IPv6 ACL rule. Specifying any implies specifying “::/0 “ Specifying *host destination-ipv6-address* implies matching the specified IPv6 address. This *destination-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Parameter	Description
`sequence` ***sequence-number***	Specifies a sequence number for the ACL rule. Every rule receives a sequence number. The sequence number is specified by the user or is generated by the device. If a sequence number is not specified for the rule, a sequence number that is 10 greater than the last sequence number in ACL is used and this rule is placed at the end of the list. If this is the first ACL rule in the given ACL, a sequence number of 10 is assigned. If the calculated sequence number exceeds the maximum sequence number value, the ACL rule creation fails. It is not allowed to create a rule that duplicates an already existing one. A rule cannot be configured with a sequence number that is already used for another rule. For example, if a user adds new ACL rule to ACL without specifying a sequence number, it is placed at the bottom of the list. By changing the sequence number, user can move the ACL rule to a different position in the ACL
`[dscp` ***dscp***`]`	Specifies the dscp value to match for for the IPv6 rule.
`flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]`	Specifies that the IPv6 ACL rule matches on the tcp flags. When +<tcpflagname> is specified, a match occurs if specified <tcpflagname> flag is set in the TCP header. When "-<tcpflagname>" is specified, a match occurs if specified <tcpflagname> flag is *NOT* set in the TCP header. When established is specified, a match occurs if specified either RST or ACK bits are set in the TCP header. Two rules are installed in hardware to when "established" option is specified. This option is visible only if protocol is "tcp".
`[icmp-type` ***icmp-type*** `[icmp-code` ***icmp-code]*** `| icmp-message` ***icmp-message***`]`	**NOTE:** This option is available only if the protocol is icmpv6. Specifies a match condition for ICMP packets. When *icmp-type* is specified, IPv6 ACL rule matches on the specified ICMP message type, a number from 0 to 255. When *icmp-code* is specified, IPv6 ACL rule matches on the specified ICMP message code, a number from 0 to 255. Specifying *icmp-message* implies both icmp-type and icmp-code are specified. The following icmp-messages are supported: *destination-unreachable*, *echo-reply*, *echo-request*, *header*, *hop-limit*, *mld-query*, *mld-reduction*, *mld-report*, *nd-na*, *nd-ns*, *next-header*, *no-admin*, *no-route*, *packet-too-big*, *port-unreachable*, *router-solicitation*, *router-advertisement*, *router-renumbering*, *time-exceeded*, and *unreachable*. The ICMP message is decoded into the corresponding ICMP type and ICMP code within that ICMP type.
`Fragments`	Specifies that IPv6 ACL rule matches on fragmented IPv6 packets (packets that have the next header field set to 44).
`Routing`	Specifies that IPv6 ACL rule matches on IPv6 packets that have the routing extension header (the next header field is set to 43).
`Log`	Specifies that this rule is to be logged.

Parameter	Description
`time-range` *time-range-name*	Allows imposing a time limitation on the ACL rule as defined by the parameter *time-range-name*. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, the ACL rule is applied immediately. If a time range with the specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, the ACL rule is applied when the time-range with the specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive.
`assign-queue` *queue-id*	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned.
`{mirror | redirect}` *unit/slot/ port*	Specifies the mirror or redirect interface which is the unit/slot/port to which packets matching this rule are copied or forwarded, respectively.
`rate-limit` *rate burst-size*	Specifies the allowed rate of traffic as per the configured rate in kbps, and burst-size in kbytes.
`sflow-remote-agent`	Configures the sFlow sampling action. This action, if configured, copies the packet matching the rule to the remote sFlow agent.

Example: The following shows an example of the command.

```
(Routing) (Config)#ipv6 access-list ip61
(Routing) (Config-ipv6-acl)#permit udp any any rate-limit 32 16
(Routing) (Config-ipv6-acl)#exit
```

12.9.0.4.1 no *sequence-number*

Use this command to remove the ACL rule with the specified sequence number from the ACL.

Format `no` *sequence-number*

Mode Ipv6-Access-List Config

12.9.0.5 ipv6 traffic-filter

This command either attaches a specific IPv6 ACL identified by *name* to an interface or range of interfaces, or associates it with a VLAN ID in a given direction. The *name* parameter must be the name of an existing IPv6 ACL.

An optional sequence number may be specified to indicate the order of this mac access list relative to other IPv6 access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specifiedIPv6 access list replaces the currently attached IPv6 access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

This command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces. The `vlan` keyword is only valid in the Global Config mode. The Interface Config mode command is only available on platforms that support independent per-port class of service queue configuration.

An optional *control-plane* is specified to apply the ACL on CPU port. The IPv6 control packets like IGMPv6 are also dropped because of the implicit *deny all* rule added at the end of the list. To overcome this, permit rules must be added to allow the IPv6 control packets.

NOTE: Note the following:

- The keyword *control-plane* is only available in Global Config mode.
- You should be aware that the *out* option may or may not be available, depending on the platform.

Format `ipv6 traffic-filter name {{control-plane |in|out}|vlan vlan-id {in|out}} [sequence 1-4294967295]`

Modes
- Global Config
- Interface Config

Example: The following shows an example of the command.

```
(Routing)(Config)#ipv6 traffic-filter ip61 control-plane
```

12.9.0.5.1 no ipv6 traffic-filter

This command removes an IPv6 ACL identified by *name* from the interface(s) in a given direction.

Format `no ipv6 traffic-filter <name{{control-plane | in | out} | vlan <vlan-id> {in|out}}`

Modes
- Global Config
- Interface Config

Example: The following shows an example of the command.

```
(Routing) (Config)#no ipv6 traffic-filter ip61 control-plane
```

12.9.0.6 show ipv6 access-lists

This command displays summary information of all the IPv6 Access lists. Use the access list *name* to display detailed information of a specific IPv6 ACL.

This command displays information about the attributes icmp-type, icmp-code, fragments, routing, tcp flags, and source and destination L4 port ranges. It displays committed rate,committed burst size and ACL rule hit count of packets matching the configured ACL rule within an ACL. This counter value rolls-over on reaching the maximum value. There is a dedicated counter for each ACL rule. ACL counters do not interact with PBR counters.

For ACL with multiple rules, once a match occurs at any one specific rule, counters associated with this rule only get incremented (for example, consider an ACL with three rules, after matching rule two, counters for rule three would not be incremented).

For ACL counters, If an ACL rule is configured without RATE-LIMIT, the counter value is a count of the forwarded/discarded packets. (For example: for a burst of 100 packets, the Counter value is 100).

If an ACL rule is configured with RATE LIMIT, the counter value is that of the MATCHED packet count. If the sent traffic rate exceeds the configured limit, the counters still display matched packet count (despite getting dropped beyond the configured limit since match criteria is met) that equals the sent rate. For example, if the rate limit is set to 10 kbps and ‘matching’ traffic is sent at 100 kbps, counters would reflect 100 kbps value. If the sent traffic rate is less than the configured limit, the counters display only the matched packet count. Either way, only the matched packet count is reflected in the counters, irrespective of whether they get dropped or forwarded. ACL counters do not interact with DiffServ policies.

Format `show ipv6 access-lists [name]`

Mode Privileged EXEC

Term	Definition
ACL Counters	Shows whether ACL counters are enabled or disabled.
Current number of all ACLs	The number of ACLs of any type currently configured on the system.
Maximum number of all ACLs	The number of ACLs of any type that can be configured on the system.
IPv6 ACL Name	The configured ACL name.
Rules	The number of rules configured for the ACL.
Direction	Shows whether the ACL is applied to traffic coming into the interface (inbound/ingress) or leaving the interface (outbound/egress).
Interface(s)	Identifies the interface(s) to which the ACL is applied (ACL interface bindings).
VLAN(s)	Identifies the VLANs to which the ACL is applied (ACL VLAN bindings).

If you specify an IPv6 ACL name, the following information displays:

NOTE: Only the access list fields that you configure are displayed. Thus, the command output varies based on the match criteria configured within the rules of an ACL.

Term	Definition
ACL Name	The user-configured name of the ACL.
ACL Counters	Identifies whether the ACL counters are enabled or disabled.
Interface(s)	The inbound and/or outbound interfaces to which the ACL is applied.
Sequence Number	The ordered rule number identifier defined within the IPv6 ACL.
Action	The action associated with each rule. The possible values are Permit or Deny.
Match All	Indicates whether this access list applies to every packet. Possible values are True or False.
Protocol	The protocol to filter for this rule.
Committed Rate	The committed rate defined by the rate-limit attribute.
Committed Burst Size	The committed burst size defined by the rate-limit attribute.
Source IP Address	The source IP address for this rule.
Source L4 Port Keyword	The source port for this rule.
Destination IP Address	The destination IP address for this rule.
Destination L4 Port Keyword	The destination port for this rule.
IP DSCP	The value specified for IP DSCP.
Flow Label	The value specified for IPv6 Flow Label.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	The *slot/port* to which packets matching this rule are copied.
Redirect Interface	The *slot/port* to which packets matching this rule are forwarded.
Time Range Name	Displays the name of the time-range if the IPv6 ACL rule has referenced a time range.
redirectExtAgent	Indicates whether matching flow packets are allowed to be sent to external applications running alongside EFOS on a control CPU. agent-id is a unique identifier for the external receive client application. agent-id is an integer in the range 1 to 100. The `redirectExtAgent` action is mutually exclusive with the `redirect` and `mirror` actions.
Committed Rate	The committed rate defined by the rate-limit attribute.
Committed Burst Size	The committed burst size defined by the rate-limit attribute.
Rule Status	Status (Active/Inactive) of the IPv6 ACL rule.
sFlow Remote Agent	Indicates whether the sFlow sampling action is configured. This action, if configured, copies the packet matching the rule to the remote sFlow agent.

Term	Definition
ACL Hit Count	The ACL rule hit count of packets matching the configured ACL rule within an ACL.

Example: The following shows example CLI display output for the command.

```
(Routing) #show ipv6 access-lists ip61

ACL Name: ip61
ACL Counters: Enabled
Outbound Interface(s): control-plane

Rule Number: 1
Action..................................... permit
Match Every................................ FALSE
Protocol................................... 17(udp)
Committed Rate............................. 32
Committed Burst Size....................... 16
ACL hit count ..............................0
```

12.10 Management Access Control and Administration List

In order to ensure the security of the switch management features, the administrator may elect to configure a management access control list. The Management Access Control and Administration List (MACAL) feature is used to ensure that only known and trusted devices are allowed to remotely manage the switch via TCP/IP.

MACALs can be applied only to in-band ports and cannot be applied to the service port.

12.10.0.1 management access-list

Use this command to create a management access list and to enter access-list configuration mode, where you must define the denied or permitted access conditions with the `deny` and `permit` commands. If no match criteria are defined, the default is `deny`. If you reenter to an access- list context, the new rules would be entered at the end of the access-list. Use the `management access-class` command to choose the active access-list. The active management list cannot be updated or removed. The *name* value can be up to 32 characters.

Format `management access-list` *name*
Mode Global Config

12.10.0.1.1 no management access-list

This command deletes the management ACAL identified by *name* from the system.

Format `no management access-list` *name*
Mode Global Config

12.10.0.2 {deny | permit} (Management ACAL)

This command creates a new rule for the current management access list. A rule may either deny or permit traffic according to the specified classification fields. Rules with `ethernet`, `vlan` and `port-channel` parameters will be valid only if an IP address is defined on the appropriate interface. Each rule should have a unique priority.

Format *{deny | permit} [ethernet interface-number | vlan vlan-id | port-channel number] [service service] [priority priority-value]*

{deny | permit} ip-source ip-address [mask mask | prefix-length] [ethernet interface-number | vlan vlan-id | port-channel number] [service service] [priority priority-value]

Mode Management-ACAL Config

Parameter	Description
ethernet	Ethernet port number.
ip-source	Source IP address
port-channel	Port-channel number.
priority	Priority for rule.

Parameter	Description
service	Service type condition, which can be one of the following key words: ■ java ■ tftp ■ telnet ■ ssh ■ http ■ https ■ snmp ■ sntp ■ any
vlan	VLAN number.
mask	The network mask of the source IP address (0–32)
prefix-length	The number of bits that comprise the source IP address prefix. prefix length must be preceded by a forward slash (/).

Example: The following example shows how to configure two management interfaces:

```
ethernet 0/1 and ethernet 0/9.
(Routing) (Config)#management access-list mlist
(Routing) (config-macal)#permit ethernet 0/1 priority 63
(Routing) (config-macal)#permit ethernet 0/9 priority 64
(Routing) (config-macal)#exit
(Routing) (Config)#management access-class mlist
```

Example: The following example shows how to configure all the interfaces to be management interfaces except for two interfaces: ethernet 0/1 and ethernet 0/9.

```
(Routing) (Config)#management access-list mlist
(Routing) (config-macal)#deny ethernet 0/1 priority 62
(Routing) (config-macal)#deny ethernet 0/9 priority 63
(Routing) (config-macal)#permit priority 64
(Routing) (config-macal)#exit
```

12.10.0.3 management access-class

Use this command to restrict management connections. The `console-only` keyword specifies that the device can be managed only from the console.

Format `management access-class {console-only | name}`

Mode Global Config

12.10.0.3.1 no management access-class

This command disables the management restrictions

Format `no management access-class`

Mode Global Config

12.10.0.4 show management access-list

This command displays management access-lists.

Format `show management access-list [name]`

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) #show management access-list

List Name..................................... mlist
List Admin Mode............................... Disabled
Packets Filtered.............................. 0

Rules:

permit ethernet 0/1 priority 63
permit ethernet 0/9 priority 64

NOTE: All other access is implicitly denied.
```

12.10.0.5 show management access-class

This command displays information about the active management access list.

Format `show management access-class [name]`

Mode Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(Routing) # show management access-class

Management access-class is enabled, using access list mlist
```

12.11 Time Range Commands for Time-Based ACLs

Time-based ACLs allow one or more rules within an ACL to be based on time. Each ACL rule within an ACL except for the implicit *deny all* rule can be configured to be active and operational only during a specific time period. The time range commands allow you to define specific times of the day and week in order to implement time-based ACLs. The time range is identified by a name and can then be referenced by an ACL rule defined with in an ACL.

12.11.0.1 time-range

Use this command to create a time range identified by *name*, consisting of one absolute time entry and/or one or more periodic time entries. The *name* parameter is a case-sensitive, alphanumeric string from 1 to 31 characters that uniquely identifies the time range. An alpha-numeric string is defined as consisting of only alphabetic, numeric, dash, underscore, or space characters.

If a time range by this name already exists, this command enters Time-Range config mode to allow updating the time range entries.

NOTE: When you successfully execute this command, the CLI mode changes to Time-Range Config mode.

Format	`time-range` *name*
Mode	Global Config

12.11.0.1.1 no time-range

This command deletes a time-range identified by *name*.

Format	`no time-range` *name*
Mode	Global Config

12.11.0.2 absolute

Use this command to add an absolute time entry to a time range. Only one absolute time entry is allowed per time-range. The *time* parameter is based on the currently configured time zone.

The *`[start time date]`* parameters indicate the time and date at which the configuration that referenced the time range starts going into effect. The time is expressed in a 24-hour clock, in the form of hours:minutes. For example, 8:00 is 8:00 am and 20:00 is 8:00 pm. The date is expressed in the format day month year. If no start time and date are specified, the configuration statement is in effect immediately.

The *`[end time date]`* parameters indicate the time and date at which the configuration that referenced the time range is no longer in effect. The end time and date must be after the start time and date. If no end time and date are specified, the configuration statement is in effect indefinitely.

Format	*`absolute {[start time date] [end time date]}`*
Mode	Time-Range Config

12.11.0.2.1 no absolute

This command deletes the absolute time entry in the time range.

Format `no absolute`
Mode Time-Range Config

12.11.0.3 periodic

Use this command to add a periodic time entry to a time range. The *time* parameter is based off of the currently configured time zone.

The first occurrence of the *`days-of-the-week`* argument is the starting day(s) from which the configuration that referenced the time range starts going into effect. The second occurrence is the ending day or days from which the configuration that referenced the time range is no longer in effect. If the end days-of-the-week are the same as the start, they can be omitted

This argument can be any single day or combinations of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday. Other possible values are:

- daily—Monday through Sunday
- weekdays—Monday through Friday
- weekend—Saturday and Sunday

If the ending days of the week are the same as the starting days of the week, they can be omitted.

The first occurrence of the `time` argument is the starting hours:minutes which the configuration that referenced the time range starts going into effect. The second occurrence is the ending hours:minutes at which the configuration that referenced the time range is no longer in effect.

The hours:minutes are expressed in a 24-hour clock. For example, 8:00 is 8:00 am and 20:00 is 8:00 pm.

Format *`periodic {days-of-the-week time} to {[days-of-the-week] time}`*
Mode Time-Range Config

12.11.0.3.1 no periodic

This command deletes a periodic time entry from a time range/

Format *`no periodic {days-of-the-week time} to {[days-of-the-week] time}`*
Mode Time-Range Config

12.11.0.4 show time-range

Use this command to display a time range and all the absolute/periodic time entries that are defined for the time range. Use the *`name`* parameter to identify a specific time range to display. When *`name`* is not specified, all the time ranges defined in the system are displayed.

Format `show time-range`
Mode Privileged EXEC

Parameter	Definition
Number of Time Ranges	Number of time ranges configured in the system.

Parameter	Definition
Time Range Name	Name of the time range.
Time Range Status	Status of the time range (active/inactive)
Absolute start	Start time and day for absolute time entry.
Absolute end	End time and day for absolute time entry.
Periodic Entries	Number of periodic entries in a time-range.
Periodic start	Start time and day for periodic entry.
Periodic end	End time and day for periodic entry.

Chapter 13: EFOS Log Messages

This section lists common log messages that are provided by EFOS, along with information regarding the cause of each message. There is no specific action that can be taken per message. When there is a problem being diagnosed, a set of these messages in the event log, along with an understanding of the system configuration and details of the problem) will assist Broadcom in determining the root cause of such a problem.

NOTE: This chapter is not a complete list of all syslog messages.

13.1 Core

Table 19: BSP Log Messages

Component	Message	Cause
BSP	Event(0xaaaaaaaa)	Switch has restarted.
BSP	Starting code...	BSP initialization complete, starting EFOS application.

Table 20: NIM Log Messages

Component	Message	Cause
NIM	NIM: L7_ATTACH out of order for interface unit x slot x port x	Interface creation out of order.
NIM	NIM: Failed to find interface at unit x slot x port x for event(x)	There is no mapping between the USP and Interface number.
NIM	NIM: L7_DETACH out of order for interface unit x slot x port x	Interface creation out of order.
NIM	NIM: L7_DELETE out of order for interface unit x slot x port x	Interface creation out of order.
NIM	NIM: event(x),intf(x),component(x), in wrong phase	An event was issued to NIM during the wrong configuration phase (probably Phase 1, 2, or WMU).
NIM	NIM: Failed to notify users of interface change	Event was not propagated to the system.
NIM	NIM: failed to send message to NIM message Queue.	NIM message queue full or non-existent.
NIM	NIM: Failed to notify the components of L7_CREATE event	Interface not created.
NIM	NIM: Attempted event (x), on USP x.x.x before phase 3	A component issued an interface event during the wrong initialization phase.
NIM	NIM: incorrect phase for operation	An API call was made during the wrong initialization phase.
NIM	NIM: Component(x) failed on event(x) for interface	A component responded with a fail indication for an interface event.
NIM	NIM: Timeout event(x), interface remainingMask = xxxx	A component did not respond before the NIM timeout occurred.

Table 21: SIM Log Message

Component	Message	Cause
SIM	IP address conflict on service port/network port for IP address x.x.x.x. Conflicting host MAC address is xx:xx:xx:xx:xx:xx	This message appears when an address conflict is detected in the LAN for the service port/network port IP.

Table 22: System Log Messages

Component	Message	Cause
SYSTEM	Configuration file fastpath.cfg size is 0 (zero) bytes	The configuration file could not be read. This message may occur on a system for which no configuration has ever been saved or for which configuration has been erased.
SYSTEM	could not separate SYSAPI_CONFIG_FILENAME	The configuration file could not be read. This message may occur on a system for which no configuration has ever been saved or for which configuration has been erased.
SYSTEM	Building defaults for file *file name* version *version num*	Configuration did not exist or could not be read for the specified feature or file. Default configuration values will be used. The file name and version are indicated.
SYSTEM	File *filename*: same version (*version num*) but the sizes (*version size – expected version size*) differ	The configuration file which was loaded was of a different size than expected for the version number. This message indicates the configuration file needed to be migrated to the version number appropriate for the code image. This message may appear after upgrading the code image to a more current release.
SYSTEM	Migrating config file *filename* from version *version num* to *version num*	The configuration file identified was migrated from a previous version number. Both the old and new version number are specified. This message may appear after upgrading the code image to a more current release.
SYSTEM	Building Defaults	Configuration did not exist or could not be read for the specified feature. Default configuration values will be used.
SYSTEM	sysapiCfgFileGet failed size = *expected size of file* version = *expected version*	Configuration did not exist or could not be read for the specified feature. This message is usually followed by a message indicating that default configuration values will be used.

13.2 Utilities

Table 23: Trap Mgr Log Message

Component	Message	Cause
Trap Mgr	Link Up/Down: slot/port	An interface changed link state.

Table 24: DHCP Filtering Log Messages

Component	Message	Cause
DHCP Filtering	Unable to create r/w lock for DHCP Filtering	Unable to create semaphore used for dhcp filtering configuration structure.
DHCP Filtering	Failed to register with nv Store.	Unable to register save and restore functions for configuration save.
DHCP Filtering	Failed to register with NIM	Unable to register with NIM for interface callback functions.
DHCP Filtering	Error on call to sysapiCfgFileWrite file	Error on trying to save configuration.

Table 25: NVStore Log Messages

Component	Message	Cause
NVStore	Building defaults for file XXX	A component's configuration file does not exist or the file's checksum is incorrect so the component's default configuration file is built.
NVStore	File XXX corrupted from file system. Checksum mismatch.	The calculated checksum of a component's configuration file in the file system did not match the checksum of the file in memory.
NVStore	Migrating config file XXX from version Y to Z	A configuration file version mismatch was detected so a configuration file migration has started.

Table 26: RADIUS Log Messages

Component	Message	Cause
RADIUS	RADIUS: Invalid data length - xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Failed to send the request	A problem communicating with the RADIUS server.
RADIUS	RADIUS: Failed to send all of the request	A problem communicating with the RADIUS server during transmit.
RADIUS	RADIUS: Could not get the Task Sync semaphore!	Resource issue with RADIUS Client service.
RADIUS	RADIUS: Buffer is too small for response processing	RADIUS Client attempted to build a response larger than resources allow.
RADIUS	RADIUS: Could not allocate accounting requestInfo	Resource issue with RADIUS Client service.
RADIUS	RADIUS: Could not allocate requestInfo	Resource issue with RADIUS Client service.
RADIUS	RADIUS: Accounting-Response failed to validate, id = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: User (xxx) needs to respond for challenge	An unexpected challenge was received for a configured user.
RADIUS	RADIUS: Could not allocate a buffer for the packet	Resource issue with RADIUS Client service.

Table 26: RADIUS Log Messages (Continued)

Component	Message	Cause
RADIUS	RADIUS: Access-Challenge failed to validate, id = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Failed to validate Message-Authenticator, id = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Access-Accept failed to validate, id = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Invalid packet length – xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Response is missing Message-Authenticator, id = xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Server address doesn't match configured server	RADIUS Client received a server response from an unconfigured server.

Table 27: TACACS+ Log Messages

Component	Message	Cause
TACACS+	TACACS+: authentication error, no server to contact	TACACS+ request needed, but no servers are configured.
TACACS+	TACACS+: connection failed to server x.x.x.x	TACACS+ request sent to server x.x.x.x but no response was received.
TACACS+	TACACS+: no key configured to encrypt packet for server x.x.x.x	No key configured for the specified server.
TACACS+	TACACS+: received invalid packet type from server.	Received packet type that is not supported.
TACACS+	TACACS+: invalid major version in received packet.	Major version mismatch.
TACACS+	TACACS+: invalid minor version in received packet.	Minor version mismatch.

Table 28: LLDP Log Message

Component	Message	Cause
LLDP	lldpTask(): invalid message type:xx. xxxxxx:xx	Unsupported LLDP packet received.

Table 29: SNTP Log Message

Component	Message	Cause
SNTP	SNTP: system clock synchronized on %s UTC	Indicates that SNTP has successfully synchronized the time of the box with the server.

Table 30: DHCPv4 Client Log Messages

Component	Message	Cause
DHCP4 Client	Unsupported subOption (xxx) in Vendor Specific Option in received DHCP pkt	This message appears when a message is received from the DHCP Server that contains an un-supported Vendor Option.
DHCP4 Client	Failed to acquire an IP address on xxx; DHCP Server did not respond.	This message appears when the DHCP Client fails to lease an IP address from the DHCP Server.

Table 30: DHCPv4 Client Log Messages (Continued)

Component	Message	Cause
DHCP4 Client	DNS name server entry add failed.	This message appears when the update of a DNS Domain name server info given by the DHCP Server to the DNS Client fails.
DHCP4 Client	DNS domain name list entry addition failed.	This message appears when the update of a DNS Domain name list info given by the DHCP Server to the DNS Client fails.
DHCP4 Client	Interface xxx Link State is Down. Connect the port and try again.	This message appears when the Network protocol is configured with DHCP without any active links in the Management VLAN.

Table 31: DHCPv6 Client Log Messages

Component	Message	Cause
DHCP6 Client	ip6Map dhcp add failed.	This message appears when the update of a DHCP leased IP address to IP6Map fails.
DHCP6 Client	osapiNetAddrV6Add failed on interface xxx.	This message appears when the update of a DHCP leased IP address to the kernel IP Stack fails.
DHCP6 Client	Failed to add DNS Server xxx to DNS Client.	This message appears when the update of a DNS6 Server address given by the DHCPv6 Server to the DNS6 Client fails.
DHCP6 Client	Failed to add Domain name xxx to DNS Client.	This message appears when the update of a DNS6 Domain name info given by the DHCPv6 Server to the DNS6 Client fails.

13.3 Management

Table 32: SNMP Log Message

Component	Message	Cause
SNMP	EDB Callback: Unit Join: x.	A new unit has joined the stack.

Table 33: EmWeb Log Messages

Component	Message	Cause
EmWeb	EMWEB (Telnet): Max number of Telnet login sessions exceeded	A user attempted to connect via telnet when the maximum number of telnet sessions were already active.
EmWeb	EMWEB (SSH): Max number of SSH login sessions exceeded	A user attempted to connect via SSH when the maximum number of SSH sessions were already active.
EmWeb	Handle table overflow	All the available EmWeb connection handles are being used and the connection could not be made.
EmWeb	*ConnectionType* EmWeb socket accept() failed: errno	Socket accept failure for the specified connection type.
EmWeb	EmWeb: connection allocation failed	Memory allocation failure for the new connection.
EmWeb	EMWEB TransmitPending: EWOULDBLOCK error sending data	Socket error on send.
EmWeb	EmWeb accept: XXXX	Accept function for new SSH connection failed. XXXX indicates the error info.

Table 34: CLI_UTIL Log Messages

Component	Message	Cause
CLI_UTIL	Telnet Send Failed errno = 0x%x	Failed to send text string to the telnet client.
CLI_UTIL	osapiFsDir failed	Failed to obtain the directory information from a volume's directory.

Table 35: SSHD Log Messages

Component	Message	Cause
SSHD	SSHD: Unable to create the global (data) semaphore	Failed to create semaphore for global data protection.
SSHD	SSHD: Msg Queue is full, event = XXXX	Failed to send the message to the SSHD message queue as message queue is full. XXXX indicates the event to be sent.
SSHD	SSHD: Unknown UI event in message, event = XXXX	Failed to dispatch the UI event to the appropriate SSHD function as it's an invalid event. XXXX indicates the event to be dispatched.
SSHD	sshdApiCnfgrCommand: Failed calling sshdIssueCmd.	Failed to send the message to the SSHD message queue.

Table 36: SSLT Log Messages

Component	Message	Cause
SSLT	SSLT: Exceeded maximum, ssltConnectionTask	Exceeded maximum allowed SSLT connections.

Table 36: SSLT Log Messages (Continued)

Component	Message	Cause
SSLT	SSLT: Can't connect to unsecure server at XXXX, result = YYYY, errno = ZZZZ	Failed to open connection to unsecure server. XXXX is the unsecure server socket address. YYYY is the result returned from connect function and ZZZZ is the error code.
SSLT	SSLT: Msg Queue is full, event = XXXX	Failed to send the received message to the SSLT message queue as message queue is full. XXXX indicates the event to be sent.
SSLT	SSLT: Unknown UI event in message, event = XXXX	Failed to dispatch the received UI event to the appropriate SSLT function as it's an invalid event. XXXX indicates the event to be dispatched.
SSLT	ssltApiCnfgrCommand: Failed calling ssltIssueCmd.	Failed to send the message to the SSLT message queue.
SSLT	SSLT: Error loading certificate from file XXXX	Failed while loading the SSLcertificate from specified file. XXXX indicates the file from where the certificate is being read.
SSLT	SSLT: Error loading private key from file	Failed while loading private key for SSL connection.
SSLT	SSLT: Error setting cipher list (no valid ciphers)	Failed while setting cipher list.
SSLT	SSLT: Could not delete the SSL semaphores	Failed to delete SSL semaphores during cleanup.of all resources associated with the OpenSSL Locking semaphores.

Table 37: User_Manager Log Messages

Component	Message	Cause
User_Manager	User Login Failed for XXXX	Failed to authenticate user login. XXXX indicates the username to be authenticated.
User_Manager	Access level for user XXXX could not be determined. Setting to Level 1.	Invalid access level specified for the user. The access level is set to Level 1. XXXX indicates the username.
User_Manager	Could not migrate config file XXXX from version YYYY to ZZZZ. Using defaults.	Failed to migrate the config file. XXXX is the config file name. YYYY is the old version number and ZZZZ is the new version number.

13.4 Switching

Table 38: Protected Ports Log Messages

Component	Message	Cause
Protected Ports	Protected Port: failed to save configuration	This appears when the protected port configuration cannot be saved.
Protected Ports	protectedPortCnfgrInitPhase1Process: Unable to create r/w lock for protected Port	This appears when protectedPortCfgRWLock Fails.
Protected Ports	protectedPortCnfgrInitPhase2Process: Unable to register for VLAN change callback	This appears when nimRegisterIntfChange with VLAN fails.
Protected Ports	Cannot add interface xxx to group yyy	This appears when an interface could not be added to a particular group.
Protected Ports	unable to set protected port group	This appears when a dtl call fails to add interface mask at the driver level.
Protected Ports	Cannot delete interface xxx from group yyy	This appears when a dtl call to delete an interface from a group fails.
Protected Ports	Cannot update group YYY after deleting interface XXX	This message appears when an update group for a interface deletion fails.
Protected Ports	Received an interface change callback while not ready to receive it	This appears when an interface change call back has come before the protected port component is ready.

Table 39: 802.1X Log Messages

Component	Message	Cause
802.1X	*function*: Failed calling dot1xIssueCmd	802.1X message queue is full.
802.1X	*function:* EAP message not received from server	RADIUS server did not send required EAP message.
802.1X	*function*: Out of System buffers	802.1X cannot process/transmit message due to lack of internal buffers.
802.1X	*function*: could not set state to *authorized/unauthorized*, intf xxx	DTL call failed setting authorization state of the port.
802.1X	dot1xApplyConfigData: Unable to *enable/disable* dot1x in driver	DTL call failed enabling/disabling 802.1X.
802.1X	dot1xSendRespToServer: dot1xRadiusAccessRequestSend failed	Failed sending message to RADIUS server.
802.1X	dot1xRadiusAcceptProcess: error calling radiusAccountingStart, ifIndex = xxx	Failed sending accounting start to RADIUS server.
802.1X	*function*: failed sending terminate cause, intf xxx	Failed sending accounting stop to RADIUS server.

Table 40: IGMP Snooping Log Messages

Component	Message	Cause
IGMP Snooping	*function*: osapiMessageSend failed	IGMP Snooping message queue is full.
IGMP Snooping	Failed to set global igmp snooping mode to xxx	Failed to set global IGMP Snooping mode due to message queue being full.
IGMP Snooping	Failed to set igmp snooping mode xxx for interface yyy	Failed to set interface IGMP Snooping mode due to message queue being full.
IGMP Snooping	Failed to set igmp mrouter mode xxx for interface yyy	Failed to set interface multicast router mode due to IGMP Snooping message queue being full.

Table 40: IGMP Snooping Log Messages (Continued)

Component	Message	Cause
IGMP Snooping	Failed to set igmp snooping mode xxx for vlan yyy	Failed to set VLAN IGM Snooping mode due to message queue being full.
IGMP Snooping	Failed to set igmp mrouter mode%d for interface xxx on Vlan yyy	Failed to set VLAN multicast router mode due to IGMP Snooping message queue being full.
IGMP Snooping	snoopCnfgrInitPhase1Process: Error allocating small buffers	Could not allocate buffers for small IGMP packets.
IGMP Snooping	snoopCnfgrInitPhase1Process: Error allocating large buffers	Could not allocate buffers for large IGMP packets.

Table 41: 802.3ad Log Messages

Component	Message	Cause
802.3ad	dot3adReceiveMachine: received default event %x	Received a LAG PDU and the RX state machine is ignoring this LAGPDU.
802.3ad	dot3adNimEventCompletionCallback, dot3adNimEventCreateCompletionCallback: DOT3AD: notification failed for event(%d), intf(%d), reason(%d)	The event sent to NIM was not completed successfully.

Table 42: FDB Log Message

Component	Message	Cause
FDB	fdbSetAddressAgingTimeOut: Failure setting fid %d address aging timeout to %d	Unable to set the age time in the hardware.

Table 43: Double VLAN Tag Log Message

Component	Message	Cause
Double Vlan Tag	dvlantagIntfIsConfigurable: Error accessing dvlantag config data for interface %d	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no preconfiguration.

Table 44: IPv6 Provisioning Log Message

Component	Message	Cause
IPV6 Provisioning	ipv6ProvIntfIsConfigurable: Error accessing IPv6 Provisioning config data for interface %d	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no preconfiguration.

Table 45: MFDB Log Message

Component	Message	Cause
MFDB	mfdbTreeEntryUpdate: entry does not exist	Trying to update a non existing entry.

Table 46: 802.1Q Log Messages

Component	Message	Cause
802.1Q	dot1qIssueCmd: Unable to send message %d to dot1qMsgQueue for vlan %d - %d msgs in queue	dot1qMsgQueue is full.
802.1Q	dot1qVlanCreateProcess: Attempt to create a vlan with an invalid vlan id %d ; VLAN %d not in range,	This accommodates for reserved vlan ids. i.e. 4094 - x.
802.1Q	dot1qMapIntfIsConfigurable: Error accessing DOT1Q config data for interface %d in dot1qMapIntfIsConfigurable.	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no preconfiguration.
802.1Q	dot1qVlanDeleteProcess: Deleting the default VLAN	Typically encountered during clear Vlan and clear config.
802.1Q	dtl failure when adding ports to vlan id %d - portMask = %s	Failed to add the ports to VLAN entry in hardware.
802.1Q	dtl failure when deleting ports from vlan id %d - portMask = %s	Failed to delete the ports for a VLAN entry from the hardware.
802.1Q	dtl failure when adding ports to tagged list for vlan id %d - portMask = %s	Failed to add the port to the tagged list in hardware.
802.1Q	dtl failure when deleting ports from tagged list for vlan id %d - portMask = %s"	Failed to delete the port to the tagged list from the hardware.
802.1Q	dot1qTask: unsuccessful return code on receive from dot1qMsgQueue: %08x"	Failed to receive the dot1q message from dot1q message queue.
802.1Q	Unable to apply VLAN creation request for VLAN ID %d, Database reached MAX VLAN count!	Failed to create VLAN ID, VLAN Database reached maximum values.
802.1Q	Attempt to create a vlan (%d) that already exists	Creation of the existing Dynamic VLAN ID from the CLI.
802.1Q	DTL call to create VLAN %d failed with rc %d"	Failed to create VLAN ID in hardware.
802.1Q	Problem unrolling data for VLAN %d	Failed to delete VLAN from the VLAN database after failure of VLAN hardware creation.
802.1Q	VLAN %d does not exist	Failed to delete VLAN entry.
802.1Q	VLAN %d requestor type %d does not exist	Failed to delete dynamic VLAN ID if the given requestor is not valid.
802.1Q	Can not delete the VLAN, Some unknown component has taken the ownership!	Failed to delete, as some unknown component has taken the ownership.
802.1Q	Not valid permission to delete the VLAN %d requestor %d	Failed to delete the VLAN ID as the given requestor and VLAN entry status are not same.
802.1Q	VLAN Delete Call failed in driver for vlan %d	Failed to delete VLAN ID from the hardware.
802.1Q	Problem deleting data for VLAN %d	Failed to delete VLAN ID from the VLAN database.
802.1Q	Dynamic entry %d can only be modified after it is converted to static	Failed to modify the VLAN group filter
802.1Q	Cannot find vlan %d to convert it to static	Failed to convert Dynamic VLAN to static VLAN. VLAN ID not exists.
802.1Q	Only Dynamically created VLANs can be converted	Error while trying to convert the static created VLAN ID to static.
802.1Q	Cannot modify tagging of interface %s to non existence vlan %d"	Error for a given interface sets the tagging property for all the VLANs in the VLAN mask.
802.1Q	Error in updating data for VLAN %d in VLAN database	Failed to add VLAN entry into VLAN database.
802.1Q	DTL call to create VLAN %d failed with rc %d	Failed to add VLAN entry in hardware.
802.1Q	Not valid permission to delete the VLAN %d	Failed to delete static VLAN ID. Invalid requestor.
802.1Q	Attempt to set access vlan with an invalid vlan id %d	Invalid VLAN ID.

Table 46: 802.1Q Log Messages (Continued)

Component	Message	Cause
802.1Q	Attempt to set access vlan with (%d) that does not exist	VLAN ID not exists.
802.1Q	VLAN create currently underway for VLAN ID %d	Creating a VLAN which is already under process of creation.
802.1Q	VLAN ID %d is already exists as static VLAN	Trying to create already existing static VLAN ID.
802.1Q	Cannot put a message on dot1q msg Queue, Returns:%d	Failed to send Dot1q message on Dot1q message Queue.
802.1Q	Invalid dot1q Interface: %s	Failed to add VLAN to a member of port.
802.1Q	Cannot set membership for user interface %s on management vlan %d	Failed to add VLAN to a member of port.
802.1Q	Incorrect tagmode for vlan tagging. tagmode: %d Interface: %s	Incorrect tagmode for VLAN tagging.
802.1Q	Cannot set tagging for interface %d on non existent vlan %d"	The VLAN ID does not exist.
802.1Q	Cannot set tagging for interface %d which is not a member of vlan %d	Failure in Setting the tagging configuration for a interface on a range of vlan.
802.1Q	VLAN create currently underway for VLAN ID %d"	Trying to create the VLAN ID which is already under process of creation.
802.1Q	VLAN ID %d already exists	Trying to create the VLAN ID which is already exists.
802.1Q	Failed to delete, Default VLAN %d cannot be deleted	Trying to delete Default VLAN ID.
802.1Q	Failed to delete, VLAN ID %d is not a static VLAN	Trying to delete Dynamic VLAN ID from CLI.
802.1Q	Requestor %d attempted to release internal vlan %d: owned by %d	–

Table 47: 802.1S Log Messages

Component	Message	Cause
802.1S	dot1sIssueCmd: Dot1s Msg Queue is full!!!!Event: %u, on interface: %u, for instance: %u	The message Queue is full.
802.1S	dot1sStateMachineRxBpdu(): Rcvd BPDU Discarded	The current conditions, like port is not enabled or we are currently not finished processing another BPDU on the same interface, does not allow us to process this BPDU.
802.1S	dot1sBpduTransmit(): could not get a buffer	Out of system buffers.

Table 48: Port Mac Locking Log Message

Component	Message	Cause
Port Mac Locking	pmlMapIntfIsConfigurable: Error accessing PML config data for interface %d in pmlMapIntfIsConfigurable.	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no preconfiguration.

13.5 QoS

Table 49: ACL Log Messages

Component	Message	Cause
ACL	Total number of ACL rules (x) exceeds max (y) on intf i.	The combination of all ACLs applied to an interface has resulted in requiring more rules than the platform supports.
ACL	ACL *name*, rule *x*: This rule is not being logged	The ACL configuration has resulted in a requirement for more logging rules than the platform supports. The specified rule is functioning normally except for the logging action.
ACL	aclLogTask: error logging ACL rule trap for correlator *number*	The system was unable to send an SNMP trap for this ACL rule which contains a logging attribute.
ACL	IP ACL *number*: Forced truncation of one or more rules during config migration	While processing the saved configuration, the system encountered an ACL with more rules than is supported by the current version. This may happen when code is updated to a version supporting fewer rules per ACL than the previous version.

Table 50: CoS Log Message

Component	Message	Cause
COS	cosCnfgrInitPhase3Process: Unable to apply saved config -- using factory defaults	The COS component was unable to apply the saved configuration and has initialized to the factory default settings.

Table 51: DiffServ Log Messages

Component	Message	Cause
DiffServ	diffserv.c 165: diffServRestore Failed to reset DiffServ. Recommend resetting device	While attempting to clear the running configuration an error was encountered in removing the current settings. This may lead to an inconsistent state in the system and resetting is advised.
DiffServ	Policy invalid for service intf: “policy *name*, interface *x*, direction *y*	The DiffServ policy definition is not compatible with the capabilities of the interface specified. Check the platform release notes for information on configuration limitations.

13.6 Routing/IPv6 Routing

Table 52: DHCP Relay Log Messages

Component	Message	Cause
DHCP relay	REQUEST hops field more than config value	The DHCP relay agent has processed a DHCP request whose HOPS field is larger than the maximum value allowed. The relay agent will not forward a message with a hop count greater than 4.
DHCP relay	Request's seconds field less than the config value	The DHCP relay agent has processed a DHCP request whose SECS field is larger than the configured minimum wait time allowed.
DHCP relay	processDhcpPacket: invalid DHCP packet type: %u\n	The DHCP relay agent has processed an invalid DHCP packet. Such packets are discarded by the relay agent.

Table 53: OSPFv2 Log Messages

Component	Message	Cause
OSPFv2	Best route client deregistration failed for OSPF Redist	OSPFv2 registers with the IPv4 routing table manager (“RTO”) to be notified of best route changes. There are cases where OSPFv2 deregisters more than once, causing the second deregistration to fail. The failure is harmless.
OSPFv2	XX_Call() failure in _checkTimers for thread 0x869bcc0	An OSPFv2 timer has fired but the message queue that holds the event has filled up. This is normally a fatal error.
OSPFv2	Warning: OSPF LSDB is 90% full (22648 LSAs).	OSPFv2 limits the number of Link State Advertisements (LSAs) that can be stored in the link state database (LSDB). When the database becomes 90 or 95 percent full, OSPFv2 logs this warning. The warning includes the current size of the database.
OSPFv2	The number of LSAs, 25165, in the OSPF LSDB has exceeded the LSDB memory allocation.	When the OSPFv2 LSDB becomes full, OSPFv2 logs this message. OSPFv2 reoriginates its router LSAs with the metric of all non-stub links set to the maximum value to encourage other routers to not compute routes through the overloaded router.
OSPFv2	Dropping the DD packet because of MTU mismatch	OSPFv2 ignored a Database Description packet whose MTU is greater than the IP MTU on the interface where the DD was received.
OSPFv2	LSA Checksum error in LsUpdate, dropping LSID 1.2.3.4 checksum 0x1234.	OSPFv2 ignored a received link state advertisement (LSA) whose checksum was incorrect.

Table 54: OSPFv3 Log Messages

Component	Message	Cause
OSPFv3	Best route client deregistration failed for OSPFv3 Redist	OSPFv3 registers with the IPv6 routing table manager (“RTO6”) to be notified of best route changes. There are cases where OSPFv3 deregisters more than once, causing the second deregistration to fail. The failure is harmless.

Table 54: OSPFv3 Log Messages (Continued)

Component	Message	Cause
OSPFv3	Warning: OSPF LSDB is 90% full (15292 LSAs).	OSPFv3 limits the number of Link State Advertisements (LSAs) that can be stored in the link state database (LSDB). When the database becomes 90 or 95 percent full, OSPFv3 logs this warning. The warning includes the current size of the database.
OSPFv3	The number of LSAs, 16992, in the OSPF LSDB has exceeded the LSDB memory allocation.	When the OSPFv3 LSDB becomes full, OSPFv3 logs this message. OSPFv3 reoriginates its router LSAs with the R-bit clear indicating that OSPFv3 is overloaded.
OSPFv3	LSA Checksum error detected for LSID 1.2.3.4 checksum 0x34f5. OSPFv3 Database may be corrupted.	OSPFv3 periodically verifies the checksum of each LSA in memory. OSPFv3 logs this.

Table 55: Routing Table Manager Log Messages

Component	Message	Cause
RTO	RTO is no longer full. Routing table contains xxx best routes, xxx total routes, xxx reserved local routes.	When the number of best routes drops below full capacity, RTO logs this notice. The number of bad adds may give an indication of the number of route adds that failed while RTO was full, but a full routing table is only one reason why this count is incremented.
RTO	RTO is full. Routing table contains xxx best routes, xxx total routes, xxx reserved local routes. The routing table manager stores a limited number of best routes. The count of total routes includes alternate routes, which are not installed in hardware.	The routing table manager, also called “RTO,” stores a limited number of best routes, based on hardware capacity. When the routing table becomes full, RTO logs this alert. The count of total routes includes alternate routes, which are not installed in hardware.

Table 56: VRRP Log Messages

Component	Message	Cause
VRRP	VRRP packet of size xxx dropped. Min VRRP packet size is xxx; Max VRRP packet size is xxx.	This message appears when there is flood of VRRP messages in the network.
VRRP	VR xxx on interface xxx started as xxx.	This message appears when the Virtual router is started in the role of a Master or a Backup.
VRRP	This router is the IP address owner for virtual router xxx on interface xxx. Setting the virtual router priority to xxx.	This message appears when the address ownership status for a specific VR is updated. If this router is the address owner for the VR, set the VR's priority to MAX priority (as per RFC 3768). If the router is no longer the address owner, revert the priority.

Table 57: ARP Log Message

Component	Message	Cause
ARP	IP address conflict on interface xxx for IP address yyy. Conflicting host MAC address is zzz.	When an address conflict is detected for any IP address on the switch upon reception of ARP packet from another host or router.

13.7 Multicast

Table 58: IGMP/MLD Log Messages

Component	Message	Cause
IGMP/MLD	MGMD Protocol Heap Memory Init Failed; Family – xxx.	MGMD Heap memory initialization Failed for the specified address family. his message appears when trying to enable MGMD Protocol.
IGMP/MLD	MGMD Protocol Heap Memory De-Init Failed; Family – xxx.	MGMD Heap memory de-initialization Failed for the specified address family. This message appears when trying to disable MGMD (IGMP/MLD) Protocol. As a result of this, the subsequent attempts to enable/disable MGMD will also fail.
IGMP/MLD	MGMD Protocol Initialization Failed; Family – xxx.	MGMD protocol initialization sequence Failed. This could be due to the nonavailability of some resources. This message appears when trying to enable MGMD Protocol.
IGMP/MLD	MGMD All Routers Address - xxx Set to the DTL Mcast List Failed; Mode – xxx, intf – xxx.	This message appears when trying to enable/disable MGMD Protocol.
IGMP/MLD	MGMD All Routers Address - xxx Add to the DTL Mcast List Failed.	MGMD All Routers Address addition to the local multicast list Failed. As a result of this, MGMD Multicast packets with this address will not be received at the application.
IGMP/MLD	MGMD All Routers Address – xxx Delete from the DTL Mcast List Failed.	MGMD All Routers Address deletion from the local multicast list Failed. As a result of this, MGMD Multicast packets are still received at the application though MGMD is disabled.
IGMP/MLD	MLDv2 GroupAddr-[FF02::16] Enable with Interpeak Stack Failed; rtrIfNum - xxx, intf – xxx.	Registration of this Group address with the Interpeak stack failed. As a result of this, MLDv2 packets will not be received at the application.
IGMP/MLD	MGMD Group Entry Creation Failed; grpAddr - xxx, rtrIfNum – xxx.	The specified Group Address registration on the specified router interface failed.
IGMP/MLD	MGMD Socket Creation/Initialization Failed for addrFamily – xxx.	MGMD Socket Creation/options Set Failed. As a result of this, the MGMD Control packets cannot be sent out on an interface.

Table 59: IGMP-Proxy Log Messages

Component	Message	Cause
IGMP-Proxy/MLD-Proxy	MGMD-Proxy Protocol Initialization Failed; Family – xxx.	MGMD-Proxy protocol initialization sequence Failed. This could be due to the non-availability of some resources. This message appears when trying to enable MGMD-Proxy Protocol.
IGMP-Proxy/MLD-Proxy	MGMD-Proxy Protocol Heap Memory De-Init Failed; Family – xxx.	MGMD-Proxy Heap memory de-initialization is Failed for the specified address family. This message appears when trying to disable MGMD-Proxy Protocol. As a result of this, the subsequent attempts to enable/disable MGMD-Proxy will also fail.
IGMP-Proxy/MLD-Proxy	MGMD Proxy Route Entry Creation Failed; grpAddr - xxx, srcAddr – xxx, rtrIfNum – xxx.	Registration of the Multicast Forwarding entry for the specified Source and Group Address Failed when MGMD-Proxy is used.

Table 60: PIM-SM Log Messages

Component	Message	Cause
PIMSM	Non-Zero SPT/Data Threshold Rate – xxx is currently Not Supported on this platform.	This message appears when the user tries to configure the PIMSM SPT threshold value.
PIMSM	PIMSM Protocol Heap Memory Init Failed; Family – xxx.	PIMSM Heap memory initialization Failed for the specified address family. This message appears when trying to enable PIMSM Protocol.
PIMSM	PIMSM Protocol Heap Memory De-Init Failed; Family – xxx.	PIMSM Heap memory de-initialization Failed for the specified address family. This message appears when trying to disable PIMSM Protocol. As a result of this, the subsequent attempts to enable/disable PIMSM will also fail.
PIMSM	PIMSM Protocol Initialization Failed; Family –xxx.	PIMSM protocol initialization sequence Failed. This could be due to the non-availability of some resources. This message appears when trying to enable PIMSM Protocol.
PIMSM	PIMSM Protocol De-Initialization Failed; Family – xxx.	PIMSM protocol de-initialization sequence Failed. This message appears when trying to disable PIMSM Protocol.
PIMSM	PIMSM SSM Range Table is Full.	PIMSM SSM Range Table is Full. This message appears when the protocol cannot accommodate new SSM registrations.
PIMSM	PIM All Routers Address – xxx Delete from the DTL Mcast List Failed for intf – xxx.	PIM All Routers Address deletion from the local multicast list Failed. As a result of this, PIM Multicast packets are still received at the application though PIM is disabled.
PIMSM	PIM All Routers Address - xxx Add to the DTL Mcast List Failed for intf – xxx.	PIM All Routers Address addition to the local multicast list Failed. As a result of this, PIM Multicast packets with this address will not be received at the application.
PIMSM	Mcast Forwarding Mode Disable Failed for intf – xxx.	Multicast Forwarding Mode Disable Failed. As a result of this, Multicast packets are still received at the application though no protocol is enabled.
PIMSM	Mcast Forwarding Mode Enable Failed for intf – xxx.	Multicast Forwarding Mode Enable Failed. As a result of this, Multicast packets will not be received at the application though a protocol is enabled.
PIMSM	PIMSMv6 Socket Memb'ship Enable Failed for rtrIfNum - xxx.	PIMSMv6 Socket Creation/options Set with Kernel IP Stack Failed. As a result of this, the PIM Control packets cannot be received on the interface.
PIMSM	PIMSMv6 Socket Memb'ship Disable Failed for rtrIfNum – xxx.	PIMSMv6 Socket Creation/options Disable with Kernel IP Stack Failed. As a result of this, the PIM Control packets are still received on the interface at the application though no protocol is enabled.
PIMSM	PIMSM (S,G,RPt) Table Max Limit – xxx Reached; Cannot accommodate any further routes.	PIMSM Multicast Route table (S,G,RPt) has reached maximum capacity and cannot accommodate new registrations anymore.
PIMSM	PIMSM (S,G) Table Max Limit - xxx Reached; Cannot accommodate any further routes.	PIMSM Multicast Route table (S,G) has reached maximum capacity and cannot accommodate new registrations anymore.
PIMSM	PIMSM (*,G) Table Max Limit - xxx Reached; Cannot accommodate any further routes.	PIMSM Multicast Route table (*,G) has reached maximum capacity and cannot accommodate new registrations anymore.

Table 61: PIM-DM Log Messages

Component	Message	Cause
PIMDM	PIMDM Protocol Heap Memory Init Failed; Family – xxx.	PIMDM Heap memory initialization Failed for the specified address family. This message appears when trying to enable PIMDM Protocol.
PIMDM	PIMDM Protocol Heap Memory De-Init Failed; Family – xxx.	PIMDM Heap memory de-initialization Failed for the specified address family. This message appears when trying to disable PIMDM Protocol. As a result of this, the subsequent attempts to enable/disable PIMDM will also fail.
PIMDM	PIMDM Protocol Initialization Failed; Family –xxx.	PIMDM protocol initialization sequence Failed. This could be due to the non-availability of some resources. This message appears when trying to enable PIMDM Protocol.
PIMDM	PIMDM Protocol De-Initialization Failed; Family – xxx.	PIMDM protocol de-initialization sequence Failed. This message appears when trying to disable PIMDM Protocol.
PIMDM	PIM All Routers Address – xxx Delete from the DTL Mcast List Failed for intf – xxx.	PIM All Routers Address deletion from the local multicast list Failed. As a result of this, PIM Multicast packets are still received at the application though PIM is disabled.
PIMDM	PIM All Routers Address - xxx Add to the DTL Mcast List Failed for intf – xxx.	PIM All Routers Address addition to the local multicast list Failed. As a result of this, PIM Multicast packets with this address will not be received at the application.
PIMDM	Mcast Forwarding Mode Disable Failed for intf – xxx.	Multicast Forwarding Mode Disable Failed. As a result of this, Multicast packets are still received at the application though no protocol is enabled.
PIMDM	Mcast Forwarding Mode Enable Failed for intf – xxx.	Multicast Forwarding Mode Enable Failed. As a result of this, Multicast packets will not be received at the application though a protocol is enabled.
PIMDM	PIMDMv6 Socket Memb'ship Enable Failed for rtrIfNum - xxx.	PIMDMv6 Socket Creation/options Set with Kernel IP Stack Failed. As a result of this, the PIM Control packets cannot be received on the interface.
PIMDM	PIMDMv6 Socket Memb'ship Disable Failed for rtrIfNum – xxx.	PIMDMv6 Socket Creation/options Disable with Kernel IP Stack Failed. As a result of this, the PIM Control packets are still received on the interface at the application though no protocol is enabled.
PIMDM	PIMDM FSM Action Invoke Failed; rtrIfNum - xxx Out of Bounds for Event – xxx.	The PIMDM FSM Action invocation Failed due to invalid Routing interface number. In such cases, the FSM Action routine can never be invoked which may result in abnormal behavior. The failed FSM-name can be identified from the specified Event name.
PIMDM	PIMDM Socket Initialization Failed for addrFamily - xxx.	PIMDM Socket Creation/options Set Failed. As a result of this, the PIM Control packets cannot be sent out on an interface.
PIMDM	PIMDMv6 Socket Memb'ship Enable Failed for rtrIfNum - xxx.	Socket options Set to enable the reception of PIMv6 packets Failed. As a result of this, the PIMv6 packets will not be received by the application.
PIMDM	PIMDMv6 Socket Memb'ship Disable Failed for rtrIfNum – xxx.	PIMDMv6 Socket Creation/options Disable with Kernel IP Stack Failed. As a result of this, the PIMv6 Control packets are still received on the interface at the application though no protocol is enabled.
PIMDM	PIMDM MRT Table Max Limit - xxx Reached; Cannot accommodate any further routes.	PIMDM Multicast Route table (S,G) has reached maximum capacity and cannot accommodate new registrations anymore.

Table 62: DVMRP Log Messages

Component	Message	Cause
DVMRP	DVMRP Heap memory initialization is Failed for the specified address family.	This message appears when trying to enable DVMRP Protocol
DVMRP	DVMRP Heap memory de-initialization is Failed for the specified address family.	This message appears when trying to disable DVMRP Protocol. As a result of this, the subsequent attempts to enable/disable DVMRP will also fail.
DVMRP	DVMRP protocol initialization sequence Failed.	This could be due to the non-availability of some resources. This message appears when trying to enable DVMRP Protocol.
DVMRP	DVMRP All Routers Address - xxx Delete from the DTL Mcast List Failed for intf – xxx.	DMVRP All Routers Address deletion from the local multicast list Failed. As a result of this, DVMRP Multicast packets are still received at the application though DVMRP is disabled.
DVMRP	Mcast Forwarding Mode Disable Failed for intf – xxx.	The Multicast Forwarding mode Disable Failed for this routing interface.
DVMRP	DVMRP All Routers Address - xxx Add to the DTL Mcast List Failed for intf – xxx.	DMVRP All Routers Address addition to the local multicast list Failed. As a result of this, DVMRP Multicast packets with this address will not be received at the application.
DVMRP	Mcast Forwarding Mode Enable Failed for intf – xxx.	The Multicast Forwarding mode Enable Failed for this routing interface. As a result of this, the ability to forward Multicast packets does not function on this interface.
DVMRP	DVMRP Probe Control message Send Failed on rtrIfNum – xxx.	DVMRP Probe control message send failed. This could mostly be because of a Failure return status of the socket call sendto(). As a result of this, the DVMRP neighbor could be lost in the neighboring DVMRP routers.
DVMRP	DVMRP Prune Control message Send Failed; rtrIfNum – xxx.	Neighbor - %s, SrcAddr -%s, GrpAddr -%s DVMRP Prune control message send failed. This could mostly be because of a Failure return status of the socket call sendto(). As a result of this, the unwanted multicast traffic is still received and forwarded.
DVMRP	DVMRP Probe Control message Send Failed on rtrIfNum –xxx.	DVMRP Probe control message send failed. This could mostly be because of a Failure return status of the socket call sendto(). As a result of this, the DVMRP neighbor could be lost in the neighboring DVMRP routers.

13.8 Technologies

Table 63: Broadcom Error Messages

Component	Message	Cause
Broadcom	Invalid USP unit = x, slot = x, port = x	A port was not able to be translated correctly during the receive.
Broadcom	In hapiBroadSystemMacAddress call to 'bcm_l2_addr_add' - FAILED : x	Failed to add an L2 address to the MAC table. This should only happen when a hash collision occurs or the table is full.
Broadcom	Failed installing mirror action - rest of the policy applied successfully	A previously configured probe port is not being used in the policy. The release notes state that only a single probe port can be configured.
Broadcom	Policy x does not contain rule x	The rule was not added to the policy due to a discrepancy in the rule count for this specific policy. Additionally, the message can be displayed when an old rule is being modified, but the old rule is not in the policy.
Broadcom	ERROR: policy x, tmpPolicy x, size x, data x x x x x x x	An issue installing the policy due to a possible duplicate hash.
Broadcom	ACL x not found in internal table	Attempting to delete a non-existent ACL.
Broadcom	ACL internal table overflow	Attempting to add an ACL to a full table.
Broadcom	In hapiBroadQosCosQueueConfig, Failed to configure minimum bandwidth. Available bandwidth x	Attempting to configure the bandwidth beyond it’s capabilities.
Broadcom	USL: failed to put sync response on queue	A response to a sync request was not enqueued. This could indicate that a previous sync request was received after it was timed out.
Broadcom	USL: failed to sync ipmc table on unit = x	Either the transport failed or the message was dropped.
Broadcom	usl_task_ipmc_msg_send(): failed to send with x	Either the transport failed or the message was dropped.
Broadcom	USL: No available entries in the STG table	The Spanning Tree Group table is full in USL.
Broadcom	USL: failed to sync stg table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Broadcom	USL: A Trunk doesn't exist in USL	Attempting to modify a Trunk that doesn’t exist.
Broadcom	USL: A Trunk being created by bcmx already existed in USL	Possible synchronization issue between the application, hardware, and sync layer.
Broadcom	USL: A Trunk being destroyed doesn't exist in USL	Possible synchronization issue between the application, hardware, and sync layer.
Broadcom	USL: A Trunk being set doesn't exist in USL	Possible synchronization issue between the application, hardware, and sync layer.
Broadcom	USL: failed to sync trunk table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Broadcom	USL: Mcast entry not found on a join	Possible synchronization issue between the application, hardware, and sync layer.
Broadcom	USL: Mcast entry not found on a leave	Possible synchronization issue between the application, hardware, and sync layer.
Broadcom	USL: failed to sync dvlan data on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.

Table 63: Broadcom Error Messages (Continued)

Component	Message	Cause
Broadcom	USL: failed to sync policy table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Broadcom	USL: failed to sync VLAN table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Broadcom	Invalid LAG id x	Possible synchronization issue between the BCM driver and HAPI.
Broadcom	Invalid uport calculated from the BCM uport bcmx_l2_addr->lport = x	Uport not valid from BCM driver.
Broadcom	Invalid USP calculated from the BCM uport\nbcmx_l2_addr->lport = x	USP not able to be calculated from the learn event for BCM driver.
Broadcom	Unable to insert route R/P	Route R with prefix P could not be inserted in the hardware route table. A retry will be issued.
Broadcom	Unable to Insert host H	Host H could not be inserted in hardware host table. A retry will be issued.
Broadcom	USL: failed to sync L3 Intf table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Broadcom	USL: failed to sync L3 Host table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Broadcom	USL: failed to sync L3 Route table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Broadcom	USL: failed to sync initiator table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.
Broadcom	USL: failed to sync terminator table on unit = x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued.

13.9 O/S Support

Table 64: Linux BSP Log Message

Component	Message	Cause
Linux BSP	rc = 10	Second message logged at bootup, right after *Starting code…. Always* logged.

Table 65: OSAPI Linux Log Messages

Component	Message	Cause
OSAPI Linux	osapiNetLinkNeighDump: could not open socket! - or – ipstkNdpFlush: could not open socket! – or – osapiNetlinkDumpOpen: unable to bind socket! errno = XX	Couldn't open a netlink socket. Make sure "ARP Daemon support" (CONFIG_ARPD) is enabled in the Linux kernel, if the reference kernel binary is not being used.
OSAPI Linux	ipstkNdpFlush: sending delete failed	Failed when telling the kernel to delete a neighbor table entry (the message is incorrect).
OSAPI Linux	osapimRouteEntryAdd, errno XX adding 0xYY to ZZ – or – osapimRouteEntryDelete, errno XX deleting 0xYY from ZZ	Error adding or deleting an IPv4 route (listed in hex as YY), on the interface with Linux name ZZ Error code can be looked up in errno.h.
OSAPI Linux	l3intfAddRoute: Failed to Add Route – or – l3intfDeleteRoute: Failed to Delete Route	Error adding or deleting a default gateway in the kernel's routing table (the function is really osapiRawMRouteAdd()/Delete()).
OSAPI Linux	osapiNetIfConfig: ioctl on XX failed: addr: 0xYY, err: ZZ – or – osapiNetIPSet: ioctl on XX failed: addr: 0x%YY	Failed trying to set the IP address (in hex as YY) of the interface with Linux name XX, and the interface does not exist. Sometimes this is a harmless race condition (e.g., we try to set address 0 when DHCPing on the network port (dtl0) at bootup, before it's created using TAP).
OSAPI Linux	ping: sendto error	Trouble sending an ICMP echo request packet for the UI ping command. Maybe there was no route to that network.
OSAPI Linux	Failed to Create Interface	Out of memory at system initialization time.
OSAPI Linux	TAP Unable to open XX	The /dev/tap file is missing, or, if not using the reference kernel binary, the kernel is missing "Universal TUN/TAP device driver support" (CONFIG_TUN).
OSAPI Linux	Tap monitor task is spinning on select failures – then – Tap monitor select failed: XX	Trouble reading the /dev/tap device, check the error message XX for details.
OSAPI Linux	Log_Init: log file error - creating new log file	This pertains to the "event log" persistent file in flash. Either it did not exist, or had a bad checksum.
OSAPI Linux	Log_Init: Flash (event) log full; erasing	Event log file has been cleared; happens at boot time.
OSAPI Linux	Log_Init: Corrupt event log; erasing	Event log file had a non-blank entry after a blank entry; therefore, something was messed up.
OSAPI Linux	Failed to Set Interface IP Address – or – IP Netmask – or – Broadcast Address – or – Flags – or – Hardware Address – or – Failed to Retrieve Interface Flags	Trouble adding VRRP IP or MAC address(es) to a Linux network interface.

Appendix A: Related Documents

The documents in this section provide additional information about EFOS software for this release.

NOTE: Broadcom provides customer access to technical documentation and software through its Customer Support Portal (CSP) and Downloads and Support site.

For Broadcom documents, replace the “xx” in the document number with the largest number available in the repository to ensure that you have the most current version of the document.

Document (or Item) Name	Document Number	Source
EFOS Administrator’s Guide	EFOS3.X-SWUM1xx	Broadcom CSP
EFOS Functional Specification	EFOS3.X-PG1xx	Broadcom CSP
EFOS Getting Started Guide	EFOS3.X-PG2xx	Broadcom CSP
EFOS Release Notes	EFOS3.X-RN3xx	Broadcom CSP
EFOS Scaling Parameters and Values	EFOS3.X-RM1xx	Broadcom CSP

Appendix B: Command Index

Symbols

{deny | permit} (IP ACL) 1135
{deny | permit} (IPv6) 1144
{deny | permit} (MAC ACL) 1124
{deny | permit} (Management ACAL) 1152

Numerics

1583compatibility 743

A

aaa accounting 101
aaa accounting update 102
aaa authentication dot1x default 398
aaa authentication enable 97
aaa authentication login 96
aaa authorization commands 98
aaa ias-user username 100
aaa server radius dynamic-author 130
aaa session-id 101
absolute 1155
accept-mode 722
access-list 1130
access-list counters enable 1133
accounting 104
acl-trapflags 1139
addport 453
address 723
address prefix (IPv6) 878
address-family 967
address-family ipv4 969
address-family ipv6 969
address-family l2vpn evpn 971
address-family vpnv4 unicast 969
advertisement-interval (BGP Router Config) 970
advertisement-interval (IPv6 Address Family Config) 971
aggregate-address (BGP Router Config) 972
aggregate-address (IPv4 VRF Address Family) 973
application install 169
application start 170
application stop 170
area default-cost (OSPF) 743
area default-cost (OSPFv3) 841
area nssa (OSPF) 743
area nssa (OSPFv3) 841
area nssa default-info-originate (OSPF) 743
area nssa default-info-originate (OSPFv3) 841
area nssa no-redistribute (OSPF) 744
area nssa no-redistribute (OSPFv3) 842
area nssa no-summary (OSPF) 744
area nssa no-summary (OSPFv3) 842
area nssa translator-role (OSPF) 744
area nssa translator-role (OSPFv3) 842
area nssa translator-stab-intv (OSPF) 745
area nssa translator-stab-intv (OSPFv3) 843
area range (OSPF) 745
area range (OSPFv3) 843
area stub (OSPF) 746
area stub (OSPFv3) 844
area stub no-summary (OSPF) 746
area stub no-summary (OSPFv3) 844
area virtual-link (OSPF) 747
area virtual-link (OSPFv3) 844
area virtual-link authentication 747
area virtual-link dead-interval (OSPF) 747
area virtual-link dead-interval (OSPFv3) 845
area virtual-link hello-interval (OSPF) 748
area virtual-link hello-interval (OSPFv3) 845
area virtual-link retransmit-interval (OSPF) 748
area virtual-link retransmit-interval (OSPFv3) 845
area virtual-link transmit-delay (OSPF) 748
area virtual-link transmit-delay (OSPFv3) 846
arp 655
arp access-list 518
arp cachesize 655
arp dynamicrenew 656
arp purge 656
arp retries 657
arp timeout 657
assign-queue 1110
authentication command bounce-port ignore 131
authentication critical recovery max-reauth 408
authentication dynamic-vlan enable 399
authentication enable 409
authentication event fail action authorize vlan 399
authentication event no-response action authorize vlan 399

authentication event server alive action 407
authentication event server dead action 406
authentication event server dead action authorize voice 406
authentication host-mode 402
authentication host-mode all 403
authentication max-users 401
authentication monitor 404
authentication order 409
authentication periodic 401
authentication port-control 401
authentication port-control all 402
authentication priority 409
authentication timer reauthenticate 410
authentication timer restart 410
authentication violation 407
authorization commands 99
authorization network radius 132
auth-type 131
auto-cost (OSPF) 749
auto-cost (OSPFv3) 846
auto-negotiate 342
auto-negotiate all 343

B

bandwidth 759
bcmsh 284
bfd 787
bfd echo 788
bfd interval 788
bfd slow-timer 789
bgp aggregate-different-meds 974
bgp always-compare-med 974
bgp bestpath as-path ignore 975
bgp client-to-client reflection 975
bgp cluster-id 976
bgp default local-preference 976
bgp fast-external-failover 977
bgp fast-internal-failover 977
bgp graceful-restart 988
bgp graceful-restart-helper 989
bgp listen 978
bgp log-neighbor-changes 979
bgp maxas-limit 979
bgp router-id 980
bhd enable 690
bhd spine-port enable 690
boot autoinstall 166
boot host autoreboot 168
boot host autosave 167
boot host dhcp 167
boot host retrycount 167
boot system 173
bootfile 234
bootpdhcprelay cidoptmode 732
bootpdhcprelay maxhopcount 732
bootpdhcprelay minwaittime 732
bridge aging-time 573
bst device threshold 318
bst egress cpu-queue attach profile 318
bst egress cpu-queue create profile 319
bst egress mc-queue attach profile 319
bst egress mc-queue create profile 320
bst egress port-service-pool mc-shared create profile 320
bst egress port-service-pool uc-shared create profile 320
bst egress rqe-queue threshold 321
bst egress service-pool attach profile 321
bst egress service-pool mc-shared threshold 322
bst egress service-pool uc-shared threshold 322
bst egress uc-queue attach profile 322
bst egress uc-queue create profile 323
bst enable 318
bst ingress pg attach profile 323
bst ingress port-pg-shared create profile 324
bst ingress port-service-pool create profile 324
bst ingress service-pool attach profile 325
bst ingress-service-pool threshold 325
bst logging 325

C

cablestatus 285
capability opaque 749
capture file | remote | line 247
capture file size 248
capture line wrap 248
capture remote port 248
capture start 247
capture stop 247

class 1111
class-map 1101
class-map rename 1102
classofservice dot1p-mapping 1087
classofservice ip-dscp-mapping 1087
classofservice traffic-class-group 600
classofservice trust 1088
clear aaa ias-users 104
clear arp-cache 658
clear arp-switch 658
clear authentication authentication-history 411
clear authentication sessions 400
clear authentication statistics 410
clear bst events 330
clear config 212
clear config interface 212
clear counters 212
clear counters mplsd 635
clear counters nvgre 646
clear counters vxlan 646
clear cpu-traffic 254
clear dhcp l2relay statistics interface 505
clear dot1x statistics 398
clear fip-snooping statistics 618
clear host 245
clear ip access-list counters 212
clear ip address-conflict-detect 246
clear ip arp inspection statistics 521
clear ip bgp 1038
clear ip bgp counters 1038
clear ip community-list 1083
clear ip dhcp binding 238
clear ip dhcp conflict 238
clear ip dhcp server statistics 238
clear ip dhcp snooping binding 513
clear ip dhcp snooping statistics 513
clear ip helper statistics 736
clear ip mroute 909
clear ip ospf 750
clear ip ospf configuration 750
clear ip ospf counters 750
clear ip ospf neighbor 750
clear ip ospf neighbor interface 750
clear ip ospf redistribution 750
clear ip ospf stub-router 767
clear ip prefix-list 1084
clear ip route counters 683
clear ip sla statistics 800
clear ipv6 access-list counters 212
clear ipv6 dhcp 885
clear ipv6 dhcp binding 885
clear ipv6 dhcp conflict 885
clear ipv6 dhcp snooping binding 893
clear ipv6 dhcp snooping statistics 893
clear ipv6 mld counters 961
clear ipv6 mld traffic 961
clear ipv6 mroute 943
clear ipv6 neighbors 827
clear ipv6 ospf 846
clear ipv6 ospf configuration 847
clear ipv6 ospf counters 847
clear ipv6 ospf neighbor 847
clear ipv6 ospf neighbor interface 847
clear ipv6 ospf redistribution 847
clear ipv6 ospf stub-router 862
clear ipv6 prefix-list 1086
clear ipv6 route counters 836
clear ipv6 snooping counters 839
clear ipv6 statistics 840
clear isdp counters 576
clear isdp table 576
clear lldp remote-data 552
clear lldp statistics 552
clear logging buffered 206
clear logging email statistics 210
clear mac access-list counters 213
clear mac-addr-table 198
clear mldsnooping 540
clear network ipv6 dhcp statistics 80
clear network ipv6 dhcp statistics 886
clear openflow ca-cert 626
clear packet-trace packet-data 282
clear pass 213
clear port-channel all counters 468
clear port-channel counters 468
clear priority-flow-control statistics 621
clear qcn statistics 595
clear radius dynamic-author statistics 132
clear radius statistics 398
clear serviceport ipv6 dhcp statistics 80

clear serviceport ipv6 dhcp statistics 886
clear traplog 213
clear vlan 213
clear vlan stats 213
clear vpc statistics 479
clear vrrp statistics 725
client 132
client-identifier 231
client-name 231
clock set 227
clock summer-time date 227
clock summer-time recurring 228
clock timezone 228
configuration 84
conform-color 1111
copy (pre-login banner) 162
copy 217
cos-queue min-bandwidth 1088
cos-queue random-detect 1089
cos-queue strict 1089
cpu-traffic direction interface 249
cpu-traffic direction match cust-filter 249
cpu-traffic direction match dstip 250
cpu-traffic direction match srcip 250
cpu-traffic direction match tcp 250
cpu-traffic direction match udp 251
cpu-traffic mode 251
cpu-traffic trace 251
crypto key generate dsa 93
crypto key generate rsa 93
cut-through mode 434

D

dampening 686
debug aaa accounting 254
debug aaa authorization commands 254
debug aaa coa 133
debug aaa pod 133
debug arp 255
debug auto-voip 255
debug bfd event 792
debug bfd packet 792
debug clear 255
debug console 256
debug crashlog 256
debug crashlog kernel 257
debug crashlog kernel upload 257
debug dcbx packet 257
debug debug-config 257
debug dhcp packet 258
debug dot1x packet 258
debug exception 275
debug igmpsnooping packet 258
debug igmpsnooping packet receive 259
debug igmpsnooping packet transmit 259
debug ip acl 260
debug ip bgp 260
debug ip vrrp 261
debug ip vrrp 262
debug ipv6 dhcp 261
debug ipv6 ospfv3 packet 261
debug isdp packet 262
debug lacp packet 263
debug ldap 426
debug license 339
debug mldsnooping packet 263
debug mplsd packet-capture 635
debug mvr packet 452
debug mvr trace 452
debug ospf packet 263
debug packet-trace 277
debug ping packet 265
debug sflow packet 266
debug spanning-tree bpdu 266
debug spanning-tree bpdu receive 266
debug spanning-tree bpdu transmit 267
debug tacacs 268
debug telnetd start 268
debug telnetd stop 268
debug transfer 268
debug udld events 269
debug udld packet receive 269
debug udld packet transmit 269
debug vpc peer detection 480
debug vpc peer-keepalive 479
debug vpc peer-link control-message async 479
debug vpc peer-link control-message bulk 479
debug vpc peer-link control-message ckpt 479
debug vpc peer-link data-message 479
default metric 981

default-information originate 980
default-information originate (OSPF) 751
default-information originate (OSPFv3) 847
default-metric (OSPF) 751
default-metric (OSPFv3) 848
default-originate (BGP Router Config) 981
default-router 232
delay 795
delete 173
deleteport (Global Config) 454
deleteport (Interface Config) 453
description (Task Group Mode) 430
description (User Group Mode) 430
description 343
description 707
destination 490
destination interface 493
dhcp client vendor-id-option 506
dhcp client vendor-id-option-string 506
dhcp l2relay 499
dhcp l2relay circuit-id subscription-name 499
dhcp l2relay circuit-id vlan 499
dhcp l2relay remote-id subscription-name 500
dhcp l2relay remote-id vlan 500
dhcp l2relay subscription-name 501
dhcp l2relay trust 501
dhcp l2relay vlan 502
diffserv 1099
dir 174
disconnect 94
distance (BGP Router Config) 983
distance BGP (BGP Router Config) 984
distance BGP (IPv4 VRF Address Family) 984
distance BGP (IPv6 Address Family Config) 985
distance ospf (OSPF) 751
distance ospf (OSPFv3) 848
distribute-list out (OSPF) 752
distribute-list prefix in 986
distribute-list prefix out 986
dns-server (IPv6) 879
dns-server 232
do (Privileged EXEC commands) 68
domain-name (IPv6) 879
domain-name 234
domain-name enable 234
dos-control all 564
dos-control firstfrag 565
dos-control icmp 566
dos-control icmpfrag 571
dos-control icmpv4 570
dos-control icmpv6 571
dos-control l4port 566
dos-control sipdip 565
dos-control smacdmac 567
dos-control tcpfinurgpsh 570
dos-control tcpflag 566
dos-control tcpflagseq 568
dos-control tcpfrag 565
dos-control tcpoffset 568
dos-control tcpport 567
dos-control tcpsyn 569
dos-control tcpsynfin 569
dos-control udpport 568
dot1x eapolflood 398
dot1x max-reauth-req 400
dot1x max-req 400
dot1x max-start 412
dot1x pae 412
dot1x software version 404
dot1x supplicant port-control 412
dot1x supplicant user 413
dot1x system-auth-control 403
dot1x timeout 404
dot1x user 405
drop 1110
dvlan-tunnel ethertype (Interface Config) 392
dvlan-tunnel ethertype primary-tpid 392
dying-gasp 216

E

efos-show 94
enable (BGP) 987
enable (OSPF) 742
enable (OSPFv3) 848
enable (Privileged EXEC access) 68
enable authentication 100
enable password 112
encapsulation 669
environment temprange 176
environment trap 177

erase application 168
erase factory-defaults 168
erase startup-config 168
errdisable recovery cause 583
errdisable recovery interval 583
erspan-id 491
erspan-id 494
exception core-file 270
exception dump active-port 270
exception dump compression 273
exception dump filepath 271
exception dump ftp-server 273
exception dump nfs 271
exception dump tftp-server 271
exception kernel-dump 272
exception kernel-dump path 272
exception nmi 274
exception protocol 272
exception switch-chip-register 273
exit-overflow-interval (OSPF) 752
exit-overflow-interval (OSPFv3) 849
external-lsdb-limit (OSPF) 752
external-lsdb-limit (OSPFv3) 849

F

feature bfd 787
feature fip-snooping 605
feature vpc 469
fec 343
fhrp version vrrp v3 720
file verify 220
filedescr 173
filter-list (BGP Router Config) 987
filter-list (IPv6 Address Family Config) 988
fip-snooping enable 606
fip-snooping fc-map 606
fip-snooping port-mode 607
flowcontrol 435
fpti 164
frequency 797

H

hardware profile portmode 349
hardware-address 232
host 233
hostname 163

I

icmp-echo 796
ignore server-key 133
ignore session-key 133
inherit taskgroup 431
inherit usergroup 430
interface 342
interface lag 458
interface loopback 805
interface tunnel 807
interface vlan 711
ip access-group 1138
ip access-list 1134
ip access-list rename 1134
ip access-list resequence 1135
ip address 491
ip address 494
ip address 660
ip address dhcp 661
ip address-conflict-detect run 246
ip arp inspection filter 518
ip arp inspection limit 518
ip arp inspection trust 517
ip arp inspection validate 516
ip arp inspection vlan 516
ip arp inspection vlan logging 517
ip as-path access-list 1072
ip bgp fast-external-failover 989
ip bgp-community new-format 1073
ip community-list 1074
ip default-gateway 662
ip dhcp bootp automatic 237
ip dhcp conflict logging 238
ip dhcp excluded-address 236
ip dhcp ping packets 237
ip dhcp pool 231
ip dhcp snooping 507
ip dhcp snooping binding 508
ip dhcp snooping database 508
ip dhcp snooping database write-delay 508
ip dhcp snooping limit 509
ip dhcp snooping log-invalid 509
ip dhcp snooping trust 509

ip dhcp snooping verify mac-address 507
ip dhcp snooping vlan 507
ip domain list 242
ip domain lookup 242
ip domain name 242
ip domain retry 244
ip domain timeout 244
ip dscp 492
ip dvmrp 910
ip dvmrp 911
ip dvmrp metric 910
ip dvmrp trapflags 910
ip helper enable 739
ip helper-address (Global Config) 736
ip helper-address (Interface Config) 737
ip host 244
ip icmp echo-reply 786
ip icmp error-interval 786
ip igmp 929
ip igmp last-member-query-count 930
ip igmp last-member-query-interval 930
ip igmp query-interval 930
ip igmp query-max-response-time 931
ip igmp robustness 931
ip igmp router-alert-check 929
ip igmp startup-query-count 931
ip igmp startup-query-interval 932
ip igmp version 929
ip igmp-proxy 936
ip igmp-proxy reset-status 936
ip igmp-proxy unsolicit-rprt-interval 936
ip ipsec-load-sharing spi 663
ip irdp 703
ip irdp address 703
ip irdp holdtime 703
ip irdp maxadvertinterval 704
ip irdp minadvertinterval 704
ip irdp preference 704
ip load-sharing 662
ip mcast boundary 901
ip mroute 901
ip mtu 668
ip multicast 902
ip multicast ttl-threshold 902
ip name server 243
ip name source-interface 243
ip netdirbcast 667
ip ospf area 759
ip ospf authentication 759
ip ospf bfd 789
ip ospf cost 760
ip ospf database-filter all out 760
ip ospf dead-interval 760
ip ospf hello-interval 761
ip ospf mtu-ignore 763
ip ospf network 761
ip ospf prefix-suppression 761
ip ospf priority 762
ip ospf retransmit-interval 762
ip ospf transmit-delay 763
ip pim 915
ip pim bsr-border 916
ip pim bsr-candidate 917
ip pim dense 915
ip pim dr-priority 917
ip pim hello-interval 916
ip pim join-prune-interval 918
ip pim rp-address 918
ip pim rp-candidate 919
ip pim sparse 915
ip pim ssm 919
ip pim-trapflags 920
ip policy 692
ip prec 492
ip prefix-list 1074
ip prefix-list description 1076
ip redirects 785
ip resilient-hashing 458
ip route 664
ip route default 666
ip route distance 666
ip route net-prototype 666
ip route static bfd interface 667
ip routing 660
ip scp server enable 221
ip sla 792
ip sla schedule 793
ip ssh 90
ip ssh port 90
ip ssh server enable 90

ip telnet port 86
ip telnet server enable 86
ip ttl 492
ip unnumbered gratuitous-arp accept 669
ip unnumbered loopback 669
ip unreachables 785
ip verify binding 508
ip verify source 510
ip verify unicast source reachable-via 688
ip vrf 706
ip vrf forwarding 707
ip vrrp (Global Config) 713
ip vrrp (Interface Config) 713
ip vrrp accept-mode 714
ip vrrp authentication 714
ip vrrp ip 714
ip vrrp mode 713
ip vrrp preempt 715
ip vrrp priority 715
ip vrrp timers advertise 716
ip vrrp track interface 716
ip vrrp track ip route 716
ipv6 access-list 1143
ipv6 access-list rename 1143
ipv6 access-list resequence 1143
ipv6 address 810
ipv6 address autoconfig 810
ipv6 address dhcp 811
ipv6 dhcp client pd 876
ipv6 dhcp conflict logging 876
ipv6 dhcp pool 878
ipv6 dhcp relay 83
ipv6 dhcp relay destination 877
ipv6 dhcp relay remote-id 877
ipv6 dhcp server 877
ipv6 dhcp snooping 887
ipv6 dhcp snooping binding 888
ipv6 dhcp snooping database 888
ipv6 dhcp snooping database write-delay 888
ipv6 dhcp snooping limit 889
ipv6 dhcp snooping log-invalid 889
ipv6 dhcp snooping trust 888
ipv6 dhcp snooping verify mac-address 887
ipv6 dhcp snooping vlan 887
ipv6 enable 809
ipv6 hop-limit 809
ipv6 icmp error-interval 822
ipv6 mld last-member-query-count 957
ipv6 mld last-member-query-interval 957
ipv6 mld query-interval 956
ipv6 mld query-max-response-time 956
ipv6 mld router 956
ipv6 mld version 957
ipv6 mld-proxy 962
ipv6 mld-proxy reset-status 962
ipv6 mld-proxy unsolicit-rprt-interval 962
ipv6 mplsd bgp-mpls-label 634
ipv6 mroute 941
ipv6 mtu 814
ipv6 nd dad attempts 814
ipv6 nd managed-config-flag 815
ipv6 nd ns-interval 815
ipv6 nd other-config-flag 815
ipv6 nd prefix 818
ipv6 nd ra hop-limit unspecified 817
ipv6 nd raguard attach-policy 816
ipv6 nd ra-interval 816
ipv6 nd ra-lifetime 816
ipv6 nd reachable-time 817
ipv6 nd router-preference 817
ipv6 nd suppress-ra 818
ipv6 neighbor 819
ipv6 neighbors dynamicrenew 819
ipv6 nud 819
ipv6 ospf area 854
ipv6 ospf cost 854
ipv6 ospf dead-interval 854
ipv6 ospf hello-interval 855
ipv6 ospf link-lsa-suppression 855
ipv6 ospf mtu-ignore 855
ipv6 ospf network 856
ipv6 ospf prefix-suppression 856
ipv6 ospf priority 857
ipv6 ospf retransmit-interval 857
ipv6 ospf transmit-delay 857
ipv6 pim 945
ipv6 pim bsr-border 946
ipv6 pim bsr-candidate 947
ipv6 pim dense 945
ipv6 pim dr-priority 947

ipv6 pim hello-interval 946
ipv6 pim join-prune-interval 948
ipv6 pim rp-address 948
ipv6 pim rp-candidate 949
ipv6 pim sparse 945
ipv6 pim ssm 949
ipv6 policy 896
ipv6 prefix-list 820
ipv6 prefix-list 1076
ipv6 redirects 785
ipv6 route 811
ipv6 route distance 812
ipv6 route net-prototype 813
ipv6 router ospf 841
ipv6 traffic-filter 1148
ipv6 unicast-routing 809
ipv6 unreachables 821
ipv6 unresolved-traffic 821
ipv6 verify binding 890
ipv6 verify source 889
isdp advertise-v2 575
isdp enable 576
isdp holdtime 575
isdp run 575
isdp timer 575

K

key 157
keystring 157

L

lacp actor admin key 454
lacp actor admin state 455
lacp actor port priority 455
lacp admin key 454
lacp collector max-delay 454
lacp partner admin key 456
lacp partner admin state 456
lacp partner port id 456
lacp partner port priority 457
lacp partner system priority 457
lacp partner system-id 457
ldap authentication bind-first 424
ldap search-map 425
ldap-server host 424
lease 233
length value 197
license clear 339
line 84
link debounce time 286
link state group 444
link state group downstream 445
link state group upstream 445
link state track 444
linuxsh 94
lldp dcbx port-role 587
lldp dcbx version 586
lldp med 557
lldp med all 558
lldp med confignotification 557
lldp med confignotification all 558
lldp med faststartrepeatcount 558
lldp med transmit-tlv 557
lldp med transmit-tlv all 559
lldp notification 551
lldp notification-interval 552
lldp receive 550
lldp timers 550
lldp tlv-select dcbxp 587
lldp transmit 550
lldp transmit-mgmt 551
lldp transmit-tlv 551
llpf 447
load-interval 174
log-adjacency-changes 753
logging buffered 199
logging buffered wrap 199
logging cli-command 199
logging console 200
logging email 207
logging email from-addr 208
logging email logtime 208
logging email message-type subject 208
logging email message-type to-addr 207
logging email test message-type 209
logging email urgent 207
logging host 200
logging host reconfigure 201
logging host remove 201
logging persistent 201

logging protocol 201
logging syslog 202
logging syslog port 202
logging syslog source-interface 202
logging traps 209
login authentication 107
logout 214

M

mab 403
mab request format attribute 1 407
mac access-group 1126
mac access-list extended 1123
mac access-list extended rename 1123
mac access-list resequence 1124
mac-address-table limit 546
macfilter 495
macfilter adddest 495
macfilter adddest all 496
macfilter addsrc 496
macfilter addsrc all 497
mail-server 210
management access-class 1153
management access-list 1152
mark cos 1111
mark cos-as-sec-cos 1112
mark exp 1112
mark ip-dscp 1112
mark ip-precedence 1113
mark secondary-cos 1112
match access-group 1102
match access-group name 1103
match any 1103
match as-path 1077
match class-map 1103
match community 1078
match cos 1104
match destination-address mac 1104
match dstip 1105
match dstip6 1105
match dstl4port 1105
match ethertype 1105
match exp 1105
match ip address <access-list-number | access-list-name> 693
match ip address 1078
match ip dscp 1106
match ip precedence 1106
match ip tos 1106
match ip6flowlbl 1107
match ipv6 address 897
match length 696
match mac-list 696
match protocol 1107
match protocol 1107
match protocol 1107
match secondary-cos 1104
match secondary-vlan 1109
match source-address mac 1108
match src port 1109
match srcip 1108
match srcip6 1108
match srcl4port 1108
match vlan 1109
maximum routes 706
maximum-paths (BGP Router Config) 990
maximum-paths (IPv4 VRF Address Family Config) 990
maximum-paths (IPv6 Address Family Config) 991
maximum-paths (OSPF) 754
maximum-paths (OSPFv3) 850
maximum-paths igbp (BGP Router Config) 991
maximum-paths igbp (IPv4 VRF Address Family Config) 992
maximum-paths igbp (IPv6 Address Family Config) 992
maximum-prefix (BGP Router Config) 993
maximum-prefix (IPv6 Address Family Config) 994
max-metric router-lsa 766
max-metric router-lsa 861
mbuf 274
media-type 343
memory free low-watermark processor 198
mirror 1110
mode dot1q-tunnel 393
mode dvlan-tunnel 393
monitor session destination 482
monitor session filter 483
monitor session mode 483
monitor session source 481

monitor session type erspan-destination 488
monitor session type erspan-source 488
mplsd bgp-advertise 633
mplsd bgp-mpls-label 634
mplsd lfdb ipv4 633
mplsd lfdb ipv6 633
mplsd lfdb layer-2 634
mtu 344
mvr group 448
mvr immediate 448
mvr mode 449
mvr querytime 449
mvr type 449
mvr vlan group 450
mvr vlan 449
mvr 448

N

neighbor activate (IPv4 VRF/VPNv4/L2VPN Address Family Config) 994
neighbor activate (IPv6) 995
neighbor advertisement-interval (BGP Router Config) 996
neighbor advertisement-interval (IPv4 VRF Address Family Config) 997
neighbor advertisement-interval (IPv6 Address Family Config) 998
neighbor allowas-in (BGP Router Config) 997
neighbor connect-retry-interval (IPv4 Address Family Config) 999
neighbor connect-retry-interval 999
neighbor default-originate (BGP Router Config) 1000
neighbor default-originate (IPv4 VRF Address Family Config) 1001
neighbor default-originate (IPv6 Address Family Config) 1001
neighbor default-originate (IPv6 Address Family Config) 982
neighbor description 1002
neighbor ebgp-multihop (IPv4 Address Family Config) 1003
neighbor ebgp-multihop 1003
neighbor fall-over bfd 790
neighbor filter-list (BGP Router Config) 1004
neighbor filter-list (IPv4 VRF Address Family Config) 1005
neighbor filter-list (IPv6 Address Family Config) 1005
neighbor inherit peer (BGP Router Config) 1006
neighbor inherit peer (IPv4 Address Family Config) 1007
neighbor local-as (BGP Router Config) 1007
neighbor local-as (IPv4 VRF Address Family Config) 1008
neighbor maximum-prefix (BGP Router Config) 1009
neighbor maximum-prefix (IPv4 VRF Address Family Config) 1009
neighbor maximum-prefix (IPv6 Address Family Config) 1010
neighbor next-hop-self (BGP Router Config) 1011
neighbor next-hop-self (IPv4 VRF Address Family Config) 1011
neighbor next-hop-self (IPv6 Address Family Config) 1012
neighbor password (IPv4 VRF Address Family Config) 1013
neighbor password 1012
neighbor prefix-list 1013
neighbor remote-as (BGP Router Config) 1014
neighbor remote-as (IPv6 Address Family Config) 1015
neighbor remove-private-as (BGP Router Config) 1015
neighbor remove-private-as (IPv4 VRF Address Family Config) 1016
neighbor remove-private-as (IPv6 Address Family Config) 1016
neighbor rfc5549-support 1017
neighbor route-map (BGP Router Config) 1017
neighbor route-map (IPv4 VRF Address Family Config) 1018
neighbor route-map (IPv6 Address Family Config) 1018
neighbor route-reflector-client (BGP Router Config) 1019
neighbor route-reflector-client (IPv4 VRF Address Family Config) 1019
neighbor route-reflector-client (IPv6 Address Family Config) 1020
neighbor send-community (IPv4 VRF Address Family Config) 1022

neighbor send-community 1021
neighbor send-community extended 1021
neighbor shutdown (IPv4 VRF Address Family Config) 1023
neighbor shutdown 1022
neighbor timers (IPv4 VRF Address Family Config) 1024
neighbor timers 1023
neighbor update-source (IPv4 VRF Address Family Config) 1026
neighbor update-source 1025
netbios-name-server 235
netbios-node-type 235
network (BGP Router Config) 1027
network (DHCP Pool Config) 233
network (IPv6 Address Family Config) 1027
network area (OSPF) 742
network ipv6 address 76
network ipv6 enable 73
network ipv6 gateway 76
network ipv6 neighbor 75
network mac-address 70
network mac-type 70
network mgmt_vlan 374
network parms 69
network protocol 70
network protocol dhcp 70
next-server 236
no monitor 484
no monitor session 484
no userprofile 426
nsf (OSPFv3) 859
nsf 764
nsf helper (OSPFv3) 860
nsf helper 765
nsf helper strict-lsa-checking (OSPFv3) 861
nsf helper strict-lsa-checking 766
nsf ietf helper disable (OSPFv3) 860
nsf ietf helper disable 765
nsf restart-interval (OSPFv3) 859
nsf restart-interval 764
nv overlay evpn 1028
nvgre enable 640
nvgre nve 640
nvgre source-ip 641
nvgre tenant-system 641
nvgre vlan 642

O

openflow controller 625
openflow default-table 625
openflow enable 624
openflow ip-mode 625
openflow passive-mode 626
openflow static-ip 624
openflow variant 626
option 236
origin ip address 491

P

packet-trace eth 277
packet-trace ipv4 277
packet-trace ipv6 277
packet-trace l4 277
passive-interface (OSPF) 755
passive-interface (OSPFv3) 850
passive-interface default (OSPF) 755
passive-interface default (OSPFv3) 850
password (AAA IAS User Configuration) 103
password (Line Configuration) 111
password (Mail Server Config Mode) 211
password (User EXEC) 112
password 111
passwords aging 114
passwords history 113
passwords lock-out 114
passwords min-length 113
passwords strength exclude-keyword 117
passwords strength maximum consecutive-characters 115
passwords strength maximum repeated-characters 115
passwords strength minimum character-classes 116
passwords strength minimum lowercase-letters 115
passwords strength minimum numeric-characters 116
passwords strength minimum special-characters 116
passwords strength minimum uppercase-letters 115
passwords strength-check 114
peer detection enable 470
peer detection interval 470
peer-keepalive destination 470

peer-keepalive enable 471
peer-keepalive timeout 471
periodic 1156
permit ip host mac host 519
ping 214
ping ipv6 80
ping ipv6 interface 80
police-simple 1113
police-single-rate 1114
police-two-rate 1114
policy-map 1114
policy-map rename 1115
port (Dynamic Authorization Mode) 134
port (Mail Server Config Mode) 211
port (TACACS Config Mode) 157
port lacpmode 459
port lacpmode enable all 459
port lacptimeout (Global Config) 460
port lacptimeout (Interface Config) 460
port-channel 453
port-channel adminmode 461
port-channel linktrap 461
port-channel load-balance 461
port-channel min-links 462
port-channel name 462
port-channel resilient-hashing 458
port-channel static 459
port-channel system priority 462
port-locator disable 288
port-locator enable 288
port-security 544
port-security mac-address 545
port-security mac-address move 545
port-security mac-address sticky 545
port-security max-dynamic 544
port-security max-static 544
preempt 721
prefix-delegation (IPv6) 879
prefix-suppression (Router OSPF Config) 753
prefix-suppression (Router OSPFv3 Config) 753
priority 158
priority 722
priority-flow-control mode 620
priority-flow-control priority 621
private-vlan 385
process cpu threshold 189

Q

qcn cnm-transmit-priority 591
qcn cnpv-priority 593
qcn cnpv-priority (datacenter bridging config) 592
qcn cnpv-priority alternate-priority 592
qcn cnpv-priority alternate-priority 594
qcn cnpv-priority cp-creation 593
qcn cnpv-priority defense-mode-choice 593
qcn enable 591
qcn transmit-tlv enable 594
quit 215

R

radius accounting mode 134
radius server attribute 135
radius server attribute 32 include-in-access-req 136
radius server attribute 44 include-in-access-req 136
radius server dead-criteria 137
radius server deadtime 137
radius server host 138
radius server host link-local 139
radius server host test 140
radius server key 140
radius server load-balance 141
radius server msgauth 142
radius server primary 142
radius server retransmit 143
radius server timeout 144
radius server vsa send 145
radius source-interface 143
random-detect 1090
random-detect exponential weighting-constant 1090
random-detect queue-parms 1090
rd 1028
redirect 1111
redistribute (BGP Router Config) 1029
redistribute (IPv4 VRF Address Family Config) 1030
redistribute (IPv6 Address Family Config) 1031
redistribute (OSPF) 754
redistribute (OSPFv3) 851
reflector-port 493
release dhcp 663
reload 215

remark 1127
remote-span 485
renew dhcp 663
renew dhcp network-port 663
renew dhcp service-port 664
resptime 657
retain route-target all 1034
rmon alarm 305
rmon collection history 308
rmon event 307
rmon hcalarm 306
role priority 471
route-map 693
router bgp 967
router ospf 742
route-reflector-client 1032
router-id (OSPF) 754
router-id (OSPFv3) 851
route-target 1033
routing 660

S

script apply 160
script delete 161
script list 161
script show 161
script validate 161
sdm prefer 299
security 210
serial baudrate 84
serial timeout 85
server-key 144
service dhcp 237
service-policy 1116
serviceport ip 69
serviceport ipv6 address 74
serviceport ipv6 enable 73
serviceport ipv6 gateway 74
serviceport ipv6 neighbor 75
serviceport protocol 69
serviceport protocol dhcp 69
session-limit 87
session-timeout 88
set as-path 1079
set clibanner 162
set comm-list delete 1080
set community 1080
set igmp 523
set igmp fast-leave 524
set igmp groupmembership-interval 525
set igmp header-validation 523
set igmp interfacemode 524
set igmp maxresponse 525
set igmp mcrtrexpiretime 526
set igmp mrouter 526
set igmp mrouter interface 526
set igmp querier 530
set igmp querier election participate 531
set igmp querier query-interval 530
set igmp querier timer expiry 531
set igmp querier version 531
set igmp report-suppression 527
set interface 697
set ip default next-hop 698
set ip next-hop 698
set ip precedence 699
set ipv6 default next-hop 899
set ipv6 next-hop (BGP) 1082
set ipv6 next-hop 898
set ipv6 precedence 900
set local-preference 1081
set metric (BGP) 1081
set mld 534
set mld fast-leave 535
set mld groupmembership-interval 535
set mld interfacemode 534
set mld maxresponse 536
set mld mcrtexpiretime 536
set mld mrouter 537
set mld mrouter interface 537
set mld querier 541
set mld querier election participate 542
set mld querier query_interval 541
set mld querier timer expiry 542
set prompt 162
sflow poller 293
sflow receiver 290
sflow receiver owner notimeout 291
sflow receiver owner timeout 290
sflow remote-agent ip 291

sflow remote-agent monitor-session 292
sflow remote-agent port 292
sflow remote-agent source-interface 292
sflow sampler 293
sflow sampler rate 294
sflow sampler remote-agent 294
sflow source-interface 295
show aaa ias-users 104
show aaa taskgroup 432
show aaa userdb 433
show aaa usergroup 432
show access-lists 1142
show access-lists vlan 1142
show accounting 105
show accounting methods 105
show accounting update 106
show application files 170
show application 170
show arp 658
show arp access-list 522
show arp brief 659
show arp switch 174
show arp switch 659
show authentication 414
show authentication authentication-history 414
show authentication clients 415
show authentication interface 416
show authentication methods 417
show authentication statistics 418
show authorization methods 106
show autoinstall 168
show bfd neighbors 790
show bgp ipv6 1065
show bgp ipv6 aggregate-address 1066
show bgp ipv6 community 1067
show bgp ipv6 community-list 1067
show bgp ipv6 listen range 1067
show bgp ipv6 neighbors 1069
show bgp ipv6 neighbors advertised-routes 1068
show bgp ipv6 neighbors policy 1068
show bgp ipv6 neighbors routes 1068
show bgp ipv6 route-reflection 1069
show bgp ipv6 statistics 1070
show bgp ipv6 summary 1071
show bgp ipv6 update-group 1071
show bgp l2vpn evpn 1061
show bgp l2vpn evpn route-reflection 1065
show bgp l2vpn evpn statistics 1065
show bgp l2vpn evpn summary 1060
show bgp l2vpn evpn update-group 1064
show bhd status 690
show bootpdhcprelay 733
show bootvar 173
show bst device 326
show bst egress cpu-queue 326
show bst egress port 326
show bst egress rqe-queue 327
show bst egress service-pool 327
show bst events 327
show bst ingress port pg 328
show bst ingress port service-pool 328
show bst ingress service-pool 328
show bst status 328
show bst threshold 329
show bst threshold profiles 329
show capture packets 249
show class-map 1117
show classofservice dot1p-mapping 1095
show classofservice ip-dscp-mapping 1095
show classofservice ip-precedence-mapping 1095
show classofservice traffic-class-group 603
show classofservice trust 1096
show clibanner 162
show clock 229
show clock detail 229
show cpu-traffic 252
show cpu-traffic interface 253
show cpu-traffic summary 253
show cpu-traffic trace 253
show cut-through mode 434
show dampening interface 686
show debugging 269
show dhcp client vendor-id-option 506
show dhcp l2relay agent-option vlan 504
show dhcp l2relay all 502
show dhcp l2relay circuit-id vlan 502
show dhcp l2relay interface 503
show dhcp l2relay remote-id vlan 503
show dhcp l2relay stats interface 503
show dhcp l2relay subscription interface 504

show dhcp l2relay vlan 504
show dhcp lease 670
show diffserv 1117
show diffserv service 1120
show diffserv service brief 1120
show dos-control 571
show dot1q-tunnel 394
show dot1x 418
show dot1x users 421
show dvlan-tunnel 394
show dying-gasp 216
show environment 177
show errdisable recovery 584
show eventlog 175
show exception core-dump-file 276
show exception kernel-dump 274
show exception kernel-dump list 274
show exception kernel-dump log 274
show exception log 276
show exception 275
show fiber-ports optical-transceiver 303
show fiber-ports optical-transceiver-info 303
show fip-snooping 608
show fip-snooping enode 609
show fip-snooping fcf 610
show fip-snooping sessions 612
show fip-snooping statistics 614
show fip-snooping vlan 618
show flowcontrol 435
show forwardingdb agetime 573
show hardware 175
show hashdest 463
show hosts 245
show igmpsnooping 527
show igmpsnooping mrouter interface 528
show igmpsnooping mrouter vlan 529
show igmpsnooping querier 532
show igmpsnooping ssm 529
show interface 179
show interface counters 180
show interface counters 181
show interface counters 181
show interface dampening 686
show interface debounce 286
show interface ethernet 183
show interface ethernet switchport 386
show interface fec 346
show interface loopback 805
show interface media-type 346
show interface priority-flow-control 622
show interface tunnel 808
show interfaces cos-queue 1096
show interfaces hardware profile 349
show interfaces random-detect 1097
show interfaces status 180
show interfaces status err-disabled 584
show interfaces switchport 389
show interfaces switchport 390
show interfaces switchport 397
show interfaces traffic-class-group 604
show interfaces vlan mapping 391
show ip access-lists 1140
show ip address-conflict 246
show ip arp inspection 519
show ip arp inspection interfaces 521
show ip arp inspection statistics 520
show ip as-path-access-list 1082
show ip bgp 1038
show ip bgp aggregate-address 1041
show ip bgp community 1041
show ip bgp community-list 1042
show ip bgp extcommunity-list 1042
show ip bgp listen range 1043
show ip bgp neighbors {received-routes | routes | rejected-routes} 1050
show ip bgp neighbors 1044
show ip bgp neighbors advertised-routes 1048
show ip bgp neighbors policy 1043
show ip bgp neighbors policy 1049
show ip bgp route-reflection 1051
show ip bgp statistics 1052
show ip bgp summary 1053
show ip bgp template 1054
show ip bgp traffic 1055
show ip bgp update-group 1055
show ip bgp vpnv4 1058
show ip bootpdhcprelay 733
show ip brief 670
show ip community-list 1083
show ip dhcp binding 239

show ip dhcp conflict 241
show ip dhcp global configuration 239
show ip dhcp pool configuration 239
show ip dhcp server statistics 240
show ip dhcp snooping 510
show ip dhcp snooping binding 511
show ip dhcp snooping database 511
show ip dhcp snooping interfaces 512
show ip dhcp snooping statistics 512
show ip dvmrp 911
show ip dvmrp interface 911
show ip dvmrp neighbor 912
show ip dvmrp nexthop 913
show ip dvmrp prune 913
show ip dvmrp route 913
show ip helper statistics 740
show ip helper-address 739
show ip igmp 932
show ip igmp groups 933
show ip igmp interface 933
show ip igmp interface membership 934
show ip igmp interface stats 935
show ip igmp-proxy 937
show ip igmp-proxy groups 938
show ip igmp-proxy groups detail 939
show ip igmp-proxy interface 937
show ip interface 671
show ip interface brief 673
show ip irdp 705
show ip load-sharing 673
show ip mcast 902
show ip mcast boundary 903
show ip mcast interface 903
show ip mcast mroute group 907
show ip mcast mroute source 908
show ip mcast mroute static 908
show ip mfc 920
show ip mroute 903
show ip ospf 768
show ip ospf abr 771
show ip ospf area 771
show ip ospf asbr 772
show ip ospf database 773
show ip ospf database database-summary 774
show ip ospf interface 774
show ip ospf interface brief 776
show ip ospf interface stats 776
show ip ospf lsa-group 778
show ip ospf neighbor 778
show ip ospf range 780
show ip ospf statistics 781
show ip ospf stub table 782
show ip ospf traffic 782
show ip ospf virtual-link 783
show ip ospf virtual-link brief 784
show ip pim 921
show ip pim bsr-router 924
show ip pim interface 923
show ip pim neighbor 924
show ip pim rp mapping 926
show ip pim rp-hash 925
show ip pim ssm 922
show ip pim statistics 927
show ip policy 699
show ip prefix-list 1083
show ip protocols 673
show ip resilient-hashing 464
show ip route 676
show ip route ecmp-groups 679
show ip route hw-failure 680
show ip route net-prototype 680
show ip route preferences 683
show ip route static bfd 681
show ip route summary 681
show ip route track-table 802
show ip sla configuration 801
show ip sla statistics 801
show ip source binding 514
show ip ssh 91
show ip stats 684
show ip verify interface 514
show ip verify source 513
show ip vlan 712
show ip vrf 708
show ip vrrp 718
show ip vrrp interface 718
show ip vrrp interface brief 719
show ip vrrp interface stats 717
show ipv6 access-lists 1149
show ipv6 brief 822

show ipv6 dhcp 880
show ipv6 dhcp binding 881
show ipv6 dhcp conflict 882
show ipv6 dhcp interface 825
show ipv6 dhcp interface 881
show ipv6 dhcp pool 882
show ipv6 dhcp snooping 890
show ipv6 dhcp snooping binding 891
show ipv6 dhcp snooping database 891
show ipv6 dhcp snooping interfaces 892
show ipv6 dhcp snooping statistics 892
show ipv6 dhcp statistics 880
show ipv6 interface 823
show ipv6 mld groups 958
show ipv6 mld interface 959
show ipv6 mld traffic 960
show ipv6 mld-proxy 963
show ipv6 mld-proxy groups 964
show ipv6 mld-proxy groups detail 965
show ipv6 mld-proxy interface 963
show ipv6 mroute 941
show ipv6 mroute group 942
show ipv6 mroute source 942
show ipv6 mroute static 943
show ipv6 nd raguard policy 826
show ipv6 neighbors 826
show ipv6 ospf 863
show ipv6 ospf abr 865
show ipv6 ospf area 865
show ipv6 ospf asbr 866
show ipv6 ospf database 866
show ipv6 ospf database database-summary 867
show ipv6 ospf interface 868
show ipv6 ospf interface brief 868
show ipv6 ospf interface stats 869
show ipv6 ospf lsa-group 870
show ipv6 ospf max-metric 871
show ipv6 ospf neighbor 871
show ipv6 ospf range 873
show ipv6 ospf statistics 873
show ipv6 ospf stub table 874
show ipv6 ospf virtual-link 874
show ipv6 ospf virtual-link brief 875
show ipv6 pim 950
show ipv6 pim bsr-router 953
show ipv6 pim interface 951
show ipv6 pim neighbor 952
show ipv6 pim rp mapping 954
show ipv6 pim rp-hash 954
show ipv6 pim ssm 951
show ipv6 policy 900
show ipv6 prefix-list 1085
show ipv6 protocols 827
show ipv6 route 829
show ipv6 route ecmp-groups 831
show ipv6 route hw-failure 832
show ipv6 route net-prototype 832
show ipv6 route preferences 833
show ipv6 route static bfd 833
show ipv6 route summary 834
show ipv6 route track-table 802
show ipv6 snooping counters 836
show ipv6 source binding 895
show ipv6 traffic 837
show ipv6 verify 893
show ipv6 verify source 894
show ipv6 vlan 836
show isdp 576
show isdp entry 577
show isdp interface 577
show isdp neighbors 577
show isdp traffic 578
show issu status 337
show issu status detail 337
show lacp actor 465
show lacp partner 465
show ldap-search-map 427
show ldap-server 427
show ldap-server statistics 428
show license 340
show license features 341
show license file 340
show link state group detail 446
show link state group 445
show lldp 552
show lldp dcbx interface 588
show lldp interface 553
show lldp local-device 556
show lldp local-device detail 556
show lldp med 559

show lldp med interface 559
show lldp med local-device detail 560
show lldp med remote-device 561
show lldp med remote-device detail 562
show lldp remote-device 554
show lldp remote-device detail 555
show lldp statistics 553
show lldp tlv-select 588
show llpf interface all 447
show logging 203
show logging buffered 204
show logging email config 209
show logging email statistics 210
show logging hosts 204
show logging persistent 205
show logging traplogs 205
show loginsession 94
show loginsession long 95
show mab 422
show mac access-lists 1128
show mac-address-table igmpsnooping 529
show mac-address-table limit 548
show mac-address-table mldsnooping 540
show mac-address-table multicast 573
show mac-address-table static 497
show mac-address-table staticfiltering 497
show mac-address-table stats 574
show mac-addr-table 188
show mail-server config 211
show management access-class 1154
show management access-list 1153
show mbuf total 276
show mldsnooping 537
show mldsnooping mrouter interface 538
show mldsnooping mrouter vlan 538
show mldsnooping querier 542
show mldsnooping ssm entries 539
show mldsnooping ssm groups 539
show mldsnooping ssm stats 539
show mmu config device 330
show mmu config port 330
show monitor session 485
show mplsd interface 638
show mplsd lfdb 637
show mplsd tunnels 638
show mplsd 635
show msg-queue 276
show mvr interface 451
show mvr members 450
show mvr traffic 451
show mvr 450
show network 71
show network ipv6 dhcp statistics 78
show network ipv6 dhcp statistics 883
show network ipv6 neighbors 77
show nvgre nve 648
show nvgre tenant-systems all 649
show nvgre tenant-systems 648
show nvgre 647
show openflow 626
show openflow configured controller 627
show openflow installed flows 628
show openflow installed groups 630
show openflow table-status 631
show packet-trace ecmp 278
show packet-trace lag 278
show packet-trace packet-data 278
show packet-trace port 279
show packet-trace port eth 280
show packet-trace port ipv4 281
show packet-trace port ipv6 281
show packet-trace port tcpv4 282
show packet-trace port tcpv6 282
show packet-trace port udpv4 282
show packet-trace port udpv6 282
show passwords configuration 117
show passwords result 117
show platform vpd 178
show policy-map 1118
show policy-map interface 1121
show port 347
show port description 348
show port fpti 164
show port- locator 288
show port-channel 466
show port-channel brief 465
show port-channel counters 467
show port-channel resilient-hashing 468
show port-channel system priority 468
show port-security 547

show port-security dynamic 547
show port-security static 547
show port-security violation 548
show process app-list 190
show process app-resource-list 191
show process cpu threshold 192
show process proc-list 190
show qcn active priority 598
show qcn interface 598
show qcn priority 595
show qcn statistics 599
show radius 145
show radius accounting 149
show radius accounting servers 151
show radius accounting statistics 151
show radius servers 147
show radius source-interface 153
show radius statistics 153
show rmon 308
show rmon collection history 309
show rmon events 310
show rmon hcalarms 315
show rmon history 311
show rmon log 313
show rmon statistics interfaces 314
show route-map 700
show routing heap summary 684
show running-config 192
show running-config interface 193
show running-config vpc 473
show sdm prefer 300
show serial 85
show service-policy 1121
show serviceport 72
show serviceport ipv6 dhcp statistics 79
show serviceport ipv6 dhcp statistics 884
show serviceport ipv6 neighbors 77
show sflow agent 295
show sflow pollers 296
show sflow receivers 296
show sflow remote-agents 297
show sflow remote-agents source-interface 297
show sflow samplers 298
show sflow source-interface 298
show slot 176
show snmp 127
show snmp engineID 127
show snmp filters 128
show snmp group 128
show snmp user 129
show snmp views 129
show snmp-server 128
show snmptrap source-interface 130
show sntp 225
show sntp client 225
show sntp server 225
show sntp source-interface 226
show spanning-tree 364
show spanning-tree active 365
show spanning-tree backbonefast 367
show spanning-tree brief 367
show spanning-tree interface 368
show spanning-tree mst detailed 369
show spanning-tree mst port detailed 369
show spanning-tree mst port summary 370
show spanning-tree mst port summary active 371
show spanning-tree mst summary 371
show spanning-tree summary 372
show spanning-tree uplinkfast 372
show spanning-tree vlan 373
show stats flow-based 335
show stats group 334
show storm-control 442
show switchport protected 397
show sysinfo 196
show tacacs 159
show tacacs source-interface 159
show tech-support 196
show telnet 89
show telnetcon 89
show terminal length 197
show time-range 1156
show track 803
show trapflags 129
show udld 581
show udld slot/port 582
show users 109
show users accounts 110
show users login-history 111
show users long 110

show version 177
show version bootloader 178
show vlan 379
show vlan brief 382
show vlan internal usage 380
show vlan port 382
show vlan remote-span 488
show vpc 474
show vpc brief 474
show vpc consistency-parameters 475
show vpc peer-keepalive 477
show vpc role 477
show vpc statistics 478
show vrrp 726
show vrrp brief 730
show vrrp statistics 731
show vxlan tenant-systems all 652
show vxlan tenant-systems 651
show vxlan vtep 653
show vxlan 650
show xxx|begin “string” 171
show xxx|exclude “string” 171
show xxx|include “string” 171
show xxx|include “string” exclude “string2” 171
show xxx|section “string” “string2” 172
show xxx|section “string” 172
show xxx|section “string” include “string2” 172
show 194
shutdown (VRRP Group Configuration) 723
shutdown 344
shutdown all 345
snapshot bgp 1071
snmp-server 118
snmp-server community 118
snmp-server community-group 119
snmp-server enable traps 120
snmp-server enable traps bgp 120
snmp-server enable traps linkmode 120
snmp-server enable traps multiusers 121
snmp-server enable traps stpmode 121
snmp-server enable traps violation 119
snmp-server enable traps vrrp 720
snmp-server engineID local 121
snmp-server filter 122
snmp-server group 122
snmp-server host 123
snmp-server port 124
snmp-server proxy 124
snmp-server trapsend 124
snmp-server user 125
snmp-server v3-host 126
snmp-server view 125
snmptrap source-interface 126
sntp broadcast client poll-interval 222
sntp client mode 222
sntp client port 223
sntp server 224
sntp source-interface 224
sntp unicast client poll-interval 223
sntp unicast client poll-retry 224
sntp unicast client poll-timeout 223
source 490
source 493
spanning-tree 351
spanning-tree auto-edge 351
spanning-tree backbonefast 351
spanning-tree bpdufilter 353
spanning-tree bpdufilter default 353
spanning-tree bpduflood 353
spanning-tree bpduguard 354
spanning-tree bpdumigrationcheck 354
spanning-tree configuration name 354
spanning-tree configuration revision 355
spanning-tree cost 352
spanning-tree edgeport 355
spanning-tree forward-time 355
spanning-tree guard 356
spanning-tree max-age 356
spanning-tree max-hops 356
spanning-tree mode 357
spanning-tree mst 357
spanning-tree mst instance 358
spanning-tree mst priority 359
spanning-tree mst vlan 359
spanning-tree port mode 359
spanning-tree port mode all 360
spanning-tree port-priority 360
spanning-tree tcnguard 361
spanning-tree transmit 360
spanning-tree uplinkfast 361

spanning-tree vlan 361
spanning-tree vlan cost 362
spanning-tree vlan forward-time 362
spanning-tree vlan hello-time 362
spanning-tree vlan max-age 363
spanning-tree vlan port-priority 363
spanning-tree vlan priority 364
spanning-tree vlan root 363
speed 345
speed all 346
sshcon maxsessions 91
sshcon timeout 91
stats flow-based (Global Config) 332
stats flow-based (Interface Config) 334
stats flow-based reporting 333
stats group (Global Config) 331
stats group (Interface Config) 333
storm-control broadcast 437
storm-control broadcast action 438
storm-control broadcast level 438
storm-control broadcast rate 438
storm-control multicast 439
storm-control multicast action 439
storm-control multicast level 440
storm-control multicast rate 440
storm-control unicast 441
storm-control unicast action 441
storm-control unicast level 442
storm-control unicast rate 442
switchport access vlan 388
switchport mapping vlan 391
switchport mode 387
switchport mode private-vlan 384
switchport private-vlan 384
switchport protected (Global Config) 396
switchport protected (Interface Config) 396
switchport trunk allowed vlan 387
switchport trunk native vlan 388
system urpf enable 688
system-mac 472
system-priority 472

T

tacacs-server host 155
tacacs-server host link-local 155
tacacs-server key 156
tacacs-server keystring 156
tacacs-server source-interface 158
tacacs-server timeout 156
task [read] [write] [debug] [execute] 431
taskgroup (User Group Mode) 430
taskgroup 429
telnet 86
telnetcon maxsessions 88
telnetcon timeout 88
template peer 1035
terminal length 197
threshold 799
timeout 158
timeout 798
time-range 1155
timers advertise 722
timers bgp 1036
timers pacing flood 755
timers pacing lsa-group 851
timers pacing lsa-group 756
timers policy-apply delay 1037
timers spf 756
timers throttle spf 852
traceroute 81
traceroute ipv6 83
track interface 724
track ip route 725
track ip sla 794
traffic-class-group max-bandwidth 600
traffic-class-group min-bandwidth 601
traffic-class-group strict 602
traffic-class-group weight 603
traffic-shape 1094
transport input telnet 87
transport output telnet 87
trapflags (OSPF) 756
trapflags (OSPFv3) 852
tunnel destination 807
tunnel mode ipv6ip 807
tunnel source 807

U

udld enable (Global Config) 580
udld enable (Interface Config) 580

udld message time 580
udld port 581
udld reset 581
udld timeout interval 580
update bootcode 173
update-source 1036
usergroup 429
username (Global Config) 108
username (Mail Server Config) 211
username name nopassword 109
username unlock 109
username usergroup 429
userprofile attribute-name 426

V

vlan 374
vlan acceptframe 374
vlan database 374
vlan ingressfilter 375
vlan internal allocation 375
vlan makestatic 375
vlan name 376
vlan participation 376
vlan participation all 376
vlan port acceptframe all 377
vlan port ingressfilter all 377
vlan port priority all 395
vlan port pvid all 377
vlan port tagging all 378
vlan priority 395
vlan pvid 378
vlan routing 710
vlan tagging 378
vpc 473
vpc domain 469
vpc peer-link 473
vrf (IP SLA) 800
vrrp 721
vxlan enable 643
vxlan source-ip 643
vxlan tenant-system 644
vxlan udp-dst-port 644
vxlan vlan 645
vxlan vtep 645

W

watchdog clear 283
watchdog disable 283
watchdog enable 283
write core 275
write memory 221

Revision History

EFOS3.X-SWUM200; November 21, 2018

Initial release


BROADCOM®