NETGEAR®

CLI Command Reference Manual

M4500 Intelligent Fully Managed Switches

Software version 7.0.0 and later versions

Model M4500-32C

Model M4500-48XF8C

July 2025
202-12041-07

NETGEAR, Inc.
350 E. Plumeria Drive
San Jose, CA 95134, USA

Support and Community

Visit netgear.com/support to get your questions answered and access the latest downloads.

You can also check out our NETGEAR Community for helpful advice at community.netgear.com.

Regulatory and Legal

Si ce produit est vendu au Canada, vous pouvez accéder à ce document en français canadien à https://www.netgear.com/support/download/.

(If this product is sold in Canada, you can access this document in Canadian French at https://www.netgear.com/support/download/.)

For regulatory compliance information including the EU Declaration of Conformity, visit https://www.netgear.com/about/regulatory/.

See the regulatory compliance document before connecting the power supply.

For NETGEAR's Privacy Policy, visit https://www.netgear.com/about/privacy-policy.

By using this device, you are agreeing to NETGEAR's Terms and Conditions at https://www.netgear.com/about/terms-and-conditions. If you do not agree, return the device to your place of purchase within your return period.

Trademarks

© NETGEAR, Inc., NETGEAR, and the NETGEAR Logo are trademarks of NETGEAR, Inc. Any non-NETGEAR trademarks are used for reference purposes only.

Revision History

Publication Part Number	Publish Date	Comments
202-12041-07	July 2025	We made minor changes.
202-12041-06	September 2024	We made minor changes.
202-12041-05	July 2024	We made minor changes.
202-12041-04	August 2023	We added **show fiber-ports optics** commands and a troubleshooting section.
202-12041-03	August 2020	We made multiple changes and corrections.
202-12041-02	April 2020	We made multiple changes and corrections.
202-12041-01	September 2019	First publication.

CONTENTS

1. INTRODUCTION 63

1.1. Product Overview 63

1.1.1. Simplicity 63

1.1.2. High Availability 63

1.1.3. High-Performance L2/L3 Access Deployments 63

1.1.4. Advance IPv4 and IPv6 Routing 64

1.1.5. Data Center Application 64

1.2. Features 64

1.3. Management Options 66

1.4. Command Line Console Interface Through The Serial Port or Telnet 66

1.5. SNMP-Based Management 67

2. QUICK STARTUP 70

2.1. Quick-Start the Switch 70

2.2. Methods to Access the Switch CLI 70

2.2.1. Switch CLI Access Using a Console 71

2.2.2. Switch CLI Access Using SSH Standard Port 22 72

2.2.3. Switch CLI Access Using SSH Special Port 1234 72

2.2.4. Switch CLI Access Using Telnet Special Port 1223 73

2.2.5. Limitations for a Guest User Login 73

2.2.6. Limitations for SNMP Login 73

2.3. System Information Setup 73

2.3.1. Quick Startup Software Version Information 73

2.3.2. Quick Startup Physical Port Data 73

2.3.3. Quick Startup User Account Management 74

2.3.4. Quick Startup IP Address 74

2.3.5. Quick Startup Downloading from TFTP Server 75

2.3.6. Quick Startup Factory Defaults 76

3. CONSOLE AND TELNET ADMINISTRATION INTERFACE 77

3.1. Local Console Management 77

3.2. Setup Your Switch Using Console Access 77

3.3. Setup Your Switch Using Telnet Access 78

3.3.1. Accessing the Switch CLI through the Network 78

3.3.2. Using the Service Port or Network Interface for Remote Management 79
3.3.2.1. Configuring Service Port Information 80
3.3.2.2. Configuring the In-Band Network Interface 80
3.3.2.3. Firmware Image Update 81
4. COMMAND LINE INTERFACE STRUCTURE AND MODE-BASED CLI 82
4.1. CLI Command Format 82
4.2. CLI Mode-based Topology 83
4.2.1. Parameters 83
4.2.2. Values 83
4.2.3. Conventions 84
4.2.4. Annotations 84
5. SWITCHING COMMANDS 86
5.1. System Information and Statistics Commands 86
5.1.1. show arp 86
5.1.2. show calendar 86
5.1.3. show process cpu 87
5.1.4. show process cpu threshold 88
5.1.5. show eventlog 88
5.1.6. show running-config 89
5.1.7. show sysinfo 90
5.1.8. POST Diagnostic Commands 92
5.1.8.1. show system self-test 92
5.1.8.2. run system self-test 92
5.1.9. show system 93
5.1.10. show tech-support 93
5.1.11. show hardware 94
5.1.12. show version 96
5.1.13. show logingsessin 96
5.1.14. show command filter 97
5.1.15. show transceiver device 98
5.1.16. show transceiver interface 99
5.1.17. show process memory 100
5.1.18. show process app-list 100
5.1.19. show process app-resource-list 101

5.1.20. show process proc-list 102
5.1.21. show environment 102
5.1.22. show configuration files 104
5.1.23. process cpu threshold 105
5.1.24. memory free low-watermark processor 106
5.1.25. show supported cardtype 106
5.1.26. show supported cardtype <cardindex> 106
5.1.27. pager 107
5.1.28. show pager 107
5.2. Device Configuration Commands 108
5.2.1. Interface commands 108
5.2.1.1. show interface status 108
5.2.1.1.1. show interface status 108
5.2.1.1.2. show interface status <slot/port> 109
5.2.1.1.3. show interface status err-disabled 110
5.2.1.1.4. show interface status loopback <0-63> 110
5.2.1.1.5. show interface status port-channel <1-64> 111
5.2.1.1.6. show interface status tunnel <0-7> 112
5.2.1.1.7. show interface status vlan <1-4093> 112
5.2.1.2. show interface counters 113
5.2.1.2.1. show interface counters 114
5.2.1.2.2. show interface counters detailed 115
5.2.1.2.3. show interface counters detailed switchport 119
5.2.1.3. show interface dampening 121
5.2.1.4. show interface loopback 121
5.2.1.5. show interface port-channel 122
5.2.1.6. show interface port-mode 123
5.2.1.7. show interface priority flow control 124
5.2.1.8. show interface switch 125
5.2.1.9. show interface switchport 126
5.2.1.10. show interface tunnel 128
5.2.1.11. show interface description 129
5.2.1.12. show interface fec 129
5.2.1.13. show interface advertise 130
5.2.1.14. show fiber-ports optics commands 131

5.2.1.14.1. .... show fiber-port optics 131
5.2.1.14.2. .... show fiber-port optics-diag 131
5.2.1.14.3. .... show fiber-port optics-eeprom 132
5.2.1.14.4. .... show fiber-port optics-info 132
5.2.1.15. Interface configuraton commands 132
5.2.1.15.1. .... interface 132
5.2.1.15.2. .... description 133
5.2.1.15.3. .... no description 133
5.2.1.15.4. .... flowcontrol 134
5.2.1.15.5. .... no flowcontrol 134
5.2.1.15.6. .... mtu 134
5.2.1.15.7. .... no mtu 134
5.2.1.15.8. .... port-mode 135
5.2.1.15.9. .... no port-mode 135
5.2.1.15.10. .. shutdown 136
5.2.1.15.11. .. shutdown all 136
5.2.1.15.12. .. fec 136
5.2.1.15.13. .. negotiate 137
5.2.1.16. show port status all 137
5.2.1.17. Show flowcontrol 138
5.2.2. Show BMC Commands 139
5.2.2.1. show bmc 139
5.2.2.2. bmc account password 140
5.2.2.3. bmc ip 141
5.2.2.4. bmc watchdog 141
5.2.3. L2 MAC Address and Multicast Forwarding Database Tables 141
5.2.3.1. show mac-addr-table 141
5.2.3.2. show mac-addr-table count 142
5.2.3.3. show mac-addr-table interface 142
5.2.3.4. show mac-address-table igmpsnooping 142
5.2.3.5. show mac-address-table multicast 143
5.2.3.6. show mac-address-table status 144
5.2.3.7. show mac-addr-table agetime 144
5.2.3.8. mac-addr-table aging-time 144
5.2.3.9. no mac-addr-table aging-time 144
5.2.3.10. clear mac-addr-table dynamic 145

5.2.4. VLAN Commands 145
5.2.4.1. vlan database 145
5.2.4.2. vlan 145
5.2.4.3. no vlan 145
5.2.4.4. vlan makestatic 146
5.2.4.5. vlan name 146
5.2.4.6. no vlan name 146
5.2.4.7. switchport acceptable-frame-types 146
5.2.4.8. no switchport acceptable-frame-types 147
5.2.4.9. switchport acceptbale-frame-type all 147
5.2.4.10. no switchport acceptable-frame-types all 147
5.2.4.11. switchport ingress-filtering 147
5.2.4.12. no switchport ingress-filtering 148
5.2.4.13. switchport ingress-filtering all 148
5.2.4.14. no switchport ingress-filtering all 148
5.2.4.15. switchport native vlan 148
5.2.4.16. no switchport native vlan 149
5.2.4.17. switchport native vlan all 149
5.2.4.18. no switchport native vlan all 149
5.2.4.19. switchport allowed vlan 149
5.2.4.20. switchport allowed vlan all 150
5.2.4.21. switchport tagging 150
5.2.4.22. no switchport tagging 150
5.2.4.23. switchport tagging all 150
5.2.4.24. no switchport tagging all 151
5.2.4.25. show vlan 151
5.2.4.26. show vlan id 151
5.2.4.27. show vlan internal usage 152
5.2.4.28. show interface switchport 153
5.2.4.29. show vlan private-vlan 153
5.2.4.30. show vlan remote-span 153
5.2.5. Private VLAN Commands 154
5.2.5.1. switchport private-vlan 154
5.2.5.2. no switchport private-vlan 154

5.2.5.3. switchport mode private-vlan 154
5.2.5.4. no switchport mode private-vlan 155
5.2.5.5. private-vlan 155
5.2.5.6. no private-vlan 155
5.2.6. Switch Ports 156
5.2.6.1. switchport mode 156
5.2.6.2. no switchport mode 156
5.2.6.3. switchport trunk allowed vlan 156
5.2.6.4. no switchport trunk allowed vlan 157
5.2.6.5. switchport trunk native vlan 157
5.2.6.6. no switchport trunk native vlan 157
5.2.6.7. switchport access vlan 158
5.2.6.8. no switchport access vlan 158
5.2.6.9. show interfaces switchport 158
5.2.7. Double VLAN Commands 158
5.2.7.1. dvlan-tunnel ethertype 158
5.2.7.2. no dvlan-tunnel ethertype 159
5.2.7.3. dot1q-tunnel ethertype 159
5.2.7.4. no dot1q-tunnel ethertype 159
5.2.7.5. mode dot1q-tunnel 159
5.2.7.6. no mode dot1q-tunnel 160
5.2.7.7. mode dvlan-tunnel 160
5.2.7.8. no mode dvlan-tunnel 160
5.2.7.9. show dot1q-tunnel 160
5.2.7.10. show dvlan-tunnel 161
5.2.8. IGMP snooping commands 162
5.2.8.1. ip igmp snooping 162
5.2.8.2. no ip igmp snooping 162
5.2.8.3. clear igmp snooping 163
5.2.8.4. ip igmp snooping interfacemode 163
5.2.8.5. no ip igmp snooping interfacemode 163
5.2.8.6. ip igmp snooping interfacemode all 163
5.2.8.7. no ip igmp snooping interfacemode all 164
5.2.8.8. ip igmp snooping fast-leave 164

5.2.8.9. no ip igmp snooping fast-leave 164
5.2.8.10. ip igmp snooping groupmembershipinterval 164
5.2.8.11. no ip igmp snooping groupmembershipinterval 165
5.2.8.12. ip igmp snooping mcrtrexpiretime 165
5.2.8.13. no ip igmp snooping mcrtrexpiretime 165
5.2.8.14. ip igmp snooping mrouter 165
5.2.8.15. no ip igmp snooping mrouter 166
5.2.8.16. set igmp 166
5.2.8.17. no set igmp 166
5.2.8.18. set igmp fast-leave 166
5.2.8.19. no set igmp fast-leave 167
5.2.8.20. set igmp groupmembership-interval 167
5.2.8.21. no set igmp groupmembership-interval 167
5.2.8.22. set igmp maxresponse 167
5.2.8.23. no set igmp maxresponse 168
5.2.8.24. set igmp mcrtrexpiretime 168
5.2.8.25. no set igmp mcrtrexpiretime 168
5.2.8.26. set igmp report-suppression 168
5.2.8.27. no set igmp report-suppression 169
5.2.8.28. set snoop-vlan-block 169
5.2.8.29. no set snoop-vlan-block 169
5.2.8.30. ip igmp snooping static 169
5.2.8.31. no ip igmp snooping static 170
5.2.8.32. ip igmp snooping router-alert-check 170
5.2.8.33. no ip igmp snooping router-alert-check 170
5.2.8.34. show ip igmp snooping 170
5.2.8.35. show ip igmp snooping mrouter interface 172
5.2.8.36. show ip igmp snooping mrouter vlan 172
5.2.8.37. show ip igmp snooping static 172
5.2.8.38. show mac-address-table igmpsnooping 173
5.2.8.39. show ip igmp snooping ssm entries 173
5.2.8.40. show ip igmp snooping ssm groups 174
5.2.8.41. show ip igmp snooping ssm stats 174
5.2.8.42. ip igmp snooping maxresponse 174

5.2.8.43. no ip igmp snooping maxresponse 175
5.2.9. IGMP snooping querier commands 175
5.2.9.1. ip igmp snooping querier 175
5.2.9.2. no ip igmp snooping querier 175
5.2.9.3. ip igmp snooping querier address 175
5.2.9.4. no ip igmp snooping querier address 176
5.2.9.5. ip igmp snooping querier query-interval 176
5.2.9.6. no ip igmp snooping querier query-interval 176
5.2.9.7. ip igmp snooping querier querier-expiry-interval 176
5.2.9.8. no ip igmp snooping querier querier-expiry-interval 177
5.2.9.9. ip igmp snooping querier version 177
5.2.9.10. no ip igmp snooping querier version 177
5.2.9.11. ip igmp snooping querier vlan 177
5.2.9.12. no ip igmp snooping querier vlan <vlan-id> 177
5.2.9.13. ip igmp snooping querier vlan address 178
5.2.9.14. no ip igmp snooping querier vlan address 178
5.2.9.15. ip igmp snooping querier vlan election participate 178
5.2.9.16. no ip igmp snooping querier vlan election participate 178
5.2.9.17. show ip igmp snooping querier 179
5.2.9.18. show ip igmp snooping querier vlan 179
5.2.9.19. show ip igmp snooping querier detail 180
5.2.10. MLD Snooping Commands 181
5.2.10.1. show ipv6 mld snooping 181
5.2.10.2. show ipv6 mld snooping mrouter interface 182
5.2.10.3. show ipv6 mld snooping mrouter vlan 182
5.2.10.4. show ipv6 mld snooping static 183
5.2.10.5. show mac-address-table mldsnooping 183
5.2.10.6. show ipv6 mld snooping ssm entries 183
5.2.10.7. show ipv6 mld snooping ssm groups 184
5.2.10.8. show ipv6 mld snooping ssm stats 184
5.2.10.9. ipv6 mld snooping 184
5.2.10.10. no ipv6 mld snooping 185
5.2.10.11. clear mld snooping 185
5.2.10.12. ipv6 mld snooping interfacemode 185

5.2.10.13. no ipv6 mld snooping interfacemode 185
5.2.10.14. ipv6 mld snooping interfacemode all 186
5.2.10.15. no ipv6 mld snooping interfacemode all 186
5.2.10.16. ipv6 mld snooping fast-leave 186
5.2.10.17. no ipv6 mld snooping fast-leave 186
5.2.10.18. ipv6 mld snooping groupmembershipinterval 187
5.2.10.19. no ipv6 mld snooping groupmembershipinterval 187
5.2.10.20. ipv6 mld snooping mcrtrexpiretime 187
5.2.10.21. no ipv6 mld snooping mcrtrexpiretime 187
5.2.10.22. ipv6 mld snooping mrouter 188
5.2.10.23. no ipv6 mld snooping mrouter 188
5.2.10.24. ipv6 mld snooping static 188
5.2.10.25. no ipv6 mld snooping static 188
5.2.10.26. set mld 189
5.2.10.27. no set mld 189
5.2.10.28. set mld fast-leave 189
5.2.10.29. no set mld fast-leave 189
5.2.10.30. set mld groupmembership-interval 190
5.2.10.31. no set mld groupmembership-interval 190
5.2.10.32. set mld maxresponse 190
5.2.10.33. no set mld maxresponse 190
5.2.10.34. set mld mcrtrexpiretime 191
5.2.10.35. no set mld mcrtrexpiretime 191
5.2.11. MLD Snooping Querier Commands 191
5.2.11.1. show ipv6 mld snooing querier 191
5.2.11.2. show ipv6 mld snooping querier vlan 192
5.2.11.3. show ipv6 mld snooping querier detail 192
5.2.11.4. ipv6 mld snooping querier 193
5.2.11.5. no ipv6 mld snooping querier 193
5.2.11.6. ipv6 mld snooping querier address 193
5.2.11.7. no ipv6 mld snooping querier address 194
5.2.11.8. ipv6 mld snooping querier query-interval 194
5.2.11.9. no ipv6 mld snooping querier querier-interval 194
5.2.11.10. ipv6 mld snooping querier querier-expiry-interval 194

5.2.11.11. no ipv6 mld snooping querier querier-expiry-interval 194
5.2.11.12. ipv6 mld snooping querier vlan 195
5.2.11.13. no ipv6 mld snooping querier vlan 195
5.2.11.14. ipv6 mld snooping querier vlan address 195
5.2.11.15. no ipv6 mld snooping querier vlan address 195
5.2.11.16. ipv6 mld snooping querier vlan election participate 196
5.2.11.17. no ipv6 mld snooping querier vlan election participate 196
5.2.12. Port-Channel/LAG (802.3ad) Commands 196
5.2.12.1. show interface port-channel brief 197
5.2.12.2. show interface port-channel 198
5.2.12.3. show interface port-channel system priority 201
5.2.12.4. show lacp actor 202
5.2.12.5. show lacp interface 202
5.2.12.6. interface port-channel 202
5.2.12.7. staticcapability 203
5.2.12.8. no staticcapability 203
5.2.12.9. port-channel linktrap 203
5.2.12.10. no port-channel linktrap 203
5.2.12.11. port-channel load-balance 204
5.2.12.12. no port-channel load-balance 204
5.2.12.13. load-balance 204
5.2.12.14. no load-balance 205
5.2.12.15. port-channel system priority 205
5.2.12.16. no port-channel system priorty 206
5.2.12.17. lacp 206
5.2.12.18. no lacp 206
5.2.12.19. lacp all 206
5.2.12.20. no lacp 206
5.2.12.21. lacp admin key 207
5.2.12.22. no lacp admin key 207
5.2.12.23. lacp actor admin key 207
5.2.12.24. no lacp actor admin key 207
5.2.12.25. lacp actor admin state 208
5.2.12.26. no lacp actor admin state 208

5.2.12.27. lacp actor port priority 208
5.2.12.28. no lacp actor port priority 209
5.2.12.29. min-links 209
5.2.12.30. no min-links 209
5.2.12.31. lacp fallback 209
5.2.12.32. no lacp fallback 210
5.2.12.33. lacp fallback timeout 210
5.2.12.34. no lacp fallback timeout 210
5.2.12.35. channel-group 210
5.2.12.36. no channel-group 211
5.2.12.37. delete-channel-group 211
5.2.12.38. port lacpmode enable all 211
5.2.12.39. port lacptimeout 211
5.2.13. Storm Control 212
5.2.13.1. show storm-control 212
5.2.13.2. storm-control Configuration 214
5.2.13.3. storm-control broadcast 214
5.2.13.4. no storm-control broadcast 214
5.2.13.5. storm-control broadcast action 215
5.2.13.6. no storm-control broadcast action 215
5.2.13.7. storm-control broadcast rate 215
5.2.13.8. no storm-control broadcast rate 216
5.2.13.9. storm-control broadcast level 216
5.2.13.10. no storm-control broadcast level 216
5.2.13.11. storm-control multicast 217
5.2.13.12. no storm-control multicast 217
5.2.13.13. storm-control multicast action 217
5.2.13.14. no storm-control multicast action 218
5.2.13.15. storm-control multicast level 218
5.2.13.16. no storm-control multicast level 218
5.2.13.17. storm-control multicast rate 218
5.2.13.18. no storm-control multicast rate 219
5.2.13.19. storm-control unicast 219
5.2.13.20. no storm-control unicast 219

5.2.13.21. storm-control unicast action 220
5.2.13.22. no storm-control unicast action 220
5.2.13.23. storm-control unicast level 220
5.2.13.24. no storm-control unicast level 221
5.2.13.25. storm-control unicast rate 221
5.2.13.26. no storm-control unicast rate 221
5.2.14. Port Mirror Commands 222
5.2.14.1. show port-mirror session 222
5.2.14.2. port-monitor session source 223
5.2.14.3. no port-monitor session source 224
5.2.14.4. port-monitor session destination 224
5.2.14.5. no port-monitor session destination 225
5.2.14.6. port-monitor session filter 225
5.2.14.7. no port-monitor session filter 226
5.2.14.8. port-monitor session mode 226
5.2.14.9. no port-monitor session mode 226
5.2.14.10. no port-monitor session 226
5.2.14.11. no port-monitor 227
5.2.15. Link State 227
5.2.15.1. show link state 227
5.2.15.2. link state group action 228
5.2.15.3. link state group 228
5.2.16. Port-backup Commands 229
5.2.16.1. show port-backup 229
5.2.16.2. port-backup 229
5.2.16.3. no port-backup 229
5.2.16.4. port-backup group 230
5.2.16.5. no port-backup group 230
5.2.16.6. port-backup group active 230
5.2.16.7. no port-backup group active 230
5.2.16.8. port-backup group backup 230
5.2.16.9. no port-backup group backup 231
5.2.16.10. port-backup group enable 231
5.2.16.11. port-backup group mac-move-update 231

5.2.16.12. no port-backup group mac-move-update 231
5.2.16.13. port-backup group failback-time 232
5.2.16.14. no port-backup group failback-time 232
5.3. Provisioning (IEEE 802.1p) Commands 233
5.3.1. switchport priority all 233
5.3.2. no switchport priority all 233
5.3.3. switchport priority 233
5.3.4. no switchport priority 233
5.4. Management Commands 234
5.4.1. Network Commands 234
5.4.1.1. show ip interface 234
5.4.1.2. show ip filter 234
5.4.1.3. mtu 235
5.4.1.4. no mtu 235
5.4.1.5. interface vlan 235
5.4.1.6. ip address 235
5.4.1.7. no ip addess 236
5.4.1.8. ip default-gateway 236
5.4.1.9. ip address dhcp 237
5.4.1.10. no ip address dhcp 237
5.4.1.11. ip filter 237
5.4.1.12. no ip filter 238
5.4.1.13. ip filter <name> {ipv4|ipv6}<ipAddr>[<mask>] 238
5.4.1.14. no ip filter<name> 238
5.4.2. Serial Interface Commands 238
5.4.2.1. show line console 238
5.4.2.2. line console 239
5.4.2.3. baudrate 239
5.4.2.4. no baudrate 240
5.4.2.5. exec-timeout 240
5.4.2.6. no exec-timeout 240
5.4.2.7. password-threshold 240
5.4.2.8. no password-threshold 241
5.4.2.9. silent-time 241

5.4.2.10. no silent-time 241
5.4.2.11. terminal length 241
5.4.2.12. line password 242
5.4.3. Telnet Session Commands 242
5.4.3.1. telnet 242
5.4.3.2. show line vty 243
5.4.3.3. line vty 243
5.4.3.4. exec-timeout 243
5.4.3.5. no exec-time out 244
5.4.3.6. password-threshold 244
5.4.3.7. no password-threshold 245
5.4.3.8. maxsessions 245
5.4.3.9. no maxsessions 245
5.4.3.10. server enable 245
5.4.3.11. no server enable 246
5.4.3.12. sessions 246
5.4.3.13. no sessions 246
5.4.3.14. telnet sessions 246
5.4.3.15. no telnet sessions 247
5.4.3.16. telnet maxsessions 247
5.4.3.17. no telnet maxsessions 247
5.4.3.18. telnet exec-timeout 247
5.4.3.19. no telnet exec-timeout 248
5.4.3.20. show telnet 248
5.4.4. SNMP Server Commands 248
5.4.4.1. show snmp 248
5.4.4.2. snmp-server sysname 250
5.4.4.3. snmp-server location 250
5.4.4.4. snmp-server contact 251
5.4.4.5. snmp-server community 251
5.4.4.6. no snmp-server community <community-string> 252
5.4.4.7. snmp-server community-group 252
5.4.4.8. no snmp-server community-group <community-string> 252
5.4.4.9. show snmp engineid 252

5.4.4.10. snmp-server engineid 253
5.4.4.11. no snmp-server engineid 253
5.4.4.12. show snmp filters 254
5.4.4.13. snmp-server filter 254
5.4.4.14. no snmp-server filter <filter-name> [<oid-tree >] 255
5.4.4.15. show snmp user 255
5.4.4.16. snmp-server user 256
5.4.4.17. no snmp-server user 256
5.4.4.18. show snmp group 256
5.4.4.19. snmp-server group 258
5.4.4.20. no snmp-server group 258
5.4.4.21. show snmp views 258
5.4.4.22. snmp-server view 259
5.4.4.23. no snmp-server view 260
5.4.5. SNMP Trap Commands 260
5.4.5.1. snmp-server host <host-addr> traps 260
5.4.5.2. no snmp-server host <host-addr> 261
5.4.5.3. *show* trapflags 261
5.4.5.4. snmp trap link-status all 262
5.4.5.5. no snmp trap link-status all 263
5.4.5.6. snmp-server enable traps acl-trapflags 263
5.4.5.7. no snmp-server enable traps acl-trapflags 263
5.4.5.8. snmp-server enable traps authentication 263
5.4.5.9. no snmp-server enable traps authentication 264
5.4.5.10. snmp-server enable traps bgp state-changes limited 264
5.4.5.11. no snmp-server enable traps bgp state-changes limited 264
5.4.5.12. snmp-server enable traps fan 264
5.4.5.13. no snmp-server enable traps fan 264
5.4.5.14. snmp-server enable traps linkmode 265
5.4.5.15. no snmp-server enable traps linkmode 265
5.4.5.16. snmp-server enable traps multiusers 265
5.4.5.17. snmp-server enable traps ospf 266
5.4.5.18. no snmp-server enable traps ospf 266
5.4.5.19. snmp-server enable traps ospfv3 266

5.4.5.20. no snmp-server enable traps ospfv3 266
5.4.5.21. snmp-server enable traps pim 267
5.4.5.22. no snmp-server enable traps pim 267
5.4.5.23. snmp-server enable traps powersupply 267
5.4.5.24. no snmp-server enable traps powersupply 267
5.4.5.25. snmp-server enable traps stpmode 268
5.4.5.26. no snmp-server enable traps stpmode 268
5.4.5.27. snmp-server enable traps temperature 268
5.4.5.28. no snmp-server enable traps temperature 268
5.4.5.29. snmp-server enable traps transceiver 268
5.4.5.30. no snmp-server enable traps transceiver 269
5.4.5.31. snmp-server enable traps violation 269
5.4.5.32. no snmp-server enable traps violation 269
5.4.5.33. show snmp source-interface 269
5.4.5.34. snmptrap source-interface 270
5.4.5.35. no snmptrap source-interface 271
5.4.5.36. snmp trap link-status 271
5.4.5.37. no snmp trap link-status 271
5.4.6. SNMP Inform Commands 271
5.4.6.1. snmp-server host <host-addr> informs 271
5.4.6.2. no snmp-server host <host-addr> 272
5.4.7. Secure Shell (SSH) Commands 272
5.4.7.1. show ip ssh 272
5.4.7.2. show ip ssh user-public-key current-user 273
5.4.7.3. show ip ssh user-public-key who-has-key 273
5.4.7.4. ip ssh 274
5.4.7.5. no ip ssh 274
5.4.7.6. ip ssh maxsessions 274
5.4.7.7. no ip ssh maxsessions 274
5.4.7.8. ip ssh port 275
5.4.7.9. no ip ssh port 275
5.4.7.10. ip ssh timeout 275
5.4.7.11. no ip ssh timeout 275
5.4.7.12. ip ssh user-password-auth 275

5.4.7.13. no ip ssh user-password-auth 276
5.4.7.14. ip ssh user-public-key-auth 276
5.4.7.15. no ip ssh user-public-key-auth 276
5.4.8. Management Security Commands 276
5.4.8.1. crypto key generation {RSA|DSA} 276
5.4.8.2. no crypto key generate {RSA | DSA} 277
5.4.8.3. crypto certificate generation 277
5.4.8.4. no crypto certificate generate 277
5.4.9. DHCP Client Commands 277
5.4.9.1. dhcp client vendor-id-option 277
5.4.9.2. no dhcp client vendor-id-option 278
5.4.9.3. dhcp client vendor-id-option-string 278
5.4.9.4. no dhcp client vendor-id-option-string 278
5.4.9.5. show dhcp client vendor-id-option 278
5.4.9.6. show dhcp lease 279
5.4.10. sfFlow Commands 279
5.4.10.1. show sflow agent 279
5.4.10.2. show sflow pollers 280
5.4.10.3. show sflow receivers 280
5.4.10.4. show sflow samplers 281
5.4.10.5. show sflow source-interface 282
5.4.10.6. sflow receiver maximum datagram 282
5.4.10.7. no sflow receiver maxdatagram <index> 282
5.4.10.8. sflow receiver owner 282
5.4.10.9. no sflow receiver <index> 283
5.4.10.10. sflow receiver ip 283
5.4.10.11. no sflow receiver <index> ip 283
5.4.10.12. sflow receiver port 284
5.4.10.13. no sflow receiver <index> port 284
5.4.10.14. sflow poller interval 284
5.4.10.15. no sflow poller interval 285
5.4.10.16. sflow sampler index 285
5.4.10.17. no sflow sampler 285
5.4.10.18. sflow poller index 285

5.4.10.19. no sflow poller 285
5.4.10.20. sflow source-interface 286
5.4.10.21. no sflow source-interface 286
5.4.10.22. sflow sampler rate 286
5.4.10.23. no sflow sampler rate 287
5.4.10.24. sflow sampler maxheadersize 287
5.4.10.25. no sflow sampler maxheadersize 287
5.4.11. Service Port Commands 287
5.4.11.1. show serviceport 287
5.4.11.2. show serviceport ipv6 dhcp statistics 288
5.4.11.3. show serviceport ipv6 neighbors 290
5.4.11.4. serviceport ip 291
5.4.11.5. serviceport protocol 291
5.4.11.6. serviceport ipv6 enable 292
5.4.11.7. no serviceport ipv6 enable 292
5.4.11.8. serviceport ipv6 address 292
5.4.11.9. no serviceport ipv6 address 293
5.4.11.10. serviceport ipv6 gateway 293
5.4.11.11. no serviceport ipv6 gateway 293
5.4.11.12. clear serviceport ipv6 dhcp statistics 294
5.4.11.13. serviceport ipv6 neighbor 294
5.4.11.14. no serviceport ipv6 neighbor 294
5.4.12. Time Range Commands 294
5.4.12.1. show time-range 294
5.4.12.2. time-range 295
5.4.12.3. no time-range 295
5.4.12.4. time-range <name> 295
5.4.12.5. no time-range <name> 296
5.4.12.6. absolute 296
5.4.12.7. no absolute 297
5.4.12.8. periodic 297
5.4.12.9. no periodic 297
5.4.13. Command Scheduler Commands 298
5.4.13.1. kron occurrence 298

5.4.13.2. no kron occurrence <name> 298
5.4.13.3. policy-list <name> 299
5.4.13.4. no policy-list <name> 299
5.4.13.5. kron policy-list 299
5.4.13.6. no kron policy-list <name> 299
5.4.13.7. cli <line><line><line> … 300
5.4.13.8. no cli <line> <line> <line> … 300
5.4.14. Switch Database Management Template Commands 300
5.4.14.1. show sdm prefer 300
5.4.14.2. sdm prefer 301
5.4.14.3. no sdm prefer 302
5.4.15. Remote Monitoring Commands 302
5.4.15.1. show rmon alarms 303
5.4.15.2. show rmon collection history 304
5.4.15.3. show rmon events 305
5.4.15.4. show rmon history 306
5.4.15.5. show rmon log 309
5.4.15.6. show rmon statistics interfaces 310
5.4.15.7. show rmon hcalarms 312
5.4.15.8. rmon alarm 314
5.4.15.9. no rmon alarm 315
5.4.15.10. rmon hcalarm 315
5.4.15.11. no rmon hcalarm 316
5.4.15.12. rmon event 316
5.4.15.13. no rmon event 317
5.4.15.14. rmon collection history 317
5.4.15.15. no rmon collection history 318
5.4.16. Statistics Application Commands 318
5.4.16.1. stats group (Global Config) 318
5.4.16.2. stats flow-based (Global Config) 320
5.4.16.3. stats flow-based reporting 321
5.4.16.4. stats group (Interface Config) 321
5.4.16.5. stats flow-based (Interface Config) 322
5.4.16.6. show stats group 322

5.4.16.7. show stats flow-based 324
5.5. Spanning Tree Protocol Commands 327
5.5.1. show spanning-tree 327
5.5.2. show spanning-tree interface 328
5.5.3. show spanning-tree vlan 328
5.5.4. show spanning-tree mst detailed 329
5.5.5. show spanning-tree mst summary 329
5.5.6. show spanning-tree mst port detailed 330
5.5.7. show spanning-tree mst port summary 331
5.5.8. show spanning-tree summary 332
5.5.9. show spanning-tree brief 332
5.5.10. spanning-tree 333
5.5.11. no spanning-tree 333
5.5.12. spanning-tree bpdu-forwarding 333
5.5.13. no spanning-tree bpdu-forwarding 333
5.5.14. spanning-tree protocol-migration 334
5.5.15. spanning-tree configuration name 334
5.5.16. no spanning-tree configuration name 334
5.5.17. spanning-tree configuration revision 334
5.5.18. no spanning-tree configuration revision 335
5.5.19. spanning-tree mode 335
5.5.20. no spanning-tree mode 335
5.5.21. spanning-tree forward-time 335
5.5.22. no spanning-tree forward-time 336
5.5.23. spanning-tree max-age 336
5.5.24. no spanning-tree max-age 336
5.5.25. spanning-tree forward-time max-age 336
5.5.26. spanning-tree max-hops 337
5.5.27. no spanning-tree max-hops 337
5.5.28. spanning-tree hold-count 337
5.5.29. no spanning-tree hold-count 337
5.5.30. spanning-tree mst instance 338
5.5.31. no spanning-tree mst instance 338
5.5.32. spanning-tree mst priority 338

5.5.33. no spanning-tree mst priority 339
5.5.34. spanning-tree mst vlan 339
5.5.35. no spanning-tree mst vlan 339
5.5.36. spanning-tree mst 339
5.5.37. no spanning-tree mst 340
5.5.38. spanning-tree port mode 340
5.5.39. no spanning-tree port mode 341
5.5.40. spanning-tree port model all 341
5.5.41. no spanning-tree port mode all 341
5.5.42. spaning-tree auot-edge 341
5.5.43. no spanning-tree auto-edge 342
5.5.44. spanning-tree cost 342
5.5.45. no spanning-tree cost 342
5.5.46. spanning-tree edgeport 342
5.5.47. no spanning-tree edgeport 343
5.5.48. spanning-tree edgeport bpduguard 343
5.5.49. no spanning-tree edgeport bpduguard 343
5.5.50. spanning-tree bpduguard 343
5.5.51. no spanning-tree bpduguard 344
5.5.52. spanning-tree guard 344
5.5.53. no spanning-tree guard 344
5.5.54. spanning-tree tcnguard 344
5.5.55. no spanning-tree tcnguard 345
5.6. System Log Commands 346
5.6.1. show logging 346
5.6.2. show logging buffered 346
5.6.3. logging buffered 348
5.6.4. logging buffered threshold 348
5.6.5. logging buffered severity level 348
5.6.6. logging buffered wrap 349
5.6.7. clear logging buffered 349
5.6.8. show logging traplogs 349
5.6.9. show logging hosts 350
5.6.10. logging host 351

5.6.11. logging host remove 351
5.6.12. logging host reconfigure 352
5.6.13. logging syslog 352
5.6.14. logging syslog port 352
5.6.15. logging syslog facility 353
5.6.16. logging syslog source-interface 353
5.6.17. logging console 353
5.6.18. logging console severity level 354
5.6.19. logging monitor 354
5.6.20. logging monitory severity level 354
5.6.21. show logging cli-command-log 355
5.6.22. logging cli-command 356
5.6.23. clear cli-command-log 356
5.7. Email Alert and Mail Server Commands 357
5.7.1. show logging email config 357
5.7.2. show logging email statistics 358
5.7.3. show mail-server config 358
5.7.4. logging email 359
5.7.5. logging email urgent and non-urgent 359
5.7.6. logging email logtime 360
5.7.7. logging email message-type and subject 360
5.7.8. logging email message-type and to-addr 360
5.7.9. logging email from-addr 361
5.7.10. mail-server configuration 361
5.7.11. mail-server security 362
5.7.12. mail-server port 362
5.7.13. mail-server username 362
5.7.14. mail-server password 363
5.7.15. clear logging email statistics 363
5.8. Script Management Commands 364
5.8.1. script apply 364
5.8.2. script delete 364
5.8.3. script list 364
5.8.4. script show 365

5.8.5. script validate 367
5.9. User Account Management Commands 369
5.9.1. show users 369
5.9.2. show users long 369
5.9.3. show users accounts 370
5.9.4. show passwords configuration 372
5.9.5. show passwords result 373
5.9.6. username 374
5.9.7. no username 375
5.9.8. username <username> unlock 375
5.9.9. passwords aging 375
5.9.10. no passwords aging 375
5.9.11. passwords history 376
5.9.12. no passwords history 376
5.9.13. passwords lock-out 376
5.9.14. no passwords lock-out 377
5.9.15. passwords min-length 377
5.9.16. no passwords min-length 377
5.9.17. passwords strength-check 377
5.9.18. no passwords strength-check 378
5.9.19. passwords strength maximum 378
5.9.20. no passwords strength maximum 378
5.9.21. passwords strength minimum 378
5.9.22. no passwords strength minimum 379
5.9.23. passwords strength exclude-keyword 379
5.9.24. no passwords strength exclude-keyword 379
5.9.25. show users login-history 379
5.9.26. user password override-complexity-check 380
5.9.27. user role 381
5.10. Port-based Network Access Control Commands 382
5.10.1. show authentication methods 382
5.10.2. show dot1x 383
5.10.3. show dot1x authentication-history 388
5.10.4. show dot1x clients 389

5.10.5. show dot1x users 390
5.10.6. aaa authentication dot1x default 390
5.10.7. no aaa authentication dot1x default 391
5.10.8. clear dot1x statistics 391
5.10.9. clear dot1x authentication-history 391
5.10.10. clear RADIUS statistics 391
5.10.11. dot1x eapolflood 392
5.10.12. no dot1x eapolflood 392
5.10.13. dot1x dynamic-vlan enable 392
5.10.14. no dot1x dynamic-vlan enable 392
5.10.15. dot1x guest-vlan 393
5.10.16. no dot1x guest-vlan 393
5.10.17. dot1x initialize 393
5.10.18. dot1x mac-auth-bypass 393
5.10.19. no dot1x mac-auth-bypass 394
5.10.20. dot1x max-req 394
5.10.21. no dot1x max-req 394
5.10.22. dot1x max-users 394
5.10.23. no dot1x max-users 395
5.10.24. dot1x port-control 395
5.10.25. no dot1x port-control 395
5.10.26. dot1x port-control all 395
5.10.27. no dot1x port-control all 396
5.10.28. dot1x re-authenticate 396
5.10.29. dot1x re-authentication 396
5.10.30. no dot1x re-authentication 396
5.10.31. dot1x system-auth-control 397
5.10.32. no dot1x system-auth-control 397
5.10.33. dot1x timeout 397
5.10.34. no dot1x timeout 398
5.10.35. dot1x unauthenticated-vlan 398
5.10.36. no dot1x unauthenticated-vlan 399
5.10.37. dot1x user 399
5.10.38. no dot1x user 399

5.11. AAA Commands 400
5.11.1. show accounting 400
5.11.2. show accounting methods 400
5.11.3. aaa authentication login 401
5.11.4. no aaa authentication login 402
5.11.5. aaa accounting 402
5.11.6. no aaa accounting 403
5.11.7. accounting 404
5.11.8. no aaa accounting 404
5.11.9. clear aaa ias-users 404
5.11.10. clear accounting statistics 405
5.12. RADIUS Commands 406
5.12.1. show radius 406
5.12.2. show radius accounting 407
5.12.3. show radius servers 410
5.12.4. show radius statistics 414
5.12.5. show radius source-interface 416
5.12.6. authentication network radius 416
5.12.7. no authorization network radius 416
5.12.8. clear radius dynamic-author statistics 416
5.12.9. radius accounting mode 417
5.12.10. no radius accounting mode 417
5.12.11. radius server attribute 4 417
5.12.12. no radius server attribute 4 418
5.12.13. radius server attribute 95 418
5.12.14. no radius server attribute 95 418
5.12.15. radius server attribute mschapv2 418
5.12.16. no radius server attribute mschapv2 419
5.12.17. radius server deadtime 419
5.12.18. no radius server deadtime 419
5.12.19. radius server host 419
5.12.20. no radius server host 420
5.12.21. radius server host link-local 421
5.12.22. no radius server host link-local 422

5.12.23. radius server key 422
5.12.24. radius server primary 422
5.12.25. radius server retransmit 423
5.12.26. no radius server retransmit 423
5.12.27. radius server timeout 423
5.12.28. no radius server timeout 423
5.12.29. radius source-interface 424
5.12.30. no radius source-interface 424
5.13. TACACS+ Commands 425
5.13.1. show tacacs 425
5.13.2. show tacacs source-interface 426
5.13.3. tacacs-server host 426
5.13.4. tacacs-server host link-local 427
5.13.5. no tacacs-server host link-local 427
5.13.6. tacacs-server key 427
5.13.7. no tacacs-server key 427
5.13.8. tacacs-server keystring 428
5.13.9. tacacs-server timeout 428
5.13.10. no tacacs-server timeout 428
5.13.11. key 429
5.13.12. no key 429
5.13.13. keystring 429
5.13.14. port 429
5.13.15. no port 430
5.13.16. priority 430
5.13.17. no priority 430
5.13.18. timeout 430
5.13.19. no timeout 431
5.13.20. tacacs-server source-interface 431
5.13.21. no tacacs-server source-interface 431
5.13.22. clear tacacs 432
5.14. Security Commands 433
5.14.1. show port-security 433
5.14.2. show port-security dynamic 434

5.14.3. show port-security static 434
5.14.4. show port-security violation 435
5.14.5. port-security 436
5.14.6. no port-security 436
5.14.7. port-security max-dynamic 436
5.14.8. no port-security max-dynamic 436
5.14.9. port-security max-static 437
5.14.10. no port-security max-static 437
5.14.11. port-security mac-address 437
5.14.12. no port-security mac-address 437
5.14.13. port-security mac-address move 438
5.14.14. port-security mac-address sticky 438
5.14.15. no port-security mac-address sticky 438
5.14.16. port-security violation shutdown 439
5.14.17. no port-security violation 439
5.15. LLDP (Link Layer Discovery Protocol) Commands 440
5.15.1. show lldp 440
5.15.2. show lldp interface 440
5.15.3. show lldp statistics 441
5.15.4. show lldp remote-device 442
5.15.5. show lldp remote-device detail 443
5.15.6. show lldp local-device 444
5.15.7. show lldp local-device detail 445
5.15.8. show lldp dcbx interface 446
5.15.9. show lldp tlv-select interface 448
5.15.10. show lldp remote-comparison 448
5.15.11. lldp notification 449
5.15.12. no lldp notification 449
5.15.13. lldp notification-interval 449
5.15.14. no lldp notification-interval 449
5.15.15. lldp receive 450
5.15.16. no lldp receive 450
5.15.17. lldp transmit 450
5.15.18. no lldp transmit 450

5.15.19. lldp transmit-mgmt 451
5.15.20. no lldp transmit-mgmt 451
5.15.21. lldp transmit-tlv 451
5.15.22. no lldp transmit-tlv 451
5.15.23. lldp timers 452
5.15.24. no lldp timers 452
5.15.25. lldp tx-delay 452
5.15.26. no lldp tx-delay 452
5.15.27. lldp dcbx version 453
5.15.28. no lldp dcbx version 453
5.15.29. lldp dcbx port-role 454
5.15.30. no lldp dcbx port-role 454
5.15.31. lldp tlv-select dcbxp 455
5.15.32. no lldp tlv-select 455
5.15.33. lldp mgmt-address 455
5.15.34. no lldp mgmt-address 456
5.15.35. lldp portid-subtype 456
5.15.36. no lldp portid-subtype 457
5.15.37. data-center-bridging 457
5.16. System Utilities 458
5.16.1. Clear 458
5.16.1.1. clear arp 458
5.16.1.2. clear traplog 458
5.16.1.3. clear eventlog 458
5.16.1.4. clear logging buffered 458
5.16.1.5. clear config 459
5.16.1.6. clear pass 459
5.16.1.7. clear counters 459
5.16.1.8. clear vlan 459
5.16.1.9. clear igmp snooping 460
5.16.1.10. clear ip filter 460
5.16.1.11. clear dot1x authentication-history 460
5.16.1.12. clear radius statistics 460
5.16.1.13. clear host 461

5.16.1.14. clear port-security dynamic 461
5.16.1.15. clear ip arp-cache 461
5.16.1.16. clear lldp statistics 461
5.16.1.17. clear lldp remote-data 462
5.16.1.18. clear ipv6 neighbors 462
5.16.1.19. clear ipv6 statistics 462
5.16.1.20. clear ipv6 dhcp statistics 462
5.16.1.21. clear ipv6 dhcp statistics per interface 463
5.16.1.22. enable password 463
5.16.1.23. clear cpu-traffic counters 464
5.16.1.24. clear cpu-traffic traces 464
5.16.1.25. clear default interface 464
5.16.1.26. clear network ipv6 dhcp statistics 465
5.16.2. copy 465
5.16.2.1. copy *source* <url> 465
5.16.2.2. copy <url> destination 466
5.16.2.3. copy running-config 467
5.16.2.4. copy {startup-config backup-config | backup-config startup-config} 467
5.16.3. delete 467
5.16.4. erase application 467
5.16.5. erase startup-config 468
5.16.6. erase user public key 468
5.16.7. dir 468
5.16.8. show bootvar 469
5.16.9. Ping Commands 470
5.16.9.1. ping 470
5.16.9.2. ping ipv6 470
5.16.9.3. ping ipv6 interface 471
5.16.10. Traceroute 472
5.16.10.1. traceroute 472
5.16.10.2. traceroute ipv6 473
5.16.11. reload 473
5.16.12. configure 474
5.16.13. disconnect 474

5.16.14. hostname 474
5.16.15. quit 475
5.16.16. AutoInstall commands 475
5.16.16.1. show autoinstall 475
5.16.16.2. boot-system autoinstall 476
5.16.16.3. boot-system host autoinstall 476
5.16.16.4. no boot-system host autoinstall 476
5.16.16.5. boot-system host autosave 476
5.16.16.6. no boot-system host autosave 477
5.16.16.7. boot-system host autoreboot 477
5.16.16.8. no boot-system host autoreboot 477
5.16.16.9. boot-system host upgrade 477
5.16.16.10. no boot-system host upgrade 478
5.16.16.11. boot-system host retrycount 478
5.16.17. Capture CPU packet commands 478
5.16.17.1. show capture 478
5.16.17.2. capture start 479
5.16.17.3. capture stop 479
5.16.17.4. capture {file | remote | line} 480
5.16.17.5. capture remote port 480
5.16.17.6. capture file size 481
5.16.17.7. capture line wrap 481
5.16.17.8. no capture line wrap 481
5.16.18. set clibanner 481
5.16.19. no set clibanner 482
5.16.20. show clibanner 482
5.16.21. Link-Flap commands 482
5.16.21.1. show link-flap 482
5.16.21.2. link-flap 483
5.16.22. Loop Detection commands 483
5.16.22.1. show loop-detection 483
5.16.22.2. show loop-detection statistics 483
5.16.22.3. loop-detection (Global Config) 484
5.16.22.4. loop-detection (Interface Config) 485

5.16.22.5. loop-detection action 485
5.16.23. In-Service Software Upgrade 485
5.16.23.1. show issu status 486
5.16.23.2. show issu status details 486
5.16.24. file verify 486
5.17. DHCP Snooping Commands 488
5.17.1. show ip dhcp snooping 488
5.17.2. show ip dhcp snooping per interface 489
5.17.3. show ip dhcp snooping binding 490
5.17.4. show ip dhcp snooping database 491
5.17.5. show ip dhcp snooping information all 491
5.17.6. show ip dhcp snooping information statistics 492
5.17.7. show ip dhcp snooping information agent-option 493
5.17.8. show ip dhcp snooping information per vlan 493
5.17.9. show ip dhcp snooping information circuit-id 493
5.17.10. show ip dhcp snooping information remote-id 494
5.17.11. show ip dhcp snooping information interface 494
5.17.12. ip dhcp snooping 495
5.17.13. ip dhcp snooping vlan 495
5.17.14. ip dhcp snooping verify mac-address 495
5.17.15. ip dhcp snooping database 495
5.17.16. ip dhcp snooping database write-delay 496
5.17.17. ip dhcp snooping binding 496
5.17.18. ip dhcp snooping information option 497
5.17.19. ip dhcp snooping information option circuit-id 497
5.17.20. ip dhcp snooping information option remote-id 497
5.17.21. ip dhcp snooping information option vlan 498
5.17.22. ip dhcp snooping information option trust 498
5.17.23. ip dhcp snooping limit 498
5.17.24. ip dhcp snooping log-invalid 499
5.17.25. ip dhcp snooping trust 499
5.17.26. ip dhcp snooping trust 499
5.17.27. clear ip dhcp snooping binding 499
5.17.28. clear ip dhcp snooping statistics 500

5.17.29. clear ip dhcp snooping information statistics 500
5.18. IP Source Guard (ISG) Commands 501
5.18.1. Show commands 501
5.18.1.1. show ip verify 501
5.18.1.2. show ip verify source 502
5.18.1.3. show ip source binding 502
5.18.2. Configuration commands 503
5.18.2.1. ip verify source 503
5.18.2.2. ip verify binding 503
5.19. Dynamic ARP Instpection (DAI) Command 505
5.19.1. Show commands 505
5.19.1.1. show ip arp instpection statistics 505
5.19.1.2. show ip arp inspection 506
5.19.1.3. show ip arp inspection interfaces 506
5.19.1.4. show arp access-list 507
5.19.2. Configuration commands 507
5.19.2.1. ip arp inspection validate 507
5.19.2.2. ip arp inspection vlan 507
5.19.2.3. ip arp inspection vlan logging 508
5.19.2.4. ip arp inspection filter 508
5.19.2.5. ip arp inspection trust 509
5.19.2.6. ip arp inspection limit 509
5.19.2.7. arp access-list 509
5.19.2.8. permit ip host mac host 510
5.19.2.9. clear ip arp inspection statistics 510
5.20. Differenciated Service Commands 511
5.20.1. General commands 512
5.20.1.1. diffserv 512
5.20.1.2. no diffserv 512
5.20.2. Class commands 513
5.20.2.1. class-map 513
5.20.2.2. no class-map 514
5.20.2.3. rename 514
5.20.2.4. match any 514

5.20.2.5. match class-map 515
5.20.2.6. no match class-map 515
5.20.2.7. match cos 516
5.20.2.8. match secondary-cos 516
5.20.2.9. match destination-address mac 516
5.20.2.10. match dstip 517
5.20.2.11. match dstI4port 517
5.20.2.12. match ethertype 518
5.20.2.13. match ip dscp 518
5.20.2.14. match ip precedence 519
5.20.2.15. match ip tos 519
5.20.2.16. match protocol 520
5.20.2.17. match source-address mac 520
5.20.2.18. match scrip 521
5.20.2.19. match srcI4port 521
5.20.2.20. match vlan 522
5.20.2.21. match secondary-vlan 522
5.20.2.22. match dstipv6 523
5.20.2.23. match srcipv6 523
5.20.2.24. match ip6flowlbl 523
5.20.3. Policy commands 524
5.20.3.1. assign-queue 524
5.20.3.2. drop 525
5.20.3.3. mirror 525
5.20.3.4. redirect 525
5.20.3.5. conform-color 526
5.20.3.6. mark cos 526
5.20.3.7. mark cos-as-sec-cos 527
5.20.3.8. class 527
5.20.3.9. no class 527
5.20.3.10. mark ip-dscp 528
5.20.3.11. mark ip-precedence 528
5.20.3.12. police-simple 528
5.20.3.13. police-single-rate 529

5.20.3.14. police-two-rate 530
5.20.3.15. policy-map 531
5.20.3.16. policy-map rename 531
5.20.4. Service commands 532
5.20.4.1. service-policy 532
5.20.4.2. no service-policy 533
5.20.5. Show commands 533
5.20.5.1. show class-map 533
5.20.5.2. show diffserv 534
5.20.5.3. show diffserv service 535
5.20.5.4. show diffserv service brief 536
5.20.5.5. show policy-map 536
5.20.5.6. show policy-map interface 538
5.20.5.7. show service-policy 539
5.21. ACL Commands 540
5.21.1. Show commands 540
5.21.1.1. show mac access-lists name 540
5.21.1.2. show mac access-lists 541
5.21.1.3. show ip access-lists 542
5.21.1.4. show access-lists interface 543
5.21.1.5. show access-lists vlan 544
5.21.2. Configuration commands 545
5.21.2.1. mac access-list extended 545
5.21.2.2. mac access-list extended rename 545
5.21.2.3. mac access-list resequence 545
5.21.2.4. mac access-list 546
5.21.2.5. mac access-group 548
5.21.2.6. ip access-list 549
5.21.2.7. ip access-list rename 549
5.21.2.8. ip access-list resequence 550
5.21.2.9. access-list (ip) 550
5.21.2.10. no access-list 554
5.21.2.11. ip access-group 554
5.21.2.12. no ip access-group 555

5.21.2.13. {deny|permit} 556
5.22. IPv6 ACL Commands 559
5.22.1. Show commands 559
5.22.1.1. show ipv6 access-lists 559
5.22.2. Configuration Commands 560
5.22.2.1. ipv6 access-list 560
5.22.2.2. ipv6 access-list rename 561
5.22.2.3. ipv6 access-list resequence 561
5.22.2.4. {deny|permit} 562
5.22.2.5. no rule-id 565
5.22.2.6. ipv6 traffic-filter 565
5.23. CoS (Class of Service) Command 567
5.23.1. Show commands 567
5.23.1.1. show queue cos-map 567
5.23.1.2. show queue ip-dscp-mapping 567
5.23.1.3. show queue trust 568
5.23.1.4. show queue cos-queue 568
5.23.1.5. show queue random-detect 569
5.23.2. Configuration commands 570
5.23.2.1. queue cos-map 570
5.23.2.2. queue trust 571
5.23.2.3. queue cos-queue min-bandwidth 572
5.23.2.4. queue cos-queue strict 572
5.23.2.5. queue cos-queue traffic-shape 573
5.23.2.6. queue cos-queue random-detect 574
5.23.2.7. random-detect exponential-weighting-constant 574
5.23.2.8. random-detect queue-parms 575
5.24. iSCSI Optimization Commands 576
5.24.1. show iscsi 576
5.24.2. show iscsi sessions 576
5.24.3. iscsi enable 577
5.24.4. no iscsi enable 577
5.24.5. iscsi aging time 578
5.24.6. no iscsi aging time 578

5.24.7. iscsi queue 578
5.24.8. no iscsi queue 579
5.24.9. iscsi target 579
5.24.10. no iscsi target 580
5.25. Domain Name Server Client Commands 581
5.25.1. show hosts 581
5.25.2. ip host 582
5.25.3. no ip host 582
5.25.4. clear host 583
5.25.5. ip domain-name 583
5.25.6. no ip domain-name 583
5.25.7. ip domain-list 583
5.25.8. no ip domain-list 584
5.25.9. ip name-server 584
5.25.10. no ip name-server 584
5.25.11. ip name-server source-interface 585
5.25.12. no ip name-server source-interface 585
5.25.13. ip domain-lookup 585
5.25.14. no ip domain-lookup 586
5.25.15. ip domain-retry 586
5.25.16. no ip domain-retry 586
5.25.17. ip domain-retry-timeout 586
5.25.18. no ip domain-retry-timeout 587
5.25.19. ipv6 host 587
5.25.20. no ipv6 host 587
5.26. Unidirectional Link Detection Commands 588
5.26.1. udld enable (Global Config) 588
5.26.2. no udld enable (Global Config) 588
5.26.3. udld message time 588
5.26.4. no udld message time 588
5.26.5. udld timeout interval 589
5.26.6. no udld timeout interval 589
5.26.7. udld enable (Interface Config) 589
5.26.8. no udld enable (Interface Config) 589

5.26.9. udld port 590
5.26.10. udld reset 590
5.26.11. show udld 590
5.27. Multi-chassis Link Aggregation Commands 593
5.27.1. mlag 593
5.27.2. no mlag 593
5.27.3. mlag domain 593
5.27.4. no mlag domain 594
5.27.5. mlag system-mac 594
5.27.6. no mlag system-mac 594
5.27.7. mlag system-priority 594
5.27.8. no mlag system-priority 595
5.27.9. mlag role priority 595
5.27.10. no mlag role priority 595
5.27.11. mlag peer-link 595
5.27.12. no mlag peer-link 596
5.27.13. mlag id 596
5.27.14. no mlag id 596
5.27.15. mlag peer detection interval 596
5.27.16. no mlag peer detection interval 597
5.27.17. mlag peer-keepalive destination 597
5.27.18. no mlag peer-keepalive destination 597
5.27.19. mlag peer-keepalive enable 597
5.27.20. no mlag peer-keepalive enable 598
5.27.21. mlag peer-keepalive timeout 598
5.27.22. no mlag peer-keepalive timeout 598
5.27.23. show mlag brief 598
5.27.24. show mlag 601
5.27.25. show mlag role 601
5.27.26. show mlag consistency-parameters 603
5.27.27. show mlag peer-keepalive 604
5.27.28. show mlag statistics 604
5.27.29. show mlag core-config 606
5.27.30. clear mlag statistics 606

5.28. Control Plane Policing Commands 607
5.28.1. interface control-plane 607
5.28.2. show access-lists interface control-plane 608
5.29. VXLAN and RIOT Commands 609
5.29.1. vxlan mode 609
5.29.2. no vxlan mode 609
5.29.3. vxlan source-interface 609
5.29.4. no vxlan source-interface 610
5.29.5. vxlan udp-port 610
5.29.6. no vxlan udp-port 611
5.29.7. vxlan unicast-group 611
5.29.8. no vxlan unicast-group 611
5.29.9. default vxlan multicast-group 612
5.29.10. no vxlan default-multicast-group 612
5.29.11. vxlan vni multicast-group 612
5.29.12. no vxlan vni multicast-group 613
5.29.13. vxlan vlan vni 613
5.29.14. no vxlan vlan vni 613
5.29.15. interface vxlan 614
5.29.16. show vxlan 614
5.29.17. show vxlan vtep 615
5.29.18. show vxlan address-table 615
5.29.19. vxlan riot 616
5.29.20. no vxlan riot 616
5.29.21. vxlan riot-physical-loopback 616
5.29.22. no vxlan riot-physical-loopback 617
5.30. Interface Error Disable and Auto Recovery 618
5.30.1. errdisable recovery cause 618
5.30.2. no errdisable recovery cause 618
5.30.3. errdisable recovery interval 618
5.30.4. no errdisable recovery interval 619
5.30.5. show errdisable recovery 619
5.30.6. show interfaces status err-disabled 620
5.31. Role-Based Access Control 621

5.31.1. role based access control enable 622
5.31.2. no role based access control enable 622
5.31.3. role name 622
5.31.4. no role name 623
5.31.5. role description 623
5.31.6. no role description 623
5.31.7. rule command 624
5.31.8. no rule (to delete a rule of command string) 624
5.31.9. rule feature 625
5.31.10. no rule (to delete a rule of feature) 625
5.31.11. rule feature group 625
5.31.12. no rule (to delete a rule of feature group) 626
5.31.13. rule <rule-id> <deny | permit> <read | read-write> 626
5.31.14. no rule (to delete a rule of read-write commands) 626
5.31.15. rule renumber 626
5.31.16. role feature-group name 627
5.31.17. no role feature-group name 627
5.31.18. feature 627
5.31.19. no feature 628
5.31.20. username role 628
5.31.21. no username role 628
5.31.22. show role 628
5.31.23. show role feature 629
5.31.24. show role feature group 629
5.31.25. show role user 630
5.32. Application Commands 632
5.32.1. show application 632
5.32.2. show application files 632
5.32.3. application install 633
5.32.4. application start 634
5.32.5. application stop 634
5.33. Precision Time Protocol Transparant Clock Commands 635
5.33.1. ptp clock e2e-transparent 635
5.33.2. show ptp clock e2e-transparent 635

6. ROUTING COMMANDS 637
6.1. Address Resolution Protocol (ARP) Commands 637
6.1.1. Show commands 637
6.1.1.1. show ip arp 637
6.1.1.2. show ip arp brief 638
6.1.1.3. show ip arp static 639
6.1.2. Configuraton commands 639
6.1.2.1. arp 639
6.1.2.2. ip proxy-arp 640
6.1.2.3. ip local-proxy-arp 640
6.1.2.4. arp cashesize 640
6.1.2.5. arp dynamicrenew 641
6.1.2.6. arp resptime 641
6.1.2.7. arp retries 642
6.1.2.8. arp timeout 642
6.1.2.9. arp access-list 642
6.1.2.10. permit ip host mac host 643
6.1.2.11. clear ip arp-cache 643
6.2. IP Routing Commands 644
6.2.1. Show commands 644
6.2.1.1. show ip brief 644
6.2.1.2. show ip interface port 644
6.2.1.3. show ip interface vlan 646
6.2.1.4. show ip interface lookback 647
6.2.1.5. show ip interface brief 648
6.2.1.6. show ip route 649
6.2.1.7. show ip route bestroutes 650
6.2.1.8. show ip route entry 651
6.2.1.9. show ip route connected 652
6.2.1.10. show ip route ospf 652
6.2.1.11. show ip route static 653
6.2.1.12. show ip route ecmp-groups 654
6.2.1.13. show ip route hw-failure 654
6.2.1.14. show ip route summary 655

6.2.1.15. clear ip route counters 657
6.2.1.16. show ip route preferences 657
6.2.1.17. show ip stats 658
6.2.1.18. show routing heap summary 658
6.2.1.19. show ip load-sharing 659
6.2.1.20. show bfd neighbors 659
6.2.2. Configuration commands 660
6.2.2.1. routing 660
6.2.2.2. ip routing 661
6.2.2.3. ip address 661
6.2.2.4. ip address dhcp 662
6.2.2.5. ip default-gateway 662
6.2.2.6. ip load-sharing 663
6.2.2.7. ip route 663
6.2.2.8. ip route default 664
6.2.2.9. ip route distance 664
6.2.2.10. ip route static bfd 665
6.2.2.11. ip route vrf static bfd 666
6.2.2.12. ip mtu 666
6.2.2.13. ip unnumbered gratuitous-arp accept 667
6.2.2.14. ip unnumbered loopback 667
6.2.2.15. encapsulation 667
6.2.2.16. fpti 668
6.3. Open Shortest Path First (OSPF) Commands 669
6.3.1. Show commands 669
6.3.1.1. show ip ospf 669
6.3.1.2. show ip ospf abr 672
6.3.1.3. show ip ospf area 673
6.3.1.4. show ip ospf asbr 674
6.3.1.5. show ip ospf database 674
6.3.1.6. show ip ospf database database-summary 676
6.3.1.7. show ip ospf interface 677
6.3.1.8. show ip ospf interface brief 678
6.3.1.9. show ip ospf interface stats 679

6.3.1.10. show ip ospf neighbor 680
6.3.1.11. show ip ospf range 682
6.3.1.12. show ip ospf statistics 683
6.3.1.13. show ip ospf stub table 684
6.3.1.14. show ip ospf traffic 684
6.3.1.15. show ip ospf virtual-link 685
6.3.1.16. show ip ospf virtual-link brief 686
6.3.1.17. show ip ospf lsa-group 686
6.3.2. Configuration commands 687
6.3.2.1. router ospf 687
6.3.2.2. enable 687
6.3.2.3. network area 688
6.3.2.4. ip ospf area 688
6.3.2.5. 1583compatibility 688
6.3.2.6. area default-cost 689
6.3.2.7. area nssa 689
6.3.2.8. area nssa default-into-originate 689
6.3.2.9. area nssa no-redistribute 689
6.3.2.10. area nssa no-summary 690
6.3.2.11. area nssa translator-role 690
6.3.2.12. area nssa translator-stab-intv 690
6.3.2.13. area range 691
6.3.2.14. area stub 692
6.3.2.15. area stub no-summary 692
6.3.2.16. area virtual-link 692
6.3.2.17. area virtual-link authentication 692
6.3.2.18. area virtual-link dead-interval 693
6.3.2.19. area virtual-link hello-interval 693
6.3.2.20. area virtual-link retransmit-interval 694
6.3.2.21. area virtual-link transmit-delay 694
6.3.2.22. auto-cost reference-bandwidth 694
6.3.2.23. bfd 695
6.3.2.24. capability opaque 695
6.3.2.25. clear ip ospf 695

6.3.2.26. clear ip ospf configuration 696
6.3.2.27. clear ip ospf counters 696
6.3.2.28. clear ip ospf neighbor 696
6.3.2.29. clear ip ospf neighbor interface 697
6.3.2.30. clear ip ospf redistribution 697
6.3.2.31. clear ip ospf stub-router 698
6.3.2.32. default-information originate 698
6.3.2.33. default-metric 698
6.3.2.34. distance ospf 699
6.3.2.35. distribute-list out 699
6.3.2.36. exit-overflow-interval 699
6.3.2.37. external-lsdb-limit 700
6.3.2.38. ip ospf authentication 700
6.3.2.39. ip ospf cost 701
6.3.2.40. ip ospf dead-interval 701
6.3.2.41. ip ospf hello-interval 701
6.3.2.42. ip ospf network 701
6.3.2.43. ip ospf prefix-suppression 702
6.3.2.44. ip ospf priority 702
6.3.2.45. ip ospf retransmit-interval 703
6.3.2.46. ip ospf transmit-delay 703
6.3.2.47. ip ospf mtu-ignore 703
6.3.2.48. ip ospf bfd 704
6.3.2.49. router-id 704
6.3.2.50. redistribute 704
6.3.2.51. maximum-paths 704
6.3.2.52. passive-interface default 705
6.3.2.53. passive-interface 705
6.3.2.54. timers spf 705
6.3.2.55. max-metric 706
6.3.2.56. log-adjacency-changes 706
6.3.2.57. prefix-suppression 707
6.3.2.58. nsf helper 707
6.3.2.59. nsf helper strict-lsa-checking 707

6.3.2.60. bandwidth 708
6.4. BOOTP/DHCP Relay Commands 709
6.4.1. Show commands 709
6.4.1.1. show bootpdhcprelay 709
6.4.2. Configuration commands 709
6.4.2.1. bootpdhcprelay cidoptmode 709
6.4.2.2. bootpdhcprelay maxhopcount 710
6.4.2.3. bootpdhcprelay minwaittime 710
6.5. IP Helper Commands 711
6.5.1. Show commands 711
6.5.1.1. show ip helper-address 711
6.5.1.2. show ip helper statistics 711
6.5.2. Configuration commands 712
6.5.2.1. ip helper-address (Global Config) 712
6.5.2.2. ip helper-address (Interface Config) 713
6.5.2.3. ip helper-address discard 714
6.5.2.4. ip helper enable 715
6.5.2.5. clear ip helper statistics 715
6.6. Router Discovery Protocol Commands 716
6.6.1. Show commands 716
6.6.1.1. show ip irdp 716
6.7. VLAN Routing Commands 717
6.7.1. Configuration commands 717
6.7.1.1. interface vlan 717
6.8. Virtual Router Redundancy Protocol (VRRP) Commands 718
6.8.1. Show commands 718
6.8.1.1. show ip vrrp 718
6.8.1.2. show ip vrrp brief 718
6.8.1.3. show ip vrrp interface 719
6.8.1.4. show ip vrrp interface stats 720
6.8.1.5. clear ip vrrp interface stat 721
6.8.2. Configuration commands 721
6.8.2.1. ip vrrp 721
6.8.2.2. ip vrrp master-backup 722

6.8.2.3. ip vrrp <vrid> 722
6.8.2.4. ip vrrp ip 722
6.8.2.5. ip vrrp mode 723
6.8.2.6. ip vrrp accept-mode 723
6.8.2.7. ip vrrp authentication 724
6.8.2.8. ip vrrp preempt 724
6.8.2.9. ip vrrp priority 724
6.8.2.10. ip vrrp timers advertise 725
6.8.2.11. ip vrrp track interface 725
6.8.2.12. ip vrrp track ip route 726
6.9. Policy Based Routing (PBR) Commands 728
6.9.1. Show commands 728
6.9.1.1. show ip policy 728
6.9.1.2. show ip prefix-list 728
6.9.1.3. show ipv6 prefix-list 729
6.9.1.4. show route-map 729
6.9.2. Configuration commands 730
6.9.2.1. ip policy route-map 730
6.9.2.2. ip prefix-list 730
6.9.2.3. ip prefix-list description 731
6.9.2.4. ipv6 prefix-list 732
6.9.2.5. route-map 733
6.9.2.6. match as-path 734
6.9.2.7. match community 734
6.9.2.8. match ip address prefix-list 735
6.9.2.9. match ip address <acl-id | acl-name> 735
6.9.2.10. match ipv6 address 736
6.9.2.11. match length 736
6.9.2.12. match mac-list 737
6.9.2.13. set as-path 737
6.9.2.14. set comm-list delete 738
6.9.2.15. set community 738
6.9.2.16. set interface 739
6.9.2.17. set ip next-hop 740

6.9.2.18. set ip default next-hop 740
6.9.2.19. set ip precedence 741
6.9.2.20. set ipv6 next-hop 741
6.9.2.21. set local-preference 742
6.9.2.22. set metric 742
6.9.2.23. clear ip prefix-list 743
6.9.2.24. clear ipv6 prefix-list 743
6.10. Border Gateway Protocol (BGP) Commands 744
6.10.1. Show commands 744
6.10.1.1. show ip bgp 744
6.10.1.2. show ip bgp <prefix/length> 745
6.10.1.3. show ip bgp aggregate-address 746
6.10.1.4. show ip bgp community 747
6.10.1.5. show ip bgp community-list 748
6.10.1.6. show ip bpg filter-list 750
6.10.1.7. show ip bgp neighbors 751
6.10.1.8. show ip bgp prefix-list 754
6.10.1.9. show ip bgp route-reflection 755
6.10.1.10. show ip bgp summary 756
6.10.1.11. show ip bgp template 757
6.10.1.12. show ip bgp traffic 757
6.10.1.13. show ip bgp update-group 758
6.10.1.14. show bgp ipv6 760
6.10.1.15. show bgp ipv6 <ipv6-prefix/prefix-length> 761
6.10.1.16. show bgp ipv6 aggregate-address 763
6.10.1.17. show bgp ipv6 community 763
6.10.1.18. show bgp ipv6 community-list 765
6.10.1.19. show ip bgp vpnv4 766
6.10.1.20. show ip bgp listen range 767
6.10.1.21. show ip protocols bgp 768
6.10.1.22. show bgp ipv6 filter-list 769
6.10.1.23. show bgp ipv6 neighbors 770
6.10.1.24. show bgp ipv6 route-reflection 773
6.10.1.25. show bgp ipv6 statistics 774

6.10.1.26. show bgp ipv6 summary 774
6.10.1.27. show bgp ipv6 update-group 775
6.10.1.28. show ipv6 protocols bgp 777
6.10.1.29. show bgp ipv6 listen range 778
6.10.2. Configuration commands 779
6.10.2.1. router bgp 779
6.10.2.2. enable 779
6.10.2.3. aggregate-address 779
6.10.2.4. bgp aggregate-different-meds 780
6.10.2.5. bgp always-compare-med 781
6.10.2.6. bgp bestpath as-path ignore 781
6.10.2.7. bgp client-to-client reflection 782
6.10.2.8. bgp cluster-id 782
6.10.2.9. bgp default local-preference 782
6.10.2.10. bgp fast-external-failover 783
6.10.2.11. bgp fast-internal-failover 783
6.10.2.12. bgp log-neighbor-changes 783
6.10.2.13. bgp router-id 784
6.10.2.14. bgp maxas-limit 784
6.10.2.15. bgp graceful-restart 785
6.10.2.16. bgp graceful-restart-helper 785
6.10.2.17. bgp graceful-restart restart-time <restart-time> 785
6.10.2.18. bgp graceful-restart stalepath-time <stalepath-time> 786
6.10.2.19. bgp listen 786
6.10.2.20. exit 787
6.10.2.21. timers bgp 787
6.10.2.22. neighbor default-originate route-map 787
6.10.2.23. neighbor inherit peer 788
6.10.2.24. neighbor local-as 789
6.10.2.25. neighbor update-source 790
6.10.2.26. neighbor description 790
6.10.2.27. neighbor ebgp-multihop 791
6.10.2.28. neighbor password 792
6.10.2.29. neighbor connect-retry-interval 792

6.10.2.30. neighbor maximum-prefix 793
6.10.2.31. neighbor next-hop-self 794
6.10.2.32. neighbor filter-list 795
6.10.2.33. neighbor prefix-list 796
6.10.2.34. neighbor remote-as 796
6.10.2.35. neighbor remove-private-as 797
6.10.2.36. neighbor route-map 798
6.10.2.37. neighbor route-reflector-client 799
6.10.2.38. neighbor shutdown 799
6.10.2.39. neighbor timers 800
6.10.2.40. neighbor advertisement-interval 801
6.10.2.41. neighbor send-community 802
6.10.2.42. neighbor send-community extended 802
6.10.2.43. neighbor active 803
6.10.2.44. neighbor rfc5549-support 803
6.10.2.45. distance 804
6.10.2.46. distance bgp 805
6.10.2.47. default-information originate 805
6.10.2.48. maximum-paths 806
6.10.2.49. default-metric 806
6.10.2.50. redistribute 807
6.10.2.51. distribute-list in 808
6.10.2.52. distribute-list out 808
6.10.2.53. ip bgp fast-external-failover {deny|permit} 809
6.10.2.54. network 809
6.10.2.55. network <ipv6-prefix>/<prefix-length> 810
6.10.2.56. template peer 811
6.10.2.57. clear ip bgp 811
6.10.2.58. clear ip bgp counters 812
6.10.2.59. ip as-path access-list 812
6.10.2.60. ip bgp-community new-format 813
6.10.2.61. ip community-list 814
6.10.2.62. show ip as-path-access-list 814
6.10.2.63. show ip community-list 815

6.10.2.64. clear ip community-list 815
6.10.2.65. rd 816
6.10.2.66. route-target 816
6.10.2.67. address-family ipv4 817
6.10.2.68. address-family ipv6 818
6.10.2.69. address-family vpnv4 818
6.10.2.70. neighbor allowas-in 818
6.11. VRRPv3 Commands 820
6.11.1. Show commands 820
6.11.1.1. show vrrp 820
6.11.1.2. show vrrp brief 821
6.11.1.3. show vrrp statistics 822
6.11.2. Configuration commands 823
6.11.2.1. fhrp version vrrp v3 823
6.11.2.2. vrrp 823
6.11.2.3. preempt 824
6.11.2.4. accept-mode 824
6.11.2.5. priority 825
6.11.2.6. timers advertise 825
6.11.2.7. shutdown 825
6.11.2.8. address 826
6.11.2.9. track interface 826
6.11.2.10. track ip route 827
6.11.2.11. clear vrrp statistics 827
6.12. Virtual Router Commands 829
6.12.1. Show commands 829
6.12.1.1. show ip vrf 829
6.12.2. Configuration commands 829
6.12.2.1. ip vrf 829
6.12.2.2. maximum routes 830
6.12.2.3. description 830
6.12.2.4. ip vrf forwarding 830
6.13. Black Hole Detection (BHD) Commands 832
6.13.1. Show commands 832

6.13.1.1. show bhd status 832
6.13.2. Configuration commands 832
6.13.2.1. bhd spine-port enable 832
6.13.2.2. bhd enable 833
6.13.2.3. clear counter bhd 833
6.14. IP Event Dampening Commands 834
6.14.1.1. dampening 834
6.14.1.2. show dampening interface 834
7. IP MULTICAST COMMANDS 835
7.1. Internet Group Management Protocol (IGMP) Commands 835
7.1.1. Show commands 835
7.1.1.1. show ip igmp 835
7.1.1.2. show ip igmp groups 835
7.1.1.3. show ip igmp interface 837
7.1.1.4. show ip igmp interface membership 838
7.1.1.5. show ip igmp interface stats 839
7.1.2. Configuration commands 840
7.1.2.1. ip igmp 840
7.1.2.2. ip igmp router-alert-check 840
7.1.2.3. ip igmp version 841
7.1.2.4. ip igmp last-member-query-count 841
7.1.2.5. ip igmp last-member-query-interval 842
7.1.2.6. ip igmp query-interval 842
7.1.2.7. ip igmp query-max-response-time 842
7.1.2.8. ip igmp robustness 843
7.1.2.9. ip igmp startup-query-count 843
7.1.2.10. ip igmp startup-query-interval 844
7.2. MLD Commands 845
7.2.1. Show commands 845
7.2.1.1. show ipv6 mld groups 845
7.2.1.2. show ipv6 mld interface 846
7.2.1.3. show ipv6 mld traffic 848
7.2.2. Configuration commands 849
7.2.2.1. ipv6 mld query-interval 849

7.2.2.2. ipv6 mld query-max-response-time 849
7.2.2.3. ipv6 mld last-member-query-interval 850
7.2.2.4. ipv6 mld last-member-query-count 850
7.2.2.5. ipv6 mld router 850
7.2.2.6. clear ipv6 mld counters 851
7.2.2.7. clear ipv6 mld traffic 851
7.2.2.8. ipv6 mld version 851
7.2.2.9. ipv6 mld reset-status 852
7.2.2.10. ipv6 mld startup-query-count 852
7.2.2.11. ipv6 mld startup-query-interval 852
7.2.2.12. ipv6 mld unsolicit-rprt-interval 853
7.3. Multicast Commands 854
7.3.1. Show commands 854
7.3.1.1. show ip mcast 854
7.3.1.2. show ip mcast boundary 855
7.3.1.3. show ip mcast interface 855
7.3.1.4. show ip mcast mroute 856
7.3.1.5. show ip mcast mroute group 857
7.3.1.6. show ip mcast mroute source 858
7.3.1.7. show ip mcast mroute static 859
7.3.1.8. show ipv6 mroute 860
7.3.1.9. show ipv6 mroute group 862
7.3.1.10. show ipv6 mroute source 862
7.3.1.11. show ipv6 mroute static 863
7.3.1.12. clear ip mroute 864
7.3.1.13. clear ipv6 mroute 864
7.3.2. Configuration commands 864
7.3.2.1. ip multicast 864
7.3.2.2. ip mcast boundary 865
7.3.2.3. ip multicast ttl-threshold 865
7.4. IPv4 Protocol Independent Multicast (PIM) Commands 866
7.4.1. Show commands 866
7.4.1.1. show ip pim 866
7.4.1.2. show ip pim bsr-router 866

7.4.1.3. show ip pim interface 867
7.4.1.4. show ip pim neighbor 868
7.4.1.5. show ip pim rp mapping 869
7.4.1.6. show ip pim rp-hash 869
7.4.1.7. show ip pim ssm 870
7.4.1.8. show ip pim statistic 870
7.4.1.9. show ip mfc 871
7.4.1.10. clear ip pim statistics 872
7.4.2. Configuration commands 873
7.4.2.1. ip pim bsr-candidate 873
7.4.2.2. ip pim rp-address 873
7.4.2.3. ip pim rp-candidate 874
7.4.2.4. ip pim sparse 875
7.4.2.5. ip pim-spt-threshold 875
7.4.2.6. ip pim ssm 876
7.4.2.7. ip pim 876
7.4.2.8. ip pim bsr-border 876
7.4.2.9. ip pim dr-priority 877
7.4.2.10. ip pim hello-interval 877
7.4.2.11. ip pim join-prune-interval 878
7.5. IPv6 Protocol Independent Mulitcast (PIM) Commands 879
7.5.1. Show commands 879
7.5.1.1. show ipv6 pim 879
7.5.1.2. show ipv6 pim ssm 879
7.5.1.3. show ipv6 pim interface 880
7.5.1.4. show ipv6 pim neighbor 881
7.5.1.5. show ipv6 pim bsr-router 881
7.5.1.6. show ipv6 pim rp-hash 882
7.5.1.7. show ipv6 pim rp-mapping 883
7.5.1.8. show ipv6 pim statistic 883
7.5.1.9. clear ipv6 pim statistics 884
7.5.2. Configuration commands 885
7.5.2.1. ipv6 pim sparse 885
7.5.2.2. ipv6 pim 885

7.5.2.3. ipv6 pim hello-interval 885
7.5.2.4. ipv6 pim bsr-border 886
7.5.2.5. ipv6 pim bsr-candiate 886
7.5.2.6. ipv6 pim dr-priority 887
7.5.2.7. ipv6 pim join-prune-interval 887
7.5.2.8. ipv6 pim rp-address 887
7.5.2.9. ipv6 pim rp-candiate 888
7.5.2.10. ipv6 pim spt-threshold 889
7.5.2.11. ipv6 pim ssm 889
8. IPV6 COMMANDS 891
8.1. Tunnel Interface Commands 891
8.1.1. Show commands 891
8.1.1.1. show interface tunnel 891
8.1.2. Configuration commands 893
8.1.2.1. interface tunnel 893
8.1.2.2. tunnel source 893
8.1.2.3. tunnel destination 893
8.1.2.4. tunnel mode 894
8.2. Loopback Interface Commands 895
8.2.1. Show commands 895
8.2.1.1. show interface loopback 895
8.2.2. Configuration commands 896
8.2.2.1. interface loopback 896
8.3. IPv6 Routing Commands 897
8.3.1. Show commands 897
8.3.1.1. show ipv6 brief 897
8.3.1.2. show ipv6 interface 898
8.3.1.3. show ipv6 interface neighbors 900
8.3.1.4. show ipv6 protocols 901
8.3.1.5. show ipv6 route 903
8.3.1.6. show ipv6 route ecmp-groups 905
8.3.1.7. show ipv6 route hw-failure 905
8.3.1.8. show ipv6 route preferences 905
8.3.1.9. show ipv6 route summary 906

8.3.1.10. show ipv6 traffic 908
8.3.2. Configuration commands 913
8.3.2.1. ipv6 hop-limit 913
8.3.2.2. ipv6 unicast-routing 913
8.3.2.3. ipv6 enable 913
8.3.2.4. ipv6 address 914
8.3.2.5. ipv6 address autoconfig 915
8.3.2.6. ipv6 address dhcp 915
8.3.2.7. ipv6 route 916
8.3.2.8. ipv6 route distance 916
8.3.2.9. ipv6 mtu 917
8.3.2.10. ipv6 nd dad attemps 917
8.3.2.11. ipv6 nd managed-config-flag 917
8.3.2.12. ipv6 nd ns-interval 918
8.3.2.13. ipv6 nd other-config-flag 918
8.3.2.14. ipv6 nd ra-interval 918
8.3.2.15. ipv6 nd ra-lifetime 919
8.3.2.16. ipv6 nd reachable-time 919
8.3.2.17. ipv6 nd router-preference 920
8.3.2.18. ipv6 nd suppress-ra 920
8.3.2.19. ipv6 nd prefix 920
8.3.2.20. ipv6 neighbor 921
8.3.2.21. ipv6 neighbor dynamicrenew 921
8.3.2.22. ipv6 nud 922
8.3.2.23. ipv6 unreachables 922
8.3.2.24. ipv6 unresolved-traffic rate-limit 923
8.3.2.25. ipv6 icmp error-interval 923
8.3.2.26. clear ipv6 route counters 923
8.3.2.27. ipv6 nd mtu 924
8.4. OSPFv3 Commands 925
8.4.1. Show commands 925
8.4.1.1. show ipv6 ospf 925
8.4.1.2. show ipv6 ospf abr 927
8.4.1.3. show ipv6 ospf area 928

8.4.1.4. show ipv6 ospf asbr 929
8.4.1.5. show ipv6 ospf database 930
8.4.1.6. show ipv6 ospf database database-summary 931
8.4.1.7. show ipv6 ospf interface 932
8.4.1.8. show ipv6 ospf interface brief 934
8.4.1.9. show ipv6 ospf interface stats 935
8.4.1.10. show ipv6 ospf lsa-group 936
8.4.1.11. show ipv6 ospf max-metric 937
8.4.1.12. show ipv6 ospf neighbor 937
8.4.1.13. show ipv6 ospf range 939
8.4.1.14. show ipv6 ospf statistics 940
8.4.1.15. show ipv6 ospf stub table 941
8.4.1.16. show ipv6 ospf virtual-link 942
8.4.1.17. show ipv6 ospf virtual-link brief 943
8.4.2. Configuration commands 943
8.4.2.1. ipv6 ospf 943
8.4.2.2. ipv6 ospf area 943
8.4.2.3. ipv6 ospf bfd 944
8.4.2.4. ipv6 ospf cost 944
8.4.2.5. ipv6 ospf dead-interval 944
8.4.2.6. ipv6 ospf hello-interval 945
8.4.2.7. ipv6 ospf link-lsa-suppression 945
8.4.2.8. ipv6 ospf mtu-ignore 946
8.4.2.9. ipv6 ospf network 946
8.4.2.10. ipv6 ospf prefix-suppression 947
8.4.2.11. ipv6 ospf priority 947
8.4.2.12. ipv6 ospf retransmit-interval 947
8.4.2.13. ipv6 ospf transmit-delay 948
8.4.2.14. ipv6 router ospf 948
8.4.2.15. area default-cost 949
8.4.2.16. area nssa 949
8.4.2.17. area nssa default-info-originate 949
8.4.2.18. area nssa no-redistribute 950
8.4.2.19. area nssa no-summry 950

8.4.2.20. area nssa translator-role 951
8.4.2.21. area nssa translator-stab-intv 951
8.4.2.22. area range 952
8.4.2.23. area stub 952
8.4.2.24. area stub no-summary 953
8.4.2.25. area virtual-link 953
8.4.2.26. area virtual-link dead-interval 954
8.4.2.27. area virtual-link hello-interval 954
8.4.2.28. area virtual-link retransmit-interval 955
8.4.2.29. area virtual-link transmit-delay 955
8.4.2.30. auto-cost reference-bandwidth 956
8.4.2.31. bfd 956
8.4.2.32. default-information originate 957
8.4.2.33. default-metric 957
8.4.2.34. distance ospf 958
8.4.2.35. enable 958
8.4.2.36. exit-overflow-interval 958
8.4.2.37. external-isdb-limit 959
8.4.2.38. max-metric 959
8.4.2.39. maximum-paths 960
8.4.2.40. passive-interface default 960
8.4.2.41. passive-interface 961
8.4.2.42. prefix-suppression 961
8.4.2.43. redistribute 962
8.4.2.44. router-id 962
8.4.2.45. clear ipv6 ospf 962
8.4.2.46. clear ipv6 ospf configuration 963
8.4.2.47. clear ipv6 ospf counters 963
8.4.2.48. clear ipv6 ospf neighbor 963
8.4.2.49. clear ipv6 ospf neighbor interface 964
8.4.2.50. clear ipv6 ospf redistribution 964
8.4.2.51. clear ipv6 ospf stub-router 964
8.5. Routing Policy Commands 965
8.5.1. Show commands 965

8.5.1.1. show ipv6 prefix-list 965
8.5.2. Configuration commands 966
8.5.2.1. ipv6 prefix-list 966
8.5.2.2. match ipv6 address 967
8.5.2.3. set ipv6 next-hop 968
8.5.2.4. clear ipv6 prefix-list 968
8.6. DHCPv6 Snooping Commands 969
8.6.1. show ipv6 dhcp snooping 969
8.6.2. show ipv6 dhcp snooping per interface 970
8.6.3. show ipv6 dhcp snooping binding 970
8.6.4. show ipv6 dhcp snooping database 971
8.6.5. ipv6 dhcp snooping 972
8.6.6. ipv6 dhcp snooping vlan 972
8.6.7. ipv6 dhcp snooping verify mac-address 972
8.6.8. ipv6 dhcp snooping database 972
8.6.9. ipv6 dhcp snooping database write-delay 973
8.6.10. ipv6 dhcp snooping binding 973
8.6.11. ipv6 dhcp snooping limit 973
8.6.12. ipv6 dhcp snooping log-invalid 974
8.6.13. ipv6 dhcp snooping trust 974
8.6.14. clear ipv6 dhcp snooping binding 975
8.6.15. clear ipv6 dhcp snooping statistics 975
8.6.16. show ipv6 dhcp snooping statistics 975
8.6.17. show ipv6 dhcp binding 976
8.6.18. clear ipv6 dhcp binding 976
8.7. DHCPv6 Commands 977
8.7.1. show ipv6 dhcp interface 977
8.7.2. show ipv6 dhcp statistics 977
8.7.3. ipv6 dhcp relay destination 978
8.7.4. ipv6 dhcp relay interface 978
8.7.5. service dhcpv6 979
9. DATA CENTER BRIDGING COMMANDS 980
9.1. FIP Snooping 980
9.1.1. show fip-snooping 980

9.1.2. show fip-snooping enode 980
9.1.3. show fip-snooping sessions 981
9.1.4. show fip-snooping fcf 984
9.1.5. show fip-snooping vlan 985
9.1.6. show fip-snooping statistics 986
9.1.7. feature fip-snooping 987
9.1.8. fip-snooping enable 988
9.1.9. fip-snooping fc-map 988
9.1.10. fip-snooping port-mode fcf 989
9.1.11. clear fip-snooping statistics 989
9.2. Priority-based Flow Control 991
9.2.1. show interface priority-flow-control 991
9.2.2. priority-flow-control mode 992
9.2.3. priority-flow-control priority 993
9.2.4. clear priority-flow-control statistics 993
9.3. OpenFlow 994
9.3.1. show openflow 994
9.3.2. show openflow configured controller 994
9.3.3. show openflow installed flows 995
9.3.4. show openflow installed groups 996
9.3.5. show openflow table-status 997
9.3.6. openflow enable 998
9.3.7. openflow static-ip 998
9.3.8. openflow controller 999
9.3.9. openflow ip-mode 999
9.3.10. openflow passive-mode 999
9.3.11. openflow failmode 1000
9.3.12. clear openflow ca-cert 1000
10. FLUENTD COMMANDS 1001
10.1. Show Commands 1001
10.1.1. show fluentd 1001
10.2. Configuration Commands 1003
10.2.1. fluentd 1003
10.2.2. fluentd <fluentd-entry> 1003

10.2.3. enable 1003
10.2.4. sourcetag 1004
10.2.5. syslog 1004
10.2.6. localsyslog 1004
10.2.7. dstat 1005
10.2.8. exec 1005
10.2.9. matchpattern 1006
10.2.10. forward 1006
10.2.11. webhdfs 1007
10.2.12. elasticsearch 1008
11. SDVOE COMMANDS 1010
11.1. Show Commands for an SDVoE Environment 1010
11.1.1. show igmpsnooping group 1010
11.1.2. show igmpsnooping fast-leave 1011
11.2. Configuration Commands for an SDVoE Environment 1012
11.2.1. igmp-plus <vlan-id> 1012
11.2.2. set igmp flood-report <vlan-id> 1012
11.2.3. set igmp exclude-mrouter-intf <vlan-id> 1012
11.2.4. set igmp fast-leave auto-assignment 1013
12. SERVICEABILITY PACKET TRACING COMMANDS 1014
12.1. CPU Traffic Commands 1014
12.1.1. show cpu-traffic 1014
12.1.2. show cpu-traffic interface 1014
12.1.3. show cpu-traffic summary 1014
12.1.4. show cpu-traffic trace 1014
12.1.5. cpu-traffic direction interface 1015
12.1.6. cpu-traffic direction match cust-filter 1015
12.1.7. cpu-traffic direction match srcip 1015
12.1.8. cpu-traffic direction match dstip 1016
12.1.9. cpu-traffic direction match tcp 1016
12.1.10. cpu-traffic direction match udp 1016
12.1.11. cpu-traffic direction match mac 1017
12.1.12. cpu-traffic direction match filter 1017
12.1.13. cpu-traffic mode 1017

12.1.14. cpu-traffic trace 1018
12.1.15. clear cpu-traffic 1018
12.2. Exception Kernel Dump Commands 1019
12.2.1. show exception kernel-dump 1019
12.2.2. show exception kernel-dump list 1019
12.2.3. show exception kernel-dump log 1019
12.2.4. exception kernel-dump 1019
12.2.5. exception kernel-dump path 1020
12.3. Memory Buffer Commands 1021
12.3.1. show mbuf 1021
12.3.2. show mbuf total 1021
12.3.3. mbuf 1022
13. TROUBLESHOOTING 1023
13.1. M4500 series Linux system and password recovery for SSH port 22 1023

1. Introduction

1.1. Product Overview

The switch provides high performance, high availability, and simplicity of management. The switch is designed for adaptability and scalability for campus use and data center use.

1.1.1. Simplicity

The switch can be managed through industry standard command-line interface (CLI) which reduces the training and operating costs. It also supports Simple Network Management Protocol (SNMP) both rom standard MIB and private MIB for network administrator to easily configure, monitor, and manage remotely. The Auto-installation feature implemented helps centralized management to simplify deployment of a truly plug-and-play experience. With the evolution from IPv4 to IPv6, the switch is an IPv6 integrated management device.

1.1.2. High Availability

The switch is designed for high availability from both hardware and software perspective. The key features include:

- 1+1 hot-swappable power supplies

- Out-of-band management supported

- 802.1D, 802.1w and 802.1s supported

- Up to 8 ports per link aggregation group (LACP) and up to 64 groups

- Multi-chassis LAG for preventing the risks of single point failure

- Up to 32 paths ECMP routing for load balancing and redundancy

- Virtual Router Redundancy Protocol (VRRP) supported

1.1.3. High-Performance L2/L3 Access Deployments

With the compact 1U form factor, high density ports in the front panel, front to back or back to front airflow design, the switch is ideal for top-of-rack deployments in high-performance, highly demanding data centers. The high switching capacity to be a powerful solution to aggregate high-performance servers in the data center.

1.1.4. Advance IPv4 and IPv6 Routing

The switch is a full layer 2 and layer 3 routing switch that supports advanced IPv4 and IPv6 routing features such as OSPFv2, BGP4, and OSPFv3. The multicast routing features for IGMP v1/v2/v3, PIM-SM, MLD v1/v2 and PIM-SM6 are all supported.

1.1.5. Data Center Application

The switch is an IEEE DCB-based switch delivering a high-performance solution to integrate server edge access. The key features include:

- Enhanced Transmission Selection (ETS, 802.1Qaz)

- Priority-based Flow Control (PFC, 802.1Qbb)

- Data Center Bridging Extension (DCBX, 802.1Qaz)

- FCoE Initiation Protocol (FIP) snooping

1.2. Features

- IEEE 802.3z and IEEE 802.3x compliant Flow Control for all Ethernet ports
- Supports 802.1S MSTP, and 802.1w Rapid Spanning Tree for redundant back up bridge paths
- Supports 802.1Q VLAN, Double VLAN, IGMP snooping, 802.1p Priority Queues, Port Channel, port mirroring
- Link Aggregation (802.1ad LACP)
- Multi-chassis Link Aggregation (MLAG)
- Supports LLDP with potential communication problems detection
- Supports Port Security
- Multi-layer Access Control (based on MAC address, IP address, VLAN, Protocol, 802.1p, DSCP)
- Quality of Service (QoS) customized control
- 802.1x access control and RADIUS client support
- TACACS+ support
- UDLD support
- Administrator-definable port security
- Supports DHCP Snooping, Dynamic ARP Inspection and IP Source Guard (IPSG)
- ARP support

- IP Routing support
- OSPF v2 and v3 support
- BGP4 Support
- Router Discovery Protocol support
- Virtual Router Redundancy Protocol (VRRP) v2 support
- VLAN Routing support
- 32-way ECMP support
- 31 subnets support
- Source IP configuration support
- Policy Based Routing (PBR)
- IP Multicast support
- IGMP v1, v2, and v3 support
- Protocol Independent Multicast - Sparse Mode (PIM-SM) support for IPv4 and IPv6
- IPv6 function
  - Supports DHCPv6 protocol, OSPFv3 protocol, Tunneling, loopback
  - Provides to configure IPv6 routing interface, routing preference
- DHCP Client and Relay support
- IP Helper (BOOTP/DHCP Relay)
- DNS Client and Relay support
- DDNS client support
- Per-port bandwidth control
- SNMP v1, v2, v3 network management, RMON support
- CLI management support
- Fully configurable either in-band or out-of-band control via RS-232 console serial connection
- Telnet remote control console
- TraceRoute support
- Traffic Segmentation
- TFTP/FTP upgrade
- SysLog support
- Email Alerting support

- CLI Scheduler support
- Simple Network Time Protocol support
- SSH Secure Shell v2.0 support; not support SSH v1.5.
- SSL Secure HTTP TLS Version 1 and SSL version 3 support
- Auto Install Support
- Fiber Channel Over Ethernet(FCoE)
  - FIP Snooping
- Data Center Bridge (DCB)
  - Enhanced Transmission Selection (ETS, IEEE 802.1Qaz)
  - Priority Flow Control (PFC, IEEE 802.1Qbb)
  - Application Priority (IEEE 802.1Qaz)
- Data Center Bridge Exchange (DCBX, IEEE802.1Qaz)
  - CEE 1.01 support
  - IEEE version support

1.3. Management Options

The system may be managed by using one Service Ports through a Telnet, SNMP function, and using the console port on the front panel through CLI command.

1.4. Command Line Console Interface Through The Serial Port or Telnet

You can also connect a computer or terminal to the serial console port or use Telnet to access the Switch. The command-line-driven interface provides complete access to all switch management features.

1.5. SNMP-Based Management

You can manage the Switch with an SNMP-compatible console program. The Switch supports SNMP version 1.0, version 2.0, and version 3.0. The SNMP agent decodes the incoming SNMP messages and responds to requests with MIB objects stored in the database. The SNMP agent updates the MIB objects to generate statistics The Switch supports a comprehensive set of MIB extensions:

- RFC 2819 RMON-MIB
- RFC 2233 Interface MIB
- RFC 2618 (Radius-Auth-Client-MIB)
- RFC 2620 (Radius-Acc-Client-MIB)
- RFC 1850 (OSPF-MIB)
- RFC 1850 (OSPF-TRAP-MIB)
- RFC 2787 (VRRP-MIB)
- RFC 3289 - DIFFSERV-DSCP-TC
- RFC 3289 - DIFFSERV-MIB
- QOS-DIFFSERV-EXTENSIONS-MIB
- QOS-DIFFSERV-PRIVATE-MIB
- RFC 2674 802.1p
- RFC 2932 (IPMROUTE-MIB)
- Private Enterprise MIB
- ROUTING-MIB
- MGMD-MIB
- RFC 2934 PIM-MIB
- IANA-RTPROTO-MIB
- MULTICAST-MIB
- ROUTING6-MIB
- IEEE8021-PAE-MIB
- INVENTORY-MIB
- MGMT-SECURITY-MIB
- QOS-MIB
- QOS-ACL-MIB
- QOS-COS-MIB

- QOS-AUTOVOIP-MIB
- QOS-DIFFSERV-PRIVATE-MIB
- QOS-ISCSI-MIB
- RFC 1907 - SNMPv2-MIB
- RFC 2465 - IPV6-MIB
- RFC 2466 - IPV6-ICMP-MIB
- TACACS-MIB
- IGMP/MLD Snooping
- IGMP/MLD Layer2 Multicast
- QoS – IPv6 ACL
- Guest VLAN
- LLDP-MIB
- LLDP MED
- RFC 2925 (DISMAN-TRACEROUTE-MIB)
- OSPFV3-MIB
- RFC 2571 - SNMP-FRAMEWORK-MIB
- RFC 2572 - SNMP-MPD-MIB
- RFC 2573 - SNMP-NOTIFICATION-MIB
- RFC 2573 - SNMP-TARGET-MIB
- RFC 2574 - SNMP-USER-BASED-SM-MIB
- RFC 2576 - SNMP-COMMUNITY-MIB
- RFC 2263 - USM-TARGET-TAG-MIB
- RFC 3176 - SFLOW-MIB
- IEEE8023-LAG-MIB (IEEE Std 802.3ad)
- RFC 2674 - P-BRIDGE-MIB
- RFC 2674 - Q-BRIDGE-MIB
- RFC 2737 - ENTITY-MIB
- RFC 2863 - IF-MIB
- RFC 3635 - Etherlike-MIB
- PORTSECURITY-PRIVATE-MIB

- RADIUS-CLIENT-PRIVATE-MIB
- RFC 5060 - PIM-STD-MIB
- RFC 5240 - PIM-BSR-MIB
- RFC 3419 - TRANSPORT-ADDRESS-MIB
- IANA-MAU-MIB

2. Quick Startup

2.1. Quick-Start the Switch

1. Read the device Installation Guide for the connectivity procedure. In-band connectivity allows access to the Switch locally. From a remote workstation, the device must be configured with IP information (IP address, subnet mask, and default gateway).

2. Turn the Power ON.

3. Allow the device to load the software until the login prompt appears. The device initial state is called the default mode.

4. Log in to the Linux system first with the following login and password information in the default mode:

   Login: **admin**
   Password: **EndGame**

   After you log in, follow the system prompts you to select a menu option:

```
  _   _   _____   _____    ____   _____      _      ____
 | \ | | | ____| |_   _|  / ___| | ____|    / \    |  _ \
 |  \| | |  _|     | |   | |  _  |  _|     / _ \   | |_) |
 | |\  | | |___    | |   | |_| | | |___   / ___ \  |  _ <
 |_| \_| |_____|   |_|    \____| |_____| /_/   \_\ |_| \_

=======================
NETGEAR M4500 Menu
=======================
1: CLI Console
2: Firmware update with verification using SCP
3: Firmware update with verification using TFTP
4: Reboot
=======================
Enter your menu option:
```

5. Change the password for the admin user.

   On first login, the switch forces you to change the default password for the admin user. The new password must be eight or more characters and must consist of letters, numbers,and special characters.

6. Log back in to the switch, using the new password.

2.2. Methods to Access the Switch CLI

You can access the switch CLI by any of the following methods:

- Console
- SSH using standard port 22
- SSH using special port 1234
- Telnet using special port 1223

2.2.1. Switch CLI Access Using a Console

When a user logs in to the switch using serial console connection, the system automatically logs in to the switch Linux shell and prompts the user to log in to switch CLI, as shown in the following example:

```
Ubuntu 16.04 LTS M4500-48XF8C ttyS0
M4500-48XF8C login: admin (automatic login)
Last login: Tue Sep 17 05:38:06 UTC 2019 from 10.1.109.26
on pts/1
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.14.4 x86_64)
* Documentation: https://help.ubuntu.com/
Initializing console session. Press ^z to exit
Connecting to /dev/pts/0
DMA pool size: 33554432
PCI unit 0: Dev 0xb873, Rev 0x01, Chip BCM56873_A0, Driver
BCM56870_A0
SOC unit 0 attached to PCI device BCM56873_A0
UNIT0 CANCUN:
CIH: LOADED
Ver: 05.00.07
CMH: LOADED
Ver: 05.00.07
CCH: LOADED
Ver: 05.00.07
CEH: LOADED
Ver: 05.00.07
*** unit 0: ports capable of limited speed range cut-thru
*** unit 0: alpm level 2 loaded: 8 banks in combined-128
started!
Sep 17 05:42:26: %1-1-SIM: [0xe92bd554] sim_util.c(4227) 7
%% Switch was reset due to power disruption or unexpected
restart.
(Unit 1)>
Applying Global configuration, please wait ...
Applying Interface configuration, please wait ...
User:
Sep 17 05:42:36: %1-2-General: [0xf7800754] Boot!(0) 207 %%
Event(0xaaaaaaaa)
User:admin
Password:
```

If user authentication is successful, the system prompts the user to change the password, if the default password was used to log in to the switch CLI, as shown in the following example:

```
Default password authentication successful.
Change default password for NETWORK ‘admin’ user.
Password requires 8 or more characters.
New password:*********
Re-enter new password: *********
Password change is successful.
!!! For guest user access, change its default password
Login again using new password
User:admin
Password:*********
(M4500-48XF8C) #
```

2.2.2. Switch CLI Access Using SSH Standard Port 22

A user can log in to the switch by using an SSH connection over standard port 22 with the default user name **admin** and default password **EndGame**, as shown in the following example:

```
switch$ ssh admin@10.1.18.206
admin@10.1.18.206's password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.14.4 x86_64)
* Documentation: https://help.ubuntu.com/
Last login: Tue Sep 24 05:32:19 2019 from 10.1.51.30
Initializing console session. Press ^z to exit
Connecting to /dev/pts/0
User:
```

If the login is sucessful, the switch prompts the user to change the default Linux password, as shown in the following example:

```
switch$ ssh admin@10.1.18.206
admin@10.1.18.206's password:
Default password authentication successful.
Change default password for SYSTEM 'admin' user.
Password requires 8 or more characters.
New password:*********
Re-enter new password: *********
Password change is successful.
Login again using new password
```

After the new password is configured, the current session is terminated and the user is forced to log in again. When the user logs in again using SSH with the new password, the switch CLI is available.

For information about recovering access, see M4500 series Linux system and password recovery for SSH port 22.

2.2.3. Switch CLI Access Using SSH Special Port 1234

A user can log in to the switch by using an SSH connection over special port 1234 using default user name **admin** and default password (which is blank), as shown in the following example:

```
switch$ ssh admin@10.1.18.206 -p 1234
admin@10.1.18.206's password:
(M4500-48XF8C) #
```

If the login is sucessful, the switch prompts the user to change the default Linux password, as shown in the following example. After the new password is configured, the current session is terminated and the user is forced to log in again. When the user logs in again using SSH with the new password, the switch CLI is available.

```
Default password authentication successful.
Change default password for NETWORK user 'admin'
Password requires 8 or more characters.
New password:*********
Re-enter new password: *********
Password change is successful.
!!! For guest user access, change its default password
Login again using new password
User:admin
Password:*********
(M4500-48XF8C) #
```

2.2.4. Switch CLI Access Using Telnet Special Port 1223

Access to the switch CLI using Telnet special port 1223 follows the same process as access to the switch CLI using SSH special port 1234.

2.2.5. Limitations for a Guest User Login

- A guest user cannot change the password. Only an admin user can change the password for a guest password.
- A guest cannot log in using default password. Guest user access is denied until an admin user sets up the password for the guest user. If a guest attempts to log in using the default password, the following message is shown, after which the login prompt is displayed.

```
Login using default password is not allowed.
Please ask network admin to set new guest user password.
```

2.2.6. Limitations for SNMP Login

- For SNMPv1 and SNMPv2, by default, no community strings such as private or public are configured.
- The SNMPv3 authentication protocol is MD5. SNMPv3 users and devicces cannot access the switch if the authentication protocol is None.

2.3.System Information Setup

2.3.1. Quick Startup Software Version Information

Table 2-1. Quick Start up Software Version Information

Command	Details
show hardware	Allows the user to see the HW & SW version the device contains System Description - switch's model name
show version	Allows the user to see Serial Number, Part Number, and Model name See SW loader, bootrom and operation version See HW version

2.3.2. Quick Startup Physical Port Data

Table 2-2. Quick Start up Physical Port

Command	Details
show interfaces status [<slot/port>]	Displays the Ports slot/port Type - Indicates if the port is a special type of port Admin Mode - Selects the Port Control Administration State

	Physical Mode - Selects the desired port speed and duplex mode Physical Status - Indicates the port speed and duplex mode Link Status - Indicates whether the link is up or down Link Trap - Determines whether or not to send a trap when link status changes LACP Mode - Displays whether LACP is enabled or disabled on this port Flow Mode - Indicates the status of flow control on this port Cap. Status - Indicates the port capabilities during auto-negotiation

2.3.3. Quick Startup User Account Management

Table 2-3. Quick Start up User Account Management

Command	Details
show users	Displays all users that are allowed to access the switch User Access Mode - Shows whether the user is able to change parameters on the switch (Read/Write) or is only able to view (Read Only). As a factory default, admin has Read/Write access and guest has Read Only access. There can only be one Read/Write user and up to 5 Read Only users.
show loginsession	Displays all login session information
username <username> {passwd}	Allows the user to set passwords or change passwords needed to login A prompt will appear after the command is entered requesting the old password. In the absence of an old password leave the area blank. The operator must press enter to execute the command. The system then prompts the user for a new password then a prompt to confirm the new password. If the new password and the confirmed password match a message will be displayed.
copy running-config startup-config	This will save passwords and all other changes to the device. If you do not save config, all configurations will be lost when a power cycle is performed on the switch or when the switch is reset.

2.3.4. Quick Startup IP Address

To view the network parameters the operator can access the device by the following three methods.

- Simple Network Management Protocol - SNMP
- Telnet via port **1223** for X86 system and via port **23** for other systems
- SSH via port **1234** for X86 system and via port **22** for other systems

Table 2-4. Quick Start up IP Address

Command	Details
show ip interface	Displays the Network Configurations Interface Status – Indicates whether the interface is up or down. IP Address - IP Address of the interface Subnet Mask - IP Subnet Mask for the interface. MAC Address - The MAC Address used for this in-band connectivity Network Configurations Protocol Current - Indicates which network protocol is being used. Default is None.
ip address	(Config)#*interface vlan 1* (if-vlan 1)#*ip address <ipaddr> <subnet-mask>* (if-vlan 1)#*exit* (Config)#*ip default-gateway <gateway-addr>* IP Address range from 0.0.0.0 to 255.255.255.255 Subnet Mask range from 0.0.0.0 to 255.255.255.255 Gateway Address range from 0.0.0.0 to 255.255.255.255 Displays all of the login session information
show serviceport	Display the serviceport's network configurations Interface Status – Indicates whether the interface is up or down. IP Address - IP Address of the interface. Default IP is 0.0.0.0 Subnet Mask - IP Subnet Mask for the interface. Default is 0.0.0.0 Default Gateway - The default Gateway for this interface. Default value is 0.0.0.0 Burned in MAC Address - The Burned in MAC Address used for out-of-band connectivity Configured IPv4 Protocol - Indicates which network protocol is being used. Default is DHCP.
serviceport ip	(Config)#*serviceport protocol none* (Config)#serviceport *ip <ipaddr> <netmask> <gateway>* (Config)#

2.3.5. Quick Startup Downloading from TFTP Server

Before starting a TFTP server download, the operator must complete the Quick Start up for the IPAddress.

Table 2-5. Quick Start up Downloading from TFTP Server

Command	Details
copy <url> startup-config <destfilename>	Sets the download datatype to be an image or config file. The URL must be specified as: tftp://ipAddr/filepath/fileName. The startup-config option downloads the config file using tftp and image option downloads the code file.

2.3.6. Quick Startup Factory Defaults

Table 2-6. Quick Start up Factory Defaults

Command	Details
clear config	Enter yes when the prompt pops up to clear all the configurations made to the switch. You can also decide if the IP settings of service port be kept or not in this command.
copy running-config startup-config	Enter yes when the prompt pops up that asks if you want to save the configurations made to the switch.
reload [warm]	Enter yes when the prompt pops up that asks if you want to reset the system. You can reset the switch or cold boot the switch; both work effectively. warm – indicates only switch application is restarted.

3. Console and Telnet Administration Interface

This chapter discusses many of the features used to manage the Switch, and explains many concepts and important points regarding these features. Configuring the Switch to implement these concepts is discussed in detail in chapter 5.

The command-line interface (CLI) provides a text-based way to manage and monitor the switch features. You can access the CLI by using a direct connection to the console port or by using a Telnet or SSH client. To access the switch by using Telnet or Secure Shell (SSH), the switch must have an IP address configured on either the service port or the network interface, and the management station you use to access the device must be able to ping the switch IP address. DHCP is enabled by default on the service port. It is disabled on the network interface.

3.1. Local Console Management

Local console management involves the administration of the Switch via a direct connection to the RS-232 DCE console port. This is an Out-of-band connection, meaning that it is on a different circuit than normal network communications, and thus works even when the network is down.

The local console management connection involves a terminal or PC running terminal emulation software to operate the Switch's built-in console program (see Chapter 5). Using the console program, a network administrator can manage, control, and monitor many functions of the Switch. Hardware components in the Switch allow it to be an active part of a manageable network. These components include a CPU, memory for data storage, other related hardware, and SNMP agent firmware. Activities on the Switch can be monitored with these components, while the Switch can be manipulated to carry out specific tasks.

3.2. Setup Your Switch Using Console Access

Out-of-band management requires connecting a terminal, such as a VT-100 or a PC running a terminal-emulation program (such as HyperTerminal, which is automatically installed with Microsoft Windows) to the RS-232 DCE console port of the Switch. Switch management using the RS-232 DCE console port is called *Local Console Management* to differentiate it from management done via management platforms, such as DView or HP OpenView.

Make sure the terminal or PC you are using to make this connection is configured to match these settings. If you are having problems making this connection on a PC, make sure the emulation is set to VT-100 or ANSI. If you still don't see anything, try pressing <Ctrl> + r to refresh the screen.

First-time configuration must be carried out through a console, that is, either (a) a VT100-type serial data terminal, or (b) a computer running communications software set to emulate a VT100. The console must be connected to the Diagnostics port. This is an RS-232 port with a 9-socket D-shell connector and DCE-type wiring. Make the connection as follows:

1. Obtain suitable cabling for the connection. You can use a null-modem RS-232 cable or an ordinary RS-232 cable and a null-modem adapter. One end of the cable (or cable/adapter combination) must have a 9-pin D-shell connector suitable for the Diagnostics port; the other end must have a connector suitable for the console's serial communications port.

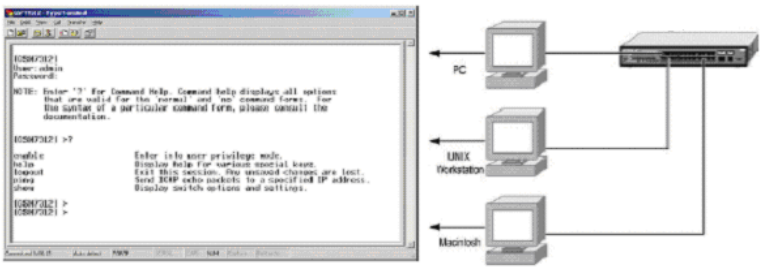
2. Power down the devices, attach the cable (or cable/adapter combination) to the correct ports, and restore power.

3. Set the console to use the following communication parameters for your terminal:

   - The console port is set for the following configuration:
   - Baud rate: 115,200
   - Data width: 8 bits
   - Parity: none
   - Stop bits: 1
   - Flow Control: none

A typical console connection is illustrated below:

Figure 3-1: Console Setting Environment



3.3. Setup Your Switch Using Telnet Access

Once you have set an IP address for your Switch, you can use a Telnet program (in a VT-100 compatible terminal mode) to access and control the Switch. The port number for Telnet is 1223 for X86 systems and 23 for other systems. Most of the screens are identical, whether accessed from the console port or from a Telnet interface.

3.3.1. Accessing the Switch CLI through the Network

Remote management of the switch is available through the service port or through the network interface. To use telnet, SSH , or SNMP for switch management, the switch must be connected to the network, and you must know the IP or IPv6 address of the management interface. The switch has no IP address by default. The DHCP client on the service port is enabled, and the DHCP client on the network interface is disabled. The port number used to access the switch CLI is as follows:

- Telnet via port **1223**.

  Example:

```
my-ubuntu:~$ telnet 10.1.18.206 1223

Trying 10.1.18.206...

Connected to 10.1.18.206.

Escape character is '^]'.
```

```
User:admin

Password:***********

(M4500-48XF8C) #
```

- SSH via port standard port **22**.

  Example:

```
my-ubuntu:~$ ssh admin@10.1.18.206

admin@10.1.18.206's password:

Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.14.4 x86_64)

 * Documentation:  https://help.ubuntu.com/

Last login: Sun Sep  8 07:16:34 2019 from 10.1.50.127

Initializing console session. Press ^z to exit

Connecting to /dev/pts/0

User:admin

Password:***********

(M4500-48XF8C) #
```

3.3.2. Using the Service Port or Network Interface for Remote Management

The service port is a dedicated Ethernet port for out-of-band management. We recommend that you use the service port to manage the switch. Traffic on this port is segregated from operational network traffic on the switch ports and cannot be switched or routed to the operational network. Additionally, if the production network is experiencing problems, the service port still allows you to access the switch management interface and troubleshoot issues. Configuration options on the service port are limited, which makes it difficult to accidentally cut off management access to the switch.

Alternatively, you can choose to manage the switch through the production network, which is known as in-band management, because in-band management traffic is mixed in with production network traffic, it is subject to all of the filtering rules usually applied on a switched/routed port such as ACLs and VLAN tagging. You can access the in-band network management interface through a connection to any front-panel port.

3.3.2.1. Configuring Service Port Information

To disable DHCP/BootP and manually assign an IPv4 address, enter commands under Global Configuration mode:

serviceport protocol none

serviceport ip ipaddress netmask

For example, serviceport ip 192.168.2.22 255.255.255.0

To disable DHCP/BootP and manually assign an IPv6 address, enter commands under Global Configuration mode:

serviceport protocol none dhcp6

serviceport ipv6 enable

serviceport ipv6 address *prefix /prefix-length*

serviceport ipv6 gateway *ipv6-address*

To view the assigned or configured network address, use:

show serviceport

To enable the DHCP/DHCPv6 client on the service port, use:

serviceport protocol dhcp

serviceport protocol dhcp6

To enable the BootP client on service port, use:

serviceport protocol bootp

3.3.2.2. Configuring the In-Band Network Interface

To use a DHCP server to obtain the IP address, subnet mask, and default gateway information, use:

interface vlan 1

ip address dhcp

ipv6 address dhcp

To manually configure the IPv4 address, subnet mask, use:

interface vlan 1

ip address ipaddr subnet-mask

To manually configure the IPv6 address, subnet mask, use:

interface vlan 1

ipv6 address prefix /prefix-length

3.3.2.3. Firmware Image Update

Starting with release 7.0.1.x, the M4500 series switches support signed firmware images only. Therefore, updating firmware directly from an unsigned 7.0.0.x image to a signed 7.0.1.x image is not supported. To update firmware from a 7.0.0.x image to a 7.0.1.x image, you first must update to a transition image before you can update to a signed 7.0.1.x image.

For example, from the unsigned 7.0.0.x image, update to the 7.0.1.6 transition image. Then, from the 7.0.1.6 transition image, update to signed 7.0.1.x image.

Similarly, to revert from a signed 7.0.1.x image to an unsigned 7.0.0.x image, first revert from the unsigned 7.0.1.x image to the 7.0.1.6 transition image, and then revert from the 7.0.1.6 transition image to the unsigned 7.0.0.x image.

The current transition firmware image version is 7.0.1.6. The transition firmware image lets you update to a signed firmware image or revert to an unsigned firmware image as shown below. The text “with verification” refers to a signed firmware image and the text “without verification” refers to an unsigned firmware image.

```
  _   _   _____   _____    ____   _____      _      ____
 | \ | | | ____| |_   _|  / ___| | ____|    / \    |  _ \
 |  \| | |  _|     | |   | |  _  |  _|     / _ \   | |_) |
 | |\  | | |___    | |   | |_| | | |___   / ___ \  |  _ <
 |_| \_| |_____|   |_|    \____| |_____| /_/   \_\ |_| \_

=======================
NETGEAR M4500 Menu
=======================
1: CLI Console
2: Firmware update without verification using SCP
3: Firmware update without verification using TFTP
4: Firmware update with verification using SCP
5: Firmware update with verification using TFTP
6: Reboot
=======================
Enter your menu option:
```

To update from one signed firmware version to another signed firmware version, you do not need to use a transition image.

4. Command Line Interface Structure and Mode-based CLI

The Command Line Interface (CLI) syntax, conventions, and terminology are described in this section. Each CLI command is illustrated using the structure outlined below.

4.1. CLI Command Format

Commands are followed by values, parameters, or both.

Example 1

ip address <ipaddr> <netmask> [<gateway>]

- **ip address** is the command name.
- **<ipaddr> <netmask>** are the required values for the command.
- **[<gateway>]** is the optional value for the command.

Example 2

snmp-server location <loc>

- **snmp-server location** is the command name.
- **<loc>** is the required parameter for the command.

Example 3

clear vlan

- **clear vlan** is the command name.

Command

The text in bold, non-italic font must be typed exactly as shown.

4.2. CLI Mode-based Topology

4.2.1. Parameters

Parameters are order dependent.

The text in bold italics should be replaced with a name or number. To use spaces as part of a name parameter, enclose it in double quotes like this: "System Name with Spaces".

Parameters may be mandatory values, optional values, choices, or a combination.

- **<parameter>.**

  The <> angle brackets indicate that a mandatory parameter must be entered in place of the brackets and text inside them.

- **[parameter].**

  The [] square brackets indicate that an optional parameter may be entered in place of the brackets and text inside them.

- **{choice1 | choice2}.**

  The | indicates that only one of the parameters should be entered.

  The {} curly braces indicate that a parameter must be chosen from the list of choices.

4.2.2. Values

- **ipaddr**

  This parameter is a valid IP address, made up of four decimal bytes ranging from 0 to 255. The default for all IP parameters consists of zeros (that is, 0.0.0.0). The interface IP address of 0.0.0.0 is invalid.

- **macaddr**

  The MAC address format is six hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.

- **areaid**

  Area IDs may be entered in dotted-decimal notation (for example, 0.0.0.1). An area ID of 0.0.0.0 is reserved for the backbone. Area IDs have the same form as IP addresses, but are distinct from IP addresses. The IP network number of the sub-netted network may be used for the area ID.

- **routerid**

  The value of <router id> must be entered in 4-digit dotted-decimal notation (for example, 0.0.0.1). A router ID of 0.0.0.0 is invalid.

- **slot/port**

This parameter denotes a valid slot number, and a valid port number. For example, 0/1 represents unit number 1, slot number 0 and port number 1. The <slot/port> field is composed of a valid slot number and a valid port number separated by a forward slash (/).

- **logical slot/port**

  This parameter denotes a logical slot number, and logical port number assigned. This is applicable in the case of a port-channel (LAG). The operator can use the logical slot number, and the logical port number to configure the port-channel.

4.2.3. Conventions

Network addresses are used to define a link to a remote host, workstation, or network. Network addresses are shown using the following syntax:

Table 4-1. Network Address Syntax

Address Type	Format	Range
IPAddr	A.B.C.D	0.0.0.0 to 255.255.255.255
MacAddr	YY:YY:YY:YY:YY:YY	hexadecimal digit pairs

Double quotation marks such as "System Name with Spaces" set off user defined strings. If the operator wishes to use spaces as part of a name parameter then it must be enclosed in double quotation marks.

Empty strings (“”) are not valid user defined strings. Command completion finishes spelling the command when enough letters of a command are typed to uniquely identify the command word. The command may be executed by typing <enter> (command abbreviation) or the command word may be completed by typing the <tab> (command completion).

The value 'Err' designates that the requested value was not internally accessible. This should never happen and indicates that there is a case in the software that is not handled correctly.

The value of '-----' designates that the value is unknown.

4.2.4. Annotations

The CLI allows the user to type single-line annotations at the command prompt for use when writing test or configuration scripts and for better 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.

Some examples are provided below:

! Script file for displaying the ip interface

! Display information about interfaces

show ip interface 0/1 !Displays the information about the first interface

! Display information about the next interface

show ip interface 0/2

! End of the script file

5. Switching Commands

5.1. System Information and Statistics Commands

This section describes the commands that use to display system information or statistics.

5.1.1. show arp

This command displays connectivity between the switch and other devices from service port or management port. The Address Resolution Protocol (ARP) cache identifies the MAC addresses of the IP stations communicating with the switch.

Format show arp

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show arp

    MAC Address        IP Address     Interface
------------------- ---------------- ------------
00:00:5E:00:01:03   172.16.3.254     Management
BC:A5:11:F6:4F:8A   172.16.3.98      Management

(M4500-32C) #
```

5.1.2. show calendar

This command displays the system time.

Format show calendar

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show calendar
```

5.1.3. show process cpu

This command provides the percentage utilization of the CPU by different tasks.

Format show process cpu

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show process cpu

Memory and Process CPU Utilization Info of Unit:1

Memory Utilization Report
status     KBytes
------ ----------
free      1277836
alloc      792756
CPU Utilization:

PID        Name                  5 Secs  60 Secs 300 Secs
---------- ------------------- -------- -------- --------
10         (rcu_sched)           0.00%    0.06%    0.07%
15         (kworker/1:0)         0.00%    0.01%    0.00%
52         (kworker/0:1)         0.00%    0.01%    0.02%
232        (hwmon0)              0.00%    0.01%    0.02%
613        (procmgr)             0.00%    0.08%    0.09%
720        osapiTimer            0.10%    0.11%    0.12%
729        bcmINTR               0.10%    0.07%    0.06%
730        socdmadesc.0          0.20%    0.14%    0.13%
733        bcmMEM_SCAN.0         0.00%    0.04%    0.07%
735        bcmL2X.0              3.11%    3.47%    3.49%
737        bcmCNTR.0             1.24%    1.50%    1.50%
740        bcmLINK.0             2.80%    2.65%    2.64%
741        bcmRX                 0.00%    0.07%    0.07%
742        cpuUtilMonitorTask    0.20%    0.24%    0.25%
744        tL7Timer0             0.00%    0.03%    0.03%
750        simPts_task           0.00%    0.04%    0.04%
753        BootP                 0.10%    0.01%    0.00%
760        emWeb                 0.10%    0.01%    0.01%
774        hapiBroadBfdCtrlTas   0.31%    0.29%    0.29%
796        dot1s_timer_task      0.00%    0.06%    0.06%
800        radius_task           0.00%    0.02%    0.01%
806        snoopTask             0.00%    0.06%    0.07%
812        SNTP                  0.10%    0.01%    0.00%
827        pbrProcessingTask     0.00%    0.01%    0.00%
851        (ospf_app)            0.00%    0.01%    0.02%
888        RMONTask              0.00%    0.21%    0.28%
900        mlagTxTask            0.10%    0.01%    0.00%
924        openrTask             1.66%    1.86%    1.93%
-------------------------- -------- -------- --------
Total CPU Utilization          10.16%   11.30%   11.53%

(M4500-32C) #
```

5.1.4. show process cpu threshold

This command displays the configurations of CPU utilization threshold.

Format show process cpu threshold

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show process cpu threshold

CPU Utilization Monitoring Parameters
Rising Threshold.............................. 90 %
Rising Interval............................... 3600 secs
Falling Threshold............................. 50 %
Falling Interval.............................. 300 secs

CPU Free Memory Monitoring Threshold........... 0 KB

(M4500-32C) #
```

5.1.5. show eventlog

This command displays the event log, which contains error messages from the system.

Format show eventlog

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show eventlog
                                                                    Time
       File                          Line TaskID   Code     yyyy/mm/dd hh:mm:ss
EVENT> Boot!                            0 48474A24 AAAAAAAA 2016/06/07 21:22:57
EVENT> Boot!                            0 48407104 AAAAAAAA 2016/06/07 17:38:56
EVENT> Manual Reload!                   0 48407104 00000000 2016/06/07 17:36:12
EVENT> Boot!                            0 48407104 AAAAAAAA 2016/06/07 17:12:40
EVENT> Manual Reload!                   0 48407104 00000000 2016/06/07 17:09:45
EVENT> Boot!                            0 48407104 AAAAAAAA 2016/06/05 00:04:36
EVENT> Manual Reload Warm!              0 48407104 00000000 2016/06/05 00:01:42
EVENT> Boot!                            0 48407104 AAAAAAAA 2016/06/04 23:38:07
EVENT> Manual Reload Warm!              0 48474A24 00000000 2016/06/04 23:35:09
EVENT> Boot!                            0 48474A24 AAAAAAAA 2016/06/04 22:01:35
EVENT> Boot!                            0 48474A24 AAAAAAAA 2016/06/02 18:09:26
EVENT> Boot!                            0 48474A24 AAAAAAAA 2016/06/02 03:26:04
EVENT> Boot!                            0 48465024 AAAAAAAA 2016/06/01 21:29:27
EVENT> Clear Event Log!                 0 48465024 AAAAAAAA 2016/05/31 23:07:58

(M4500-32C) #
```

5.1.6. show running-config

This command is used to display/capture the current setting of different protocol packages supported on switch. This command displays/captures only commands with settings/configurations with values that differ from the default value. The output is displayed in script format, which can be used to configure another switch with the same configuration.

The paramenter “<scriptname>” means to redirect the current settings to a script file with an assigned name <scriptname>, which needs a fixed file name extension “.scr”.

The paramenter “all” means to display/capture of all commands with settings/configurations that include values that are same as the default values.

The paramenter “control-plane” means to display the running config of control-plane interface.

The paramenter “mlag” means to display the running config of Multi-Chassis Link Aggregation (MLAG).

Format show running-config [<scriptname> | all | interface {<slot/port> | control-plane | loopback <loopback-id> | port-channel <portchannel-id> | tunnel <tunnel-id> | vlan <vlan-id>} | mlag]

Default None

Mode Privileged Exec

Example:

```
(M4500-48XF8C) #show running-config

!Current Configuration:
!
!System Description "M4500-48XF8C, Runtime Code 7.0.0.1"
!System Software Version "7.0.0.1"
!System Up Time          "0 days 0 hrs 9 mins 53 secs"
!Additional Packages     BGP-4,QOS,Multicast,IPv6,Routing,Data Center
!Current System Time: Aug  5 03:13:06 2019
!
configure
vlan database
set igmp 1
set igmp fast-leave 1
exit

igmp-plus 1
time-range
username "admin" passwd 7
d32036926a456949a1dd05f3768212c089add94bccd752314f0c05fedf66f52c407256118c62e461710
1230004dff4ee69c4e4d4eaed9590cfd5fe318b39dac3 level 15
username "admin" role "network-admin"
username "guest" role "network-operator"
line console
exit

line vty
exit
```

```
line ssh
exit

interface vlan 1
exit
!
interface control-plane
exit
ip igmp snooping
application install orig_restful_api
router ospf
exit
ipv6 router ospf
exit
exit

(M4500-48XF8C) #
```

5.1.7. show sysinfo

This command displays switch brief information and MIBs supported.

Format show sysinfo

Default None

Mode Privileged Exec

Example:

```
(M4500-48XF8C) #show sysinfo

System Description.............................. M4500-48XF8C, Runtime Code 7.0.0.1
System Name..................................... M4500-48XF8C
System Location.................................
System Contact..................................
System Object ID................................ 1.3.6.1.4.1.4526.100.3.10
System Up Time.................................. 2 days 21 hrs 19 mins 23 secs

MIBs Supported:

RFC 1907 - SNMPv2-MIB              The MIB module for SNMPv2 entities
HC-RMON-MIB                        The original version of this MIB, published
                                   as RFC3273.
HCNUM-TC                           A MIB module containing textual conventions
                                   for high capacity data types.
SNMP-COMMUNITY-MIB                 This MIB module defines objects to help
                                   support coexistence between SNMPv1, SNMPv2,
                                   and SNMPv3.
SNMP-MPD-MIB                       The MIB for Message Processing and
                                   Dispatching
SNMP-TARGET-MIB                    The Target MIB Module
SNMP-VIEW-BASED-ACM-MIB            The management information definitions for
                                   the View-based Access Control Model for SNMP.
SFLOW-MIB                          sFlow MIB
QNOS-UDLD-MIB                      UDLD MIB
DIFFSERV-DSCP-TC                   The Textual Conventions defined in this
                                   module should be used whenever a
```

	Differentiated Services Code Point is used in a MIB.
QNOS-KEYING-PRIVATE-MIB	The Netgear Private MIB for QNOS Keying Utility
LLDP-EXT-DOT3-MIB	The LLDP Management Information Base extension module for IEEE 802.3 organizationally defined discovery information.
DISMAN-PING-MIB	The Ping MIB (DISMAN-PING-MIB) provides the capability of controlling the use of the ping function at a remote host.
QNOS-OUTBOUNDTELNET-PRIVATE-MIB	The Netgear Private MIB for QNOS Outbound Telnet
DISMAN-TRACEROUTE-MIB	The Traceroute MIB (DISMAN-TRACEROUTE-MIB) provides access to the traceroute capability at a remote host.
RFC 1213 - RFC1213-MIB	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC 2674 - P-BRIDGE-MIB	The Bridge MIB Extension module for managing Priority and Multicast Filtering, defined by IEEE 802.1D-1998.
RFC 2737 - ENTITY-MIB	Entity MIB (Version 2)
RFC 3635 - Etherlike-MIB	Definitions of Managed Objects for the Ethernet-like Interface Types
SWITCHING-EXTENSION-MIB	Switching extension - Layer 2
QNOS-PORTSECURITY-PRIVATE-MIB	Port Security MIB.
IANAifType-MIB	This MIB module defines the IANAifType Textual Convention
MAU-MIB	Management information for 802.3 MAUs.
QNOS-PFC-MIB	The MIB definitions Priority based Flow Control Feature.
QNOS-VPC-MIB	The MIB definitions for MLAG.
QNOS-DOT1X-ADVANCED-FEATURES-MIB	The Netgear Private MIB for QNOS Dot1x Advanced Features
QNOS-RADIUS-AUTH-CLIENT-MIB	The Netgear Private MIB for QNOS Radius Authentication Client.
RADIUS-AUTH-CLIENT-MIB	RADIUS Authentication Client MIB
QNOS-MGMT-SECURITY-MIB	The Netgear Private MIB for QNOS Mgmt Security
RFC 1850 - OSPF-TRAP-MIB	The MIB module to describe traps for the OSPF Version 2 Protocol.
QNOS-ROUTING-MIB	QNOS Routing - Layer 3
IP-MIB	The MIB module for managing IP and ICMP implementations, but excluding their management of IP routes.
RFC 1657 - BGP4-MIB	Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2
QNOS-QOS-MIB	QNOS Flex QOS Support
QNOS-QOS-COS-MIB	QNOS Flex QOS COS
RFC 2932 - IPMROUTE-MIB	IPv4 Multicast Routing MIB
RFC 5060 - PIM-STD-MIB	Protocol Independent Multicast MIB
IANA-RTPROTO-MIB	IANA IP Route Protocol and IP MRoute Protocol Textual Conventions
IPMROUTE-STD-MIB	The MIB module for management of IP Multicast routing, but independent of the specific multicast routing protocol in use.
RFC 2465 - IPV6-MIB	Management Information Base for IP Version 6: Textual Conventions and General Group
RFC 3419 - TRANSPORT-ADDRESS-MIB	Textual Conventions for Transport Addresses
QNOS-IPV6-LOOPBACK-MIB	The Netgear Private MIB for QNOS Loopback IPV6 address configuration.
QNOS-DCBX-MIB	The MIB module defines objects to configure DCBX
IEEE8021-CN-MIB	Congestion notification module for managing IEEE 802.1Qau
LLDP-V2-TC-MIB	Textual conventions used throughout the IEEE Std 802.1AB version 2 and later MIB modules.

5.1.8. POST Diagnostic Commands

The M4500 series switches support Power On Self Test (POST) commands. These commands test major hardware components to detect errors and let you see the test results.

5.1.8.1. show system self-test

Use this command to display the test result of POST.

Format show system self-test

Mode Privileged Exec

Example:

```
(M4500-48XF8C) #show system self-test

 Date: Mar-13-2020 08:45:10

Version: 1.0.0.0

Summary: Diagnostics Pass

M4500-48XF8C:                 1IX8UZZ0005 QTFCU38290029

PSU-1: Present               700-013917-0000 L257U4000105P
PSU-2: Present               700-013917-0000 L257U4000305P
FAN-1: Present
FAN-2: Present
FAN-3: Present
FAN-4: Present
FAN-5: Present
FAN-6: Present

Test                          Result
==================================
CPU Detect                    Pass
IPMI Fan & Thermal Sensors    Pass
RPSU Env                      Pass
SDRAM                         Pass
SATA SSD                      Pass
Management Interface          Pass
Loopback MAC Interface        Pass
LED                           Pass
```

5.1.8.2. run system self-test

Use this command to run POST. After you enter this command, the switch reboots and runs the self-check function on the major hardware components. The major hardware components include the CPU, RAM, Flash memory, network ports, Fans, LEDs, and the power modules. After the self-check function is complete, the system reboots again and runs the operating system automatically.

Format run system self-test

Default None

Mode Privileged Exec

5.1.9. show system

This command displays switch system information.

Format show system

Default None

Mode Privileged Exec

Example:

```
(M4500-48XF8C) #show system

System description: M4500-48XF8C, Runtime Code 7.0.0.1
System object ID  : 1.3.6.1.4.1.4526.100.3.10
System information
System Up time: 2 days, 21 hours, 17 minutes, and 28 seconds
System Name                : M4500-48XF8C
System Location            :
System Contact             :
MAC address                : D8-C4-97-B5-6A-BF
Protocol Current           : None

(M4500-48XF8C) #
```

5.1.10. show tech-support

Use this command displays switch system information and configurations when you contact technical support. The output of the show tech-support command combines the output of the following commands: show version, show sysinfo, show interface status, show logging, show event log, show logging buffered, show trap log, show running config, etc.

The parameter “file” means to write the output into a file with file name “TechSupport”.

Other parameters are used to display the information of assigned component.

Format show tech-support [{{bfd | bgp | datacenter | dcvpn | dot1q | dot1s | dot3ad | igmp | layer3 | link_dependency | lldp | log | mcast | mlag | multicast | ospfv2 | ospfv3 | pimsm | routing | sim | snooping | switching | system | vrrp} [file]} | file}]

Default None

Mode Privileged Exec

Example:

```
(M4500-48XF8C) # show tech-support

*************** show version ***************


Switch: 1

System Description............................. M4500-48XF8C, Runtime Code 7.0.0.1
Machine Model.................................. M4500-48XF8C
Serial Number.................................. QTFCU38510002
Burned In MAC Address.......................... BC:A5:11:B5:6A:BF
Software Version............................... 7.0.0.1
Software Storage............................... mSATA
Additional Packages............................ BGP-4
                                                QOS
                                                Multicast
                                                IPv6
                                                Routing
                                                Data Center
                                                OpEN API
                                                Prototype Open API



*************** show sysinfo ***************


System Description............................. M4500-48XF8C
Runtime Code..................................... 7.0.0.1
System Name.................................... Switch
System Location.................................
System Contact..................................
System Object ID............................... 1.3.6.1.4.1.4526.100.3.10
System Up Time................................. 0 days 2 hrs 43 mins 19 secs

(* note: this command displays information more than 3000 lines, so here we omit
   remained messages.)
    :
    :
(M4500-48XF8C) #
```

5.1.11. show hardware

This command displays inventory and hardware information for the switch.

Format show hardware

Default None

Mode Privileged Exec

Example:

```
(M4500-48XF8C) #show hardware

Switch: 1
```

```
System Description.............................. M4500-48XF8C, Runtime Code 7.0.0.1
Machine Model................................... M4500-48XF8C
Serial Number................................... QTFCU38510002
Burned In MAC Address.........................

 Switch: 1

 System Description.............................. M4500-48XF8C, Runtime Code 7.0.0.1
 Machine Model................................... M4500-48XF8C
 Serial Number................................... QTFCU38510002
 Burned In MAC Address........................... BC:A5:11:B5:6A:BF
 Software Version................................ 7.0.0.1
 Software Storage................................ mSATA
 Additional Packages............................. BGP-4
:B5:6A:BF
Software Version................................ 7.0.0.1
Manufacturer Name............................... QSMC
Date Code....................................... 12/07/2018 00:00:00

FAN 1 Status.................................... Active
FAN 1 Airflow Direction......................... Back to Front
FAN 2 Status.................................... Active
FAN 2 Airflow Direction......................... Back to Front
FAN 3 Status.................................... Active
FAN 3 Airflow Direction......................... Back to Front
FAN 4 Status.................................... Active
FAN 4 Airflow Direction......................... Back to Front
FAN 5 Status.................................... Active
FAN 5 Airflow Direction......................... Back to Front
FAN 6 Status.................................... Active
FAN 6 Airflow Direction......................... Back to Front

Switch Power+ 1................................. Exist
Type............................................ Removable
Model........................................... ARTESYN
Serial Number................................... L257VH000Y05P
Revision Number................................. 05
FW Version...................................... 2
Airflow Direction............................... Back to Front

Switch Power+ 2................................. Exist
Type............................................ Removable
Model........................................... ARTESYN
Serial Number................................... L257V2001F05P
Revision Number................................. 05
FW Version...................................... 2
Airflow Direction............................... Back to Front

Additional Packages............................. BGP-4
................................................. QOS
................................................. Multicast
................................................. IPv6
................................................. Routing
.................................................Data Center
................................................. OpEN API
................................................. Prototype Open API

(M4500-48XF8C) #
```

5.1.12. show version

This command displays inventory, software packages and license key information for the switch.

Format show version

Default None

Mode Privileged Exec

Example:

```
(M4500-48XF8C) #show version

Switch: 1

System Description..............................  M4500-48XF8C, Runtime Code 7.0.0.1
Machine Model...................................  M4500-48XF8C
Serial Number...................................  QTFCU38510002
Burned In MAC Address...........................  BC:A5:11:B5:6A:BF
Software Version................................  7.0.0.1
Software Storage................................  mSATA
Additional Packages.............................  BGP-4
.................................................  QOS
.................................................  Multicast
.................................................  IPv6
.................................................  Routing
.................................................  Data Center
.................................................  OpEN API
.................................................  Prototype Open API
(M4500-48XF8C) #
```

5.1.13. show logingsessin

This command displays serial port or remote login connections to the switch.

The parameter “long” means to display full user names of login sessions.

Format show loginsession [long]

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show loginsession

ID   User Name     Connection From       Idle Time  Session Time Session Type
---- ------------ --------------------- ---------- ------------ ------------
00   admin         EIA-232               00:00:00   02:08:12     Serial
01   guest         172.16.3.68           00:00:05   00:00:05     SSH

(M4500-32C) #
```

5.1.14. show command filter

All commands starting with keyword “show” can use below parameters to refine output or redirect output to a file. Following any show command to use symbol “|” to set filter and it uses regular expression to math assigned keyword.

The parameter “commands” means any show command of CLI.

The parameter “**|**” means to use filter option.

The parameter “begin” sets output to begin with the line that matches assigned keyword.

The parameter “exclude” sets output to exclude lines that matches assigned keyword.

The parameter “include” sets output to include lines that matches assigned keyword only.

The parameter “section” sets output to include only a specified section of the content (e.g., “interface 0/1”) with a configurable end-of-section delimiter. If multiple sections matching the specified string match criteria are part of the output, then all instances are displayed. Each section begins with the line containing the starting keyword and ends with the line containing the ending keyword. If there is a line, for example, the line **L** that contains the starting keyword, and there is no line containing the ending keyword in the original output, the parameter “section” will extract a section from the line **L** to the final line of the original output. (The default ending keyword is “exit”.)

The parameter “redirect” means to write output to a remote file which locates the assigned “url”, and “url” could be TFTP, FTP or SFTP.

Format show command | {[begin <keyword>] [exclude <keyword>] [include <keyword>][section <starting keyword> [ending keyword]] [redirect url]}

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show interface counters detailed 0/1 | begin "Total Packets" exclude
"0"

Total Packets Received (Octets)................ 438677
Packets Received 64 Octets..................... 115
Packets Received 65-127 Octets................. 376
Packets Received 128-255 Octets................ 2136
Packets RX and TX 64 Octets.................... 117
Packets RX and TX 65-127 Octets................ 36293
Packets RX and TX 128-255 Octets............... 2136

Total Packets Received Without Errors.......... 2729
Multicast Packets Received..................... 2258
Broadcast Packets Received..................... 471

Packets Discarded by Chip Debug Counter........ 225
```

```
Total Received Packets Discarded..... 225

Packets Transmitted 64 Octets..... 2
Packets Transmitted 65-127 Octets..... 35917
Max Frame Size..... 1518

Total Packets Transmitted Successfully..... 35919
Multicast Packets Transmitted..... 35919

MSTP BPDUs Transmitted..... 33675

(M4500-32C) #
```

5.1.15. show transceiver device

This command displays summary of digital optical monitor information for the switch.

Format show transceiver device

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show transceiver device


            Gigabit Ethernet  Vendor Name       Vendor Part
Interface   Compliance Code                     Number
----------- ----------------- ----------------- -----------------
0/7          10GBase-SR       FINISAR CORP.     FTLX8571D3BCL
0/9          10GBase-SR       FINISAR CORP.     FTLX8571D3BCL


(++) : high alarm, (+) : high warning, (-) : low warning, (--) : low alarm.
mA: milliamperes, dBm: decibels (milliwatts), NA: not available, -: null/unknown.

             Temperature    Voltage    Tx bias current    Tx Power    Rx Power
Interface     (Celsius)     (Volts)         (mA)             (dBm)       (dBm)
------------ -------------- ---------- ------------------ ------------ ----------
0/7          23.15          3.31       7.92               -2.17        -2.28
0/9          30.14          3.29       7.95               -1.91        -2.02
…
…
0/51         31.59          3.27       6.88               -23.47 (--)  -3.45
0/52         30.77          3.27       6.86               -23.47 (--)  -4.15

(M4500-32C) #
```

5.1.16. show transceiver interface

This command displays detail of digital optical monitor information for the switch.

Format show transceiver interface detail [<intf-range>]

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show transceiver interface detail 0/7

(++) : high alarm, (+) : high warning, (-) : low warning, (--) : low alarm.
mA: milliamperes, dBm: decibels (milliwatts), NA: not available, -: null/unknown.

Interface..................................... 0/7
Gigabit Ethernet Compliance Codes............. 10GBase-SR
Vendor Name................................... FINISAR CORP.
Vendor Part Number............................ FTLX8571D3BCL
Vendor Serial Number.......................... AP50L3K
Vendor Revision Number........................ A
Vendor Manufacturing Date..................... 2013/02/02
Wavelength.................................... 850 nm
Link length supported for 50um OM2 fiber...... 82 m
Link length supported for 62.5um OM1 fiber..... 33 m
Link length supported for 50um OM3 fiber...... 300 m
Temperature................................... 34.66 Celsius
Voltage....................................... 3.31 Volts
Tx bias current............................... 8.17 mA
Tx Power...................................... -2.15 dBm
Rx Power...................................... -2.26 dBm
Temperature high alarm threshold.............. 80.00 Celsius
Temperature high warning threshold............ 70.00 Celsius
Temperature low warning threshold............. 0.00 Celsius
Temperature low alarm threshold............... -5.00 Celsius
Voltage high alarm threshold.................. 3.46 Volts
Voltage high warning threshold................ 3.40 Volts
Voltage low warning threshold................. 3.20 Volts
Voltage low alarm threshold................... 3.14 Volts
Tx bias current high alarm threshold.......... 12.00 mA
Tx bias current high warning threshold........ 10.00 mA
Tx bias current low warning threshold......... 2.00 mA
Tx bias current low alarm threshold........... 0.00 mA
Tx power high alarm threshold................. 3.97 dBm
Tx power high warning threshold............... 3.49 dBm
Tx power low warning threshold................ -2.50 dBm
Tx power low alarm threshold.................. -3.00 dBm
Rx power high alarm threshold................. 3.97 dBm
Rx power high warning threshold............... 3.49 dBm
Rx power low warning threshold................ -9.50 dBm
Rx power low alarm threshold.................. -10.00 dBm

(M4500-32C) #
```

5.1.17. show process memory

This command provides the memory usage by different tasks.

Format show process memory

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show process memory

  Total:              8142492 KB
  Allocated:          2451536 KB
  Free:               5690956 KB

  Component                       CurrentAllocated[change]
MaxAllocated[Allocs/Frees]
  1   - SIM                            80904570[      +0]        82085413
[1697/26]
  2   - NIM                              959361[      +0]          959361 [20/0]
  3   - TRAPMGR                            1456[      +0]            1456 [1/0]
  5   - CNFGR                             20868[      +0]           20868 [108/0]
  ...
  177 - COMMAND_SCHEDULER                 69728[      +0]           69728 [3/0]
  178 - -Unknown-                          6720[      +0]            6720 [3/0]
  179 - BHD                                7484[      +0]            7484 [2/0]

  Total Current Usage = 2064220254
  osapi Debug overhead = 1928808


(M4500-32C) #
```

5.1.18. show process app-list

This command displays user and system applications known to the Process Manager.

Format show process app-list

Default None

Example:

```
(M4500-32C) #show process app-list

                             Admin     Auto      Running

ID    Name            PID    Status    Restart   Status

---- ---------------- -----  --------- --------- --------

   1 switchdrvr       31539  Enabled   Disabled  Running
```

```
   2 syncdb           31540  Enabled   Disabled  Running

   3 syncdb-test          0  Disabled  Disabled  Stopped

   4 proctest             0  Disabled  Enabled   Stopped

   5 user.start           0 Enabled   Disabled  Stopped

   6 opensshd         32194  Enabled   Enabled   Running

   7 netconf-opensshd     0  Disabled  Enabled   Stopped

   8 vr-agent-0       32059  Enabled   Enabled   Running

   9 ospf-00          32065  Enabled   Enabled   Running

  10 ping-0           32143  Enabled   Enabled   Running

  11 traceroute-0     32150  Enabled   Enabled   Running

(M4500-32C) #
```

5.1.19. show process app-resource-list

This command displays the configured and in-use resources of each application known to the Process Manager.

Format show process app-resource-list

Default None

Example:

```
(M4500-32C) #show process app-resource-list

                            Memory     CPU        Memory      Max Mem

ID   Name              PID    Limit      Share      Usage       Usage

---- ---------------- ----   ---------- ---------  ----------  ----------

   1 switchdrvr       31539   Unlimited Unlimited     2047 MB     2047 MB

   2 syncdb           31540   Unlimited Unlimited       16 MB       16 MB

   3 syncdb-test          0   Unlimited Unlimited        0 MB        0 MB

   4 proctest             0        10 MB       20%        0 MB        0 MB

   5 user.start           0   Unlimited Unlimited        0 MB        0 MB

   6 opensshd         32194   Unlimited Unlimited        1 MB        3 MB

   7 netconf-opensshd     0   Unlimited Unlimited        0 MB        0 MB
```

```
   8 vr-agent-0       32059   Unlimited Unlimited        9 MB       10 MB

   9 ospf-00          32065   Unlimited Unlimited        6 MB        7 MB

  10 ping-0           32143   Unlimited Unlimited        0 MB        1 MB

  11 traceroute-0     32150   Unlimited Unlimited        0 MB        1 MB

(M4500-32C) #
```

5.1.20. show process proc-list

This command displays the processes started by applications created by the Process Manager.

Format show process proc-list

Default None

Example:

```
(M4500-32C) (Config)#show process proc-list

       Process         Application                   VM Size  VM Peak            Process

PID    Name            ID-VRID-Name          Chld    (KB)     (KB)    FD Count    Up Time

-----  --------------- ----------------------------  ------   ------  --------   -------------

31476 procmgr          0-0-procmgr            No          0        0         9   0days-3:43:56

31539 switchdrvr       1-0-switchdrvr         No          0        0       329   0days-3:43:56

31540 syncdb           2-0-syncdb             No          0        0        45   0days-3:43:56

32059 vr_agent_app     8-0-vr-agent-0         No          0        0        21   0days-3:43:50

32065 ospf_app         9-0-ospf-00            No          0        0        18   0days-3:43:50

32143 ping_app         10-0-ping-0            No          0        0        13   0days-3:43:48

32150 traceroute_app   11-0-traceroute-0      No          0        0        13   0days-3:43:48

32194 opensshd         6-0-opensshd           No          0        0         7   0days-3:43:43

(M4500-32C) #
```

5.1.21. show environment

This command displays vital environment status data, including temperature, fan (speed, state), RPSU (temperature, fan speed, state, and power).

Format show environment

Mode Privileged EXEC

Display Message

Fields	Definition
Temp	The current temperature (C).
Crit Temp	The maximum limit of temperature.
State	The status of module.
Max Temp	The highest temperature after the system boot.
Type	The type of module (fixed or removable).
Speed	The fan speed (RPM).
Description	The name of sensor.
Power	The power of RPSU (W).

Example:

The following shows examples of the command.

```
(M4500-32C) #show environment

Temperature Sensors:

Unit  Sensor  Description   Temp (C)   Crit_Temp (C)   State     Max_Temp (C)

----  ------  ------------  ---------  --------------  --------  -------------

1     1       Temp-1        36         67              Normal    38

1     2       Temp-2        37         65              Normal    39

1     3       Temp-3        31         61              Normal    32

1     4       Temp-4        26         59              Normal    28

1     5       Temp-5        34         64              Normal    37

1     6       Temp-6        42         76              Normal    44

1     7       Temp-7        31         67              Normal    33
```

```
Fans:

Unit Fan Description    Type      Speed (RPM)   State

---- --- -------------- --------- ------------- -------------

1    1   Fan-1          Removable -             Failed

1    2   Fan-2          Removable -             Failed

1    3   Fan-3          Removable -             Failed

1    4   Fan-4          Removable -             Failed

1    5   Fan-5          Removable -             Failed

1    6   Fan-6          Removable -             Failed

1    7   Fan-7          Removable -             Failed

1    8   Fan-8          Removable -             Failed

1    9   Fan-9          Removable -             Failed

1    10  Fan-10         Removable -             Failed

1    11  Fan-11         Removable -             Failed

1    12  Fan-12         Removable -             Failed


Power Modules:

Description  Type        Temp1 (C) Temp2 (C) Speed (RPM) Power (W) State

------------ ----------- --------- --------- ----------- --------- ------------

PS-1         Removable   28        46        3150        60        Operational

PS-2         Removable   27        45        3000        50        Operational
```

5.1.22. show configuration files

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

Fields	Definition
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.

5.1.23. 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

no process cpu threshold type total

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).
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).

5.1.24. 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 <1-8142712>

no memory free low-watermark processor

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).

5.1.25. show supported cardtype

Use this command to display the supported card type(s) information.

Format show supported cardtype

Mode Privileged Exec

Display Message

Fields	Definition
CID	The card index
Card Model ID	The model identifier for each card index

5.1.26. show supported cardtype <cardindex>

Use this command to display the specified card information.

Format show supported cardtype <cardindex>

Parameter	Definition
<cardindex>	Specifies a card index (CID) to be displayed.

Mode Privileged Exec

Display Message

Fields	Definition
Card Type	The numerical identifier unique to this card hardware
Model Identifier	The model identifier for specified card index
Card Description	The text describing this card type

5.1.27. pager

Use this command to enable or disable pager admin mode for current access line.

Format [no] pager

Default Enabled

Mode Privileged Exec

5.1.28. show pager

Use this command to display the pager configuration.

Format show pager

Mode Privileged Exec

Example:

```
(M4500-48XF8C) #show pager

Pager Admin mode.............................. Enable
```

5.2. Device Configuration Commands

5.2.1. Interface commands

5.2.1.1. show interface status

The command displays a summary of information for a specific interface or all interfaces.

Format show interface status [{<slot/port> | err-disabled | loopback <loopback-id> | port-channel <port-channel-id> | tunnel <tunnel-id> | vlan <vlan-id>}]

Parameter	Definition
no parameter	To display information for all interfaces.
<slot/port>	Specifies Interface number .
err-disabled	Specifies to display the interfaces which are err disabled.
loopback <0-63>	Specifies to display information for the loopback interfaces. The range of the loopback ID is 0 to 63
port-channel <1-64>	Specifies to display information for the port-channel interfaces. The range of the port-channel ID is 1 to 64.
tunnel <0-7>	Specifies to display information for the tunnel interfaces. The range of the tunnel ID is 0 to 7.
vlan <vlan-id>	Specifies to display information for the vlan interfaces. The range of the VLAN ID is 1 to 4093.

Mode Privileged EXEC

The following will show the information of each command with a different parameter.

5.2.1.1.1. show interface status

Displays information for all interfaces.

Fields	Definition
Intf	The physical slot and physical port.
Type	If not blank, this field indicates that this port is a special type of port. The possible values are:

	Source: This port is a monitoring port. **PC Mbr:** This port is a member of a port-channel (LAG). **Dest:** This port is a probe port.
Admi Mode (Admin Mode)	Selects the Port control administration state. The port must be enabled in order for it to be allowed into the network. It may be enabled or disabled. The factory default is enabled.
Phy Mode (Physical Mode)	Selects the desired port speed and duplex mode. If auto-negotiation support is selected, then the duplex mode and speed will be set from the auto-negotiation process. Note that the port's maximum capability (full duplex 100M) will be advertised. Otherwise, this object will determine the port's duplex mode and transmission rate. The factory default is Auto.
Phy Stat	Indicates the port speed and duplex mode.
Link Stat	Indicates whether the Link is up or down.
Link Trap	This object determines whether to send a trap when link status changes. The factory default is enabled.
LACP Mode	Displays whether LACP is enabled or disabled on this port.
Flow Mode	Displays flow control mode.
Cap. Status (Capabilities Status)	Displays interface capabilities the port supports.
Expanded From	Indicates the port from which this port is expanded.

5.2.1.1.2. show interface status <slot/port>

Displays information for a specific interface.

Fields	Definition
Interface	The physical slot and physical port.
ifIndex	Displays the interface index associated with the port.
Description	Description string attached to a port. It can be of up to 64 characters in length.
Admin Mode	Selects the Port control administration state. The port must be enabled in order for it to be allowed into the network. It may be enabled or disabled. The factory default is enabled.
Physical Mode	Selects the desired port speed and duplex mode. If auto-negotiation support is selected, then the duplex mode and speed will be set from the auto-negotiation process. Note that the port's maximum capability (full duplex 100M) will be

	advertised. Otherwise, this object will determine the port's duplex mode and transmission rate. The factory default is Auto.
Physical Status	Indicates the port speed and duplex mode.
Cable Type	Displays interface cable type.
Link Status	Indicates whether the Link is up or down.
Link Trap	This object determines whether to send a trap when link status changes. The factory default is enabled.
LACP Mode	Displays whether LACP is enabled or disabled on this port.
Flow Control Mode	Displays flow control mode.
Capability Information	Displays interface capabilities.
MAC Address	Displays interface mac address.
Bit Offset Val	Displays the bit offset value which corresponds to the port when the MIB object type PortList is used to manage in SNMP.

5.2.1.1.3. show interface status err-disabled

Displays interfaces which are error disabled.

Fields	Definition
interface	An interface that is error disabled.
Errdisabled Reason	The cause of the interface being error disabled.
Auto-Recovery Time Left	The amount of time left before auto recovery begins.

5.2.1.1.4. show interface status loopback <0-63>

Displays information for the loopback interfaces.

Fields	Definition
Interface	The interface name.
ifIndex	Displays the interface index associated with the port.
Description	Description string attached to the port-channel. It can be of up to 64 characters in length.

Admin Mode	Displays the port-channel control administration state.
Physical Mode	The speed and duplex mode setting on the interface.
Physical Status	Indicates the speed and duplex mode for the physical interface.
Cable Type	Displays interface cable type.
Link Status	Indicates whether the Link is up or down.
Link Trap	Indicates whether to send a trap when link status changes. The factory default is enabled.
LACP Mode	Displays whether LACP is enabled or disabled on this port.
Flow Control Mode	Displays flow control mode.
Capability Information	Displays interface capabilities.
MAC Address	Displays the Mac address of loopback interface.
Bit Offset Val	Displays the bit offset value which corresponds to the port when the MIB object type PortList is used to manage in SNMP.

5.2.1.1.5. show interface status port-channel <1-64>

Displays information for the port-channel interface.

Fields	Definition
Interface	The interface name.
ifIndex	Displays the interface index associated with the port.
Description	Description string attached to the port-channel. It can be of up to 64 characters in length.
Admin Mode	Displays the port-channel control administration state.
Physical Mode	The speed and duplex mode setting on the interface.
Physical Status	Indicates the speed and duplex mode for the physical interface.
Cable Type	Displays interface cable type.
Link Status	Indicates whether the Link is up or down.
Link Trap	Indicates whether to send a trap when link status changes. The factory default is enabled.
LACP Mode	Displays whether LACP is enabled or disabled on this port.

Flow Control Mode	Displays flow control mode.
Capability Information	Displays interface capabilities.
Bit Offset Val	Displays the bit offset value which corresponds to the port when the MIB object type PortList is used to manage in SNMP.

5.2.1.1.6. show interface status tunnel <0-7>

Displays information for the tunnel interface.

Fields	Definition
Interface	The interface name.
ifIndex	Displays the interface index associated with the interface.
Description	Description string attached to an interface .
Admin Mode	Displays the administration state.
Physical Mode	The speed and duplex mode setting on the interface.
Physical Status	Indicates the speed and duplex mode for the physical interface.
Cable Type	Displays interface cable type.
Link Status	Indicates whether the Link is up or down.
Link Trap	This object determines whether to send a trap when link status changes. The factory default is enabled.
LACP Mode	Displays whether LACP is enabled or disabled on this port.
Flow Control Mode	Displays flow control mode.
Capability Information	Displays interface capabilities.
MAC Address	Displays interface mac address.
Bit Offset Val	Displays the bit offset value which corresponds to the interface when the MIB object type PortList is used to manage in SNMP.

5.2.1.1.7. show interface status vlan <1-4093>

Displays information for the vlan interface.

Fields	Definition

Interface	The interface name.
ifIndex	Displays the interface index associated with the interface.
Description	Description string attached to an interface .
Admin Mode	Displays the administration state.
Physical Mode	The speed and duplex mode setting on the interface.
Physical Status	Indicates the speed and duplex mode for the physical interface.
Cable Type	Displays interface cable type.
Link Status	Indicates whether the Link is up or down.
Link Trap	This object determines whether to send a trap when link status changes. The factory default is enabled.
LACP Mode	Displays whether LACP is enabled or disabled on this port.
Flow Control Mode	Displays flow control mode.
Capability Information	Displays interface capabilities.
MAC Address	Displays interface mac address.
Bit Offset Val	Displays the bit offset value which corresponds to the interface when the MIB object type PortList is used to manage in SNMP.

5.2.1.2. show interface counters

The command displays a summary of statistics for a specific interface or all interfaces.

Format show interface counters [{<slot/port> |port-channel <port-channel-id> | detailed {<slot/port> | port-channel <port-channel-id> | switchport }}]

Parameter	Definition
no parameter	Displays summary statistics for all interfaces.
<slot/port>	Displays summary statistics for a specific interface.
port-channel <port-channel-id>	Displays summary statistics for the port-channel interfaces. The range of the port-channel ID is 1 to 64.
Detailed <slot/port>	Display detailed statistics for a specific interface.
Detailed port-channel <port-channel-id>	Display detailed statistics for the port-channel interfaces.

Detailed switchport	Display detailed statistics for the entire switch.

Mode Privileged EXEC

The following will show the counter information for the command with a different parameter.

5.2.1.2.1. show interface counters

Displays summary statistics for all interfaces.

Fields	Definition
Packets Received Without Error	The total number of packets (including broadcast packets and multicast 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.
Total Bytes Received	The total number of inbound bytes received by the interface.
Unicast Packets Received	The number of inbound unicast packets received by the interface.
Multicast Packets Received	The number of inbound multicast packets received by the interface.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Total Received 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 Errors	The total number of packets transmitted out of the interface.
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Total Bytes Transmitted	The total number of outbound bytes transmitted by the interface.
Unicast Packets Transmitted	The number of outbound unicast packets transmitted by the interface.
Multicast Packets Transmitted	The number of outbound multicast packets transmitted by the interface.
Broadcast Packets Transmitted	The number of outbound broadcast packets transmitted by the interface.
Total Transmit Packets Discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected.

Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

5.2.1.2.2. show interface counters detailed

Displays detailed statistics for a specific interface.

Fields	Definition
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 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 1518 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 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 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 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 that were between 256 and 512 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 512-1023 Octets	The total number of packets (including bad packets) received that were between 512 and 1024 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 that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX > 1518 Octets	The total number of packets (including bad packets) received that were longer than 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Total Packets Received Without Errors	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.
Multicast Packets Received	The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
Broadcast Packets Received	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
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 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.

Undersize Received	The total number of packets received that were less than 64 octets in length with GOOD CRC(excluding framing bits but including FCS octets).
Fragments Received	The total number of packets received that were less than 64 octets in length with ERROR CRC(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 FCS with a non-integral number of octets.
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 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.
MTU Errors	The number of packets whose size exceeded the MTU of the interface.
Packets Discarded by Chip Debug Counter	The number of inbound packets which were chosen to be discarded by chip debug.
Total Received 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.
Total Packets Transmitted (Octets)	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.
Packets Transmitted 64 Octets	The total number of packets (including bad packets) transmitted 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) transmitted 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) transmitted 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) transmitted 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) transmitted 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) transmitted 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 (including bad packets) transmitted that were greater than 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Max Frame Size	The maximum size of the Info (non-MAC) field that this port will receive or transmit.
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.
Multicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a Multicast 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.
Tx 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.
Total Transmit Errors	The sum of Single, Multiple, and Excessive Collisions.
FCS Error	Frame Check Sequence errors.
Total Transmit Packets Discarded	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 Collision Frames	A count of frames for which transmission on a particular interface fails due to excessive collisions.
Packets Dropped by MMU	A count for the packets dropped by the MMU. There are reasons for MMU to drop packets, such as CBP full, HOL blocking, etc.
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.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

5.2.1.2.3. show interface counters detailed switchport

Display statistics for the entire switch.

Fields	Definition
Total Packets Received (Octets)	The total number of octets of data received by the processor (excluding framing bits but including FCS octets).
Packets Received Without Error	**Packets Received Without Error:** The total number of packets (including broadcast packets and multicast packets) received by the processor.
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Multicast Packets Received	The total number of packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
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.
Multicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a Multicast 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.
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 Currently 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.
Dynamic VLAN Entries	The number of presently active VLAN entries on this switch that have been created by GVRP registration.
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.

5.2.1.3. show interface dampening

This command displays the status and configured parameters of the interfaces configured with dampening.

The CLI command “clear counters” resets the flap counter to zero.

The interface CLI command “no shutdown” reset the suppressed state to False.

Any change in the dampening configuration resets the current penalty, reuse time and suppressed state to their default value, meaning 0, 0, and False respectively.

Format show interface dampening

Mode Privileged EXEC

Display Message

Fields	Definition
Interface	The interface name.
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 second.
MaxPenalty	Maximum possible penalty.
Restart	Configured restart penalty.

5.2.1.4. show interface loopback

The command displays the configured loopback interface information.

Format show interface loopback [{<0-63> | vrf <vrf-name>}]

Parameter	Definition
<0-63>	The loopback ID
vrf-name	Specify the name of the VRF

Mode Privileged EXEC

Display Message

Fields	Definition
Loopback Id	The loopback ID associated with the rest of the information in the row. This item is shown only when a loopback Id is not specified.
interface	The interface name. This item is shown only when a loopback Id is not specified.
IP Address	The address of the interface.
Interface Link Status	Shows whether the link is up or down.
IPv6 Prefix is	The IPv6 address of the interface
MTU size	The maximum transmission size for packets on the interface in bytes

5.2.1.5. show interface port-channel

This command displays the capabilities of all port-channels (LAGs) on the device as well as a summary of individual port-channel.

Format show interface port-channel [{ <ID> | brief | system priority }]

Parameters	Definition
<ID>	The port-channel interface number. The range of the port-channel ID is 1 to 64.
brief	Display port-channel static capability and summary information for the device.
system priority	Display port-channel system priority.

Mode Privileged EXEC

Display Message

Fields	Definition
Port Channel ID	The port-channel‘s ID.

Channel Name	The name of the port-channel.
Link State	Indicates whether the link is up or down.
Admin Mode	Indicates if the port-channel is enabled or not .
Link Trap Mode	Indicates whether or not to send a trap when link status changes. The factory default is enabled.
STP Mode	Indicates if the STP mode for the interface is enabled or not .
Type	Indicates whether the port-channel is statically or dynamically maintained.
Port-channel Min-links	Indicates the minimum links for the port-channel.
Load Balance Option (Src/Dest MAC, VLAN, EType, incoming port)	The load balance option associated with this LAG..
LACP Fallback Mode	May be enabled or disabled. The factory default is disabled.
LACP Fallback Timeout	This field displays the LACP fallback timeout, the timeout default is 5sec.
Admin Key	Indicates the administrative value of the LACP actor admin key
Mbr Ports	Lists the ports that are members of this port-channel, in slot/port notation
Active Ports (Port Active)	Lists the ports that are actively participating in this port-channel.
Port Speed	Speed of the port-channel port
Device/Timeout	Displays the device timeout value of actor and partner. The value of device timeout should be short (1 second) or long(30 seconds).

5.2.1.6. show interface port-mode

The command displays the hardware profile information for the 100G ports.

Format show interface port-mode [<slot/port>]

Mode Privileged EXEC

Display Message

Fields	Definition
100G Interface	Indicates the interface number of 100G port.
40G Interface	Indicates the interface number of 40G port.
50G Interface	Indicates the interface number of 50G port.

25G Interface	Indicates the interface number of 25G port.
10G Interfaces	Indicates the interface number of 10G ports.
Configured Mode	Indicates the configured mode of the 100G port. The mode should be 1x100G, 1x40G, 2x50G, 4x25G, or 4x10G.
Operating Mode	Indicates the current operational mode of the 100G port. The mode should be 1x100G, 1x40G, 2x50G, 4x25G, or 4x10G.
Expandable Option(s)	Indicates the expanded mode this interface can support
Expanded Interfaces	Indicates the corresponding port numbers after this interface is expanded

5.2.1.7. show interface priority flow control

The command displays the priority flow control (PFC) information of a given interface or all interfaces.

Format show interface [<slot/port>] priority-flow-control

Parameter	Definition
slot/port	Specifies the interface number as the slot/port format.

Mode Privileged EXEC

When an interface number is not provided, it will display all the interfaces.

Display Message

Fields	Definition
Interface Detail	The port for which data is displayed.
Operational State	The operational status of the interface.
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.
Operational 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. The number does not include duplicate configurations.
Incompatible Configuration Count	The number of received configurations that are 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.
Port	The port list for which data is displayed.
Drop Priorities	The 802.1p priority values that are configured with a drop priority on the interface.
Non-Drop Priorities	The 802.1p priority values that are configured with a no-drop priority on the interface.
Operational Status	The operational status of the interface.

5.2.1.8. show interface switch

This command displays a summary of statistics for all CPU traffic.

Format show interfaces switch

Mode Privileged EXEC

Parameter	Definition
Packets Received Without Error	The total number of packets received from the interface.

Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
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 Errors	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.
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.

5.2.1.9. show interface switchport

This command displays VLAN port information.

Format show interface switchport [{<slot/port> | port-channel <1-64>}]

Parameter	Definition
no parameter	To display information for all ports.
<slot/port>	Specifies Interface number
port-channel <1-64>	Specifies to display information for the port-channel. The range of the port-channel ID is 1 to 64.

Mode Privileged EXEC

Display Message

Fields	Definition
Interface	Indicates by slot id and port number which is the port controlled by the fields on this line.

Port VLAN ID	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.
Default Priority	The 802.1p priority assigned to untagged packets arriving on the port.
Admin. Native VLAN	The administrative 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.
Oper. Native VLAN	The operational 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.
Mode	Indicates this interface is operating on Access mode, General mode, Trunk mode, Private Vlan Host mode and Private Vlan Promiscuous mode.
Ingress Filtering	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.
Acceptable Frame Types	Specifies 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.
VLAN ID	Displays the VLAN of which the interface is a member. (Display in administration and operation two statuses)
VLAN Name	Displays the name of the VLAN of which the interface is a member. (Display in administration and operation twstatuses)
VLAN Type	Displays the type of the VLAN of which the interface is a member. (Display in administration and operation statuses)
Egress rule	Indicate the port will untag or tag frame when sending frames in that specific VLAN. (Display in administration and operation statuses)

5.2.1.10. 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 [<0-7>]

Parameter	Definition
<0-7>	Specifies the tunnel ID

Mode Privileged EXEC

Display Message

Fields	Definition
TunnelId	Shows the tunnel identification number.
Interface	Shows the name of the tunnel interface..
Tunnel Mode	Shows the tunnel mode .
Source Address	Shows the source transport address of the tunnel
Destination Address	Shows the destination transport address of the tunnel
Routing Mode	Shows whether the routing is enabled or disabled.
Administrative Mode	Shows whether the interface administrative mode is enabled or disabled.
IPv6 Implicit Mode	Shows whether the Implicit mode is enabled, which enables the interface being capable of ipv6 operation without a global address.
IPv6 Operational Mode	Shows whether the operational state of an interface is enabled or disabled.
Interface Maximum Transmit Unit	Shows the maximum transmission unit for packets on the interface, in bytes.
Router Duplicate Address Detection Transmits	Shows the number of consecutive duplicate address detection probes to transmit.
Router Advertisement NS Interval	Shows 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	Shows the amount of time, in milliseconds, to consider a neighbor reachable after neighbor discovery confirmation.

Router Advertisement Interval (max)	Shows maximum time allowed between sending router advertisements from the interface. Range of maximum advertisement interval is (4 to 1800).Default value is 600.
Router Advertisement Interval (min)	Shows minimum time allowed between sending router advertisements from the interface. Range of minimum advertisement interval is (3 to 1350).Default value is 200.
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 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)

5.2.1.11. show interface description

This command displays the interface description.

Format show interface description [{<slot/port> | loopback <loopback-id> | port-channel <portchannel-id> | tunnel <tunnel-id> | vlan <vlan-id>}]

Mode Privileged EXEC

Display Message

Parameter	Definition
Interface	The slot/port or LAG with the information to view.
Description	The alpha-numeric description of the interface created by the **description** command.

Example: The following example shows the CLI display output for the command **show interface description 0/1**.

```
(M4500-32C) #show interface description 0/1

Interface               0/1
Description
```

5.2.1.12. show interface fec

This command displays forward error correction information for the interface.

Format show interface fec [<slot/port>]

Parameter	Definition
no parameter	To display information for all ports.
<slot/port>	Specifies Interface number

Mode Privileged EXEC

5.2.1.13. show interface advertise

Use this command to display the advertisement information for interfaces.

Format show interface advertise [<slot/port>]

Parameter	Definition
no parameter	Displays information for all ports.
<slot/port>	The interface number for which information is displayed.

Mode Privileged Exec

Example:

```
(M4500-48XF8C) # show interface advertise

Intf     Neg      Operational Link Advertisement

--------  --------  ------------------------------------

0/1      Enabled   25000f

0/2      Enabled   25000f

0/3      Enabled   25000f

0/4      Enabled   25000f

0/5      Disabled  -     -     -     -     -     -

0/6      Disabled  -     -     -     -     -     -

0/7      Disabled  -     -     -     -     -     -

0/8      Disabled  -     -     -     -     -     -

0/9      Disabled  -     -     -     -     -     -

0/10     Disabled  -     -     -     -     -     -

0/11     Disabled  -     -     -     -     -     -
```

```
0/12     Disabled  -     -     -     -     -     -
```

```
(M4500-48XF8C) #show interface advertise 0/1

Port: 0/1

Link State: Up

Auto Negotiation:Enabled

Clock:Slave

                              100000f 50000f 40000f 25000f 10000f 1000f

                              ------- ------ ------ ------ ------ ------

Admin Local link Advertisement    no     no     no     yes    no     no

Oper Local link Advertisement     no     no     no     yes    no     no

Oper Peer Advertisement           no     no     no     yes    no     no

Priority Resolution               no     no     no     yes    no     no
```

5.2.1.14. show fiber-ports optics commands

5.2.1.14.1. show fiber-port optics

Use this command to display the diagnostics information about the modules that are installed in all SFP ports or a module in a specific SFP port.

Format show fiber-ports optics [all | <slot/port>]

Parameter	Definition
all	Displays information for all ports.
<slot/port>	The interface number for which information is displayed.

Mode Privileged Exec

5.2.1.14.2. show fiber-port optics-diag

Use this command to display the raw data of the diagnostics information about the modules that are installed in all SFP ports or a module in a specific SFP port.

Format show fiber-ports optics-diag [all | <slot/port>]

Parameter	Definition
all	Displays information for all ports.
<slot/port>	The interface number for which information is displayed.

Mode Privileged Exec

5.2.1.14.3. show fiber-port optics-eeprom

Use this command to display information about the Electrically Erasable Programmable Read-Only Memory (EEPROM) of the modules that are installed in all SFP ports or a module in a specific SFP port.

Format show fiber-ports optics-eeprom [all | <slot/port>]

Parameter	Definition
all	Displays information for all ports.
<slot/port>	The interface number for which information is displayed.

Mode Privileged Exec

5.2.1.14.4. show fiber-port optics-info

Use this command to display information about the SFP vendor or vendors of the modules that are installed in all SFP ports or a module in a specific SFP port.

Format show fiber-ports optics-info [all | <slot/port>]

Parameter	Definition
all	Displays information for all ports.
<slot/port>	The interface number for which information is displayed.

Mode Privileged Exec

5.2.1.15. Interface configuraton commands

5.2.1.15.1. interface

This command is used to enter Interface configuration mode.

Format interface {<slot/port> | control-plane | loopback <0-63> | port-channel <1-64> | range <intf-range>| tunnel <0-7> | vlan <1-4093> | vxlan <1-1>}

Parameter	Definition
<slot/port>	Enter into interface mode
control-plane	Enter into Control Plane Mode
loopback <0-63>	Configuration of Loopback Interface
port-channel <1-64>	Enter into interface port-channel mode.
Range <intf-range>	Enter into interface range mode.Specifies the interface(s) in slot/port format, use comma for a list and hyphen for ranges.
tunnel <0-7>	Configure IPv6 Tunnel.
vlan <1-4093>	Enter into interface VLAN mode.
vxlan <1-1>	Enter into VxLAN Mode.

Mode Global Config

5.2.1.15.2. description

This command is used to create an alpha-numeric description of the port.

Format description <description>

Parameter	Definition
<description>	an alpha-numeric description

Default None

Mode Interface Config

5.2.1.15.3. no description

This command removes the description of the interface.

Format no description

Mode Interface Config

5.2.1.15.4. flowcontrol

This command enables 802.3x flow control for the interface(s).

Format flowcontrol {asymmetric | symmetric}

Parameter	Definition
asymmetric	Indicates to enable an asymmetric flow control
symmetric	Indicates to enable a symmetric flow control

Default Disabled

Mode Global Config
Interface Config

5.2.1.15.5. no flowcontrol

This command removes the flow control feature from the interface(s).

Format no flowcontrol

Mode Global Config, Interface Config

5.2.1.15.6. 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 ICOS implementation, the MTU size is a valid integer between 1522 and 9412 for tagged packets and a valid integer between 1518 and 9412 for untagged packets.

Format mtu <1518-9412>

Default 1518

Mode Interface Config

5.2.1.15.7. no mtu

This command sets the default MTU size (in bytes) for the interface.

Format no mtu

Mode Interface Config

5.2.1.15.8. port-mode

Use this command to configure a 100G QSFP28 port in either 1x100G, 1x40G, 2x50G, 4x25G, or 4x10G mode or four 25G SFP28 ports in either 4x25G, 4x10G, or 4x1G mode.

Note: In model M4500-48XF8C, every four 25G ports form a group from port 1 until port 48. The *port-mode* command can only be applied on the first port of each group and all the four ports in the same group are configured to the same speed. For example, you can issue the *port-mode 4x1G* command on ethernet port 0/1 but not on ethernet port 0/2, 0/3, or 0/4; all the four ports from 0/1 to 0/4 are configured to 1G.

Format port-mode {1x100G | 1x40G | 2x50G | 4x25G | 4x10G | 4x1G}

Parameter	Definition
1x100G	Configure the port as a single 100G port using four lanes.
1x40G	Configure the port as a single 40G port using four lanes.
2x50G	Configure the port as two 50G ports, each on two lanes.
4x25G	Configure the port as four 25G ports, each on a separate lane. This mode requires the use of a suitable 4x25G to 1x100G pigtail cable.
4x10G	Configure the port as a four 10G ports, each on a separate lane. This mode requires the use of a suitable 4x10G to 1x40G pigtail cable.
4x1G	Configure the port as a four 1G ports, each on a separate lane.

Default 100G for 100G ports
10G for 25G ports

Mode Interface Config

5.2.1.15.9. no port-mode

This command resets to the default value. The default value is 100G for 100G ports and 10G for 25G ports.

Format no port-mode

Mode Interface Config

5.2.1.15.10. shutdown

This command is used to disable a port.

The no command is used to enables a port.

Format [no] shutdown

Parameter	Definition
no.	Reset to default.

Default Enable

Mode Interface Config

5.2.1.15.11. shutdown all

This command is used to disable all ports.

Format [no] shutdown all

Parameter	Definition
no.	Reset to default.

Mode Global Config

5.2.1.15.12. fec

Enable forward error correction on the interface.

Note:
1. Different type of FEC should be applied on different speed. FEC CL74 is applied on 25G/50G interface, FEC CL91 is applied on 100G/50G interface, and FEC CL108 is applied on 25G interface.
2. FEC enable/disable is applied to the first interface of each group, which works in the same way as the command *port-mode*. For example, you can issue the *fec CL108* command on ethernet port 0/1 but not on ethernet port 0/2, 0/3, or 0/4; all the four ports from 0/1 to 0/4 are configured to CL108. For the 50G ports, such as 0/161 and 0/162 on M4500-32C model, you can issue the *fec CL91* command on ethernet port 0/161 but not on ethernet port 0/162; both ports, 0/161 and 0/162, are configured to CL91.

Format fec {CL74 | CL91 | CL108}

Parameter	Definition
CL74	Enable CL74/Base-R FEC .

CL91	Enable CL91/RS FEC .
CL108	Enable Enable RS108 FEC .

Default Enable

Mode Interface Config

5.2.1.15.13. negotiate

Use this command to enable auto-negotiation on a specific port. Auto-negotiation is supported on 100G/40G/25G ports with DAC cables. AOC cables and 50G/10G/1G ports do not support auto-negotiation.

Note:

- Auto-negotiation is applied to the first interface of each group, which works in the same way as the **port-mode** and **fec** commands. For example, you can issue the **negotiate** command on Ethernet port 0/1 but not on Ethernet port 0/2, 0/3, or 0/4. However, if you issue the **negotiate** command on Ethernet port 0/1, all four ports from 0/1 to 0/4 are configured for auto-negotiation.
- If you enable auto-negotiation on SFP28 ports, the advertisement of FEC is CL108. On QSFP28 ports, it is CL91.

Format negotiate

no negotiate

Default Enabled

Mode Interface Config

5.2.1.16. show port status all

This command displays the status of all ports.

Format show port status all

Mode Privileged EXEC

Display Message

Example: The following example shows the CLI display output for the command *show port status all*.

```
(M4500-32C) #show port status all

        Media        STP     Physical    Physical    Link      Loop     Partner Flow
Intf    Type         Mode    Mode        Status      Status    Status   Control
------  -----------  ------  ----------  ----------  --------  -------- ------------
0/1      DAC          FWD     25G Full    25G Full    Up                 NA
0/2      DAC          BLK     25G Full    25G Full    Up       Loop      NA
```

```
0/3                    DIS     25G Full                Down                NA
0/4                    DIS     25G Full                Down                NA
0/5      10GBase-SR    FWD     10G Full    10G Full    Up                  NA
0/6      10GBase-SR    FWD     10G Full    10G Full    Up                  NA

0/49     40GBase-SR4   FWD     40G Full    40G Full    Up                  NA
0/50     40GBase-SR4   BLK     40G Full    40G Full    Up        Loop      NA
```

5.2.1.17. 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

Mode Privileged EXEC

Display Message

Fields	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 examples of 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
```

5.2.2. Show BMC Commands

5.2.2.1. show bmc

Use this command to display the information for BMC.

Format show bmc

Mode Privileged Exec

Display Message

Fields	Definition
BMC Version	BMC Version
BMC IP Protocol	IP address protocol: DHCP or Static
BMC IP Address	BMC IP address
BMC Subnet Mask	BMC subnet mask
BMC Default Gateway	IP address of default gateway
BMC MAC Address	BMC MAC address
BMC Watchdog Status	Watchdog is Started/Running or Stopped
BMC Watchdog Actions	The action to be taken when Watchdog detects a device abnormality.

BMC Watchdog Timeout	True when Watchdog detects no response from device, else it's False.
BMC Watchdog Config Time	User configured Watchdog timeout (unit: seconds)
BMC Watchdog Present Time	Remained time to take Watchdog Actions (unit: seconds).

Example:

```
(M4500-48XF8C) # show bmc
BMC Version..................................... 3.06.00

BMC IP Protocol................................. DHCP

BMC IP Address.................................. 172.20.0.71

BMC Subnet Mask................................. 255.255.0.0

BMC Default Gateway............................. 172.20.255.254

BMC MAC Address................................. bc:a5:11:b4:87:cb

BMC Watchdog Status............................. Stopped

BMC Watchdog Actions............................ Hard Reset

BMC Watchdog Timeout............................ False

BMC Watchdog Config Time (sec).................. 60

BMC Watchdog Present Time (sec)................. 60


BMC User List

------------------------

qct.admin
```

5.2.2.2. bmc account password

Use this command to change the password of the specific account for BMC. The password must be in plain text between 8 and 16 characters. The text that you type is displayed in asterisk characters.

Format bmc account <username> password

Default The same as the user name of the account

Mode Global Config

5.2.2.3. bmc ip

Use this command to set a static IP address for BMC or change its IP protocol to DHCP.

Format bmc ip {dhcp | static <ipaddr> <netmask> <gateway>}

Default bmc ip dhcp

Mode Global Config

5.2.2.4. bmc watchdog

Use this command to start or stop the BMC watchdog or to modify the watchdog timer for time-out detection.

If you enable the watchdog, NOS resets the countdown timer each fifth of the time that is set for the watchdog configuration time. For example, if the watchdog configuration time is 60 seconds, the countdown timer reset each 20 seconds.

Format bmc watchdog [timer <10-600>]

no bmc watchdog [timer]

Default The watchdog is disabled. If enabled, the default time is 60 seconds.

Mode Global Config

5.2.3. L2 MAC Address and Multicast Forwarding Database Tables

5.2.3.1. show mac-addr-table

This command displays the forwarding database entries. If the command is entered with no parameter, the entire table is displayed. The administrator can enter a MAC Address to display the table entry for the requested MAC address and all entries following the requested MAC address.

Format show mac-addr-table [{<macaddr> <vlan-id>}]

Default None

Mode Privileged EXEC

Example: The following example shows the CLI display output for the command *show mac-addr-table*.

```
(M4500-32C) #show mac-addr-table

VLAN ID  MAC Address         Interface              IfIndex  Status

-------  ------------------  ---------------------  -------  ------------

1         BC:A5:11:56:D3:57   vlan 1                  136      Management
```

5.2.3.2. show mac-addr-table count

This command displays the total forwarding database entries, the number of static and learnning mac address, and the max address available on the switch.

Format show mac-addr-table count

Default None

Mode Privileged EXEC

Example: The following example shows the CLI display output for the command *show mac-addr-table count*.

```
(M4500-32C) #show mac-addr-table count

Dynamic Address count..... 0

Static Address (User-defined) count..... 1

Total MAC Addresses in use..... 1

Total MAC Addresses available..... 98304
```

5.2.3.3. show mac-addr-table interface

This command displays the forwarding database entries. The user can search FDB table by using specific interface number.

Format show mac-addr-table interface {<slot/port> | port-channel <portchannel-id> | vlan <vlan-id>}

Mode Privileged EXEC

Example: The following example shows the CLI display output for the command **show mac-addr-table vlan 1**.

```
(M4500-32C) #show mac-addr-table interface vlan 1

MAC Address        VLAN ID            Status

-----------------  -----------------  -----------------

BC:A5:11:56:D3:57  1                  Management
```

5.2.3.4. show mac-address-table igmpsnooping

This command displays the IGMP Snooping entries in the Multicast Forwarding Database (MFDB) table.

Format show mac-address-table igmpsnooping

Mode Privileged EXEC

Example: The following example shows the CLI display output for the command *show mac-address-table igmpsnooping.*

```
(M4500-32C) (Config)#show mac-address-table igmpsnooping

VLAN ID  MAC Address     Type     Description       Interfaces

-----------------------  -------  ----------------  -------------------------

00:01:01:00:5E:01:01:01  Static   Network Assist    Fwd: 0/1,ch1

00:02:01:00:5E:AA:BB:CC  Static   Network Assist    Fwd: 0/2
```

5.2.3.5. show mac-address-table multicast

This command displays the MFDB information. If the command is entered with no parameter, the entire table is displayed. This is the same as entering the all parameter. The user 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

Example: The following example shows the CLI display output for the command *show mac-address-table multicast.*

```
(M4500-32C) (Config)#show mac-address-table multicast

                                                                    Fwd

VLAN ID MAC Address       Source  Type    Description     Interface Interface

------- ----------------- ------- ------- --------------- --------- ---------

1       01:00:5E:01:01:01 IGMP    Static  Network Assist  Fwd:      Fwd:

                                                          0/1,      0/1,

                                                          ch1       ch1

2       01:00:5E:AA:BB:CC IGMP    Static  Network Assist  Fwd:      Fwd:

                                                          0/2       0/2
```

5.2.3.6. show mac-address-table status

This command displays the MFDB statistics.

Format show mac-address-table stats

Mode Privileged EXEC

Example: The following example shows the CLI display output for the command *show mac-address-table stats.*

```
(M4500-32C) #show mac-address-table stats

Max MFDB Table Entries..... 1024

Most MFDB Entries Since Last Reset..... 0

Current Entries..... 0
```

5.2.3.7. show mac-addr-table agetime

This command displays the forwarding database address aging timeout.

Format show mac-addr-table agetime

Mode Privileged EXEC

Example: The following example shows the CLI display output for the command *show mac-addr-table agetime.*

(M4500-32C) #show mac-addr-table agetime

Address Aging Timeout:300

5.2.3.8. mac-addr-table aging-time

This command configures the forwarding database address aging timeout in seconds.

Format mac-addr-table aging-time <10-1000000>

Default 300s

Mode Global Config

5.2.3.9. no mac-addr-table aging-time

Use this command to return the address aging timeout the default settings.

Format no mac-addr-table aging-time

Mode Global Config

5.2.3.10. clear mac-addr-table dynamic

This command clears dynamic MAC entries.

Format clear mac-addr-table dynamic

Default None

Mode Privileged Exec

5.2.4. VLAN Commands

This section describes the commands you use to configure VLAN settings.

5.2.4.1. vlan database

This command gives you access to the VLAN Config mode, which allows you to configure VLAN characteristics.

Format vlan database

Mode Global Config

5.2.4.2. 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 <vlan-list>

Mode VLAN Config

5.2.4.3. 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 <vlan-list>

Mode VLAN Config

5.2.4.4. 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 2-4093.

Format vlan makestatic <2-4093>

Mode VLAN Config

5.2.4.5. 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.

Format vlan name <1-4093> <newname>

Default VLAN ID 1 - default
Other VLANS - blank string

Mode VLAN Config

5.2.4.6. no vlan name

This command sets the name of a VLAN to a blank string.

Format no vlan name <1-4093>

Mode VLAN Config

5.2.4.7. switchport acceptable-frame-types

This command sets the frame acceptance mode per interface. 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. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN specification.

Format switchport acceptable-frame-types {all | tagged | untagged}

Default all

Mode Interface Config

5.2.4.8. no switchport acceptable-frame-types

This command resets the frame acceptance mode for the interface to the default value.

Format no switchport acceptable-frame-types

Mode Interface Config

5.2.4.9. switchport acceptbale-frame-type all

This command sets the frame acceptance mode for all 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. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN specification.

Format switchport acceptable-frame-types all {all | tagged | untagged}

Default all

Mode Global Config

5.2.4.10. no switchport acceptable-frame-types all

This command resets the frame acceptance mode for all interfaces to the default value.

Format no switchport acceptable-frame-types all

Mode Global Config

5.2.4.11. switchport ingress-filtering

This command enables 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 switchport ingress-filtering

Default disabled

Mode Interface Config

5.2.4.12. no switchport ingress-filtering

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 switchport ingress-filtering

Mode Interface Config

5.2.4.13. switchport ingress-filtering all

This command enables ingress filtering for all 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.

Format switchport ingress-filtering all

Default disabled

Mode Global Config

5.2.4.14. no switchport ingress-filtering all

This command disables ingress filtering for all 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.

Format no switchport ingress-filtering all

Mode Global Config

5.2.4.15. switchport native vlan

This command changes the VLAN ID which will be assigned to untagged or priority tagged frames per interface.

Format switchport native vlan <1-4093>

Default 1

Mode Interface Config

5.2.4.16. no switchport native vlan

This command sets the VLAN ID per interface to 1.

Format no switchport native vlan

Mode Interface Config

5.2.4.17. switchport native vlan all

This command changes the VLAN ID which will be assigned to untagged or priority tagged frames for all interfaces.

Format switchport native vlan all <1-4093>

Default 1

Mode Global Config

5.2.4.18. no switchport native vlan all

This command sets the VLAN ID for all interfaces to 1.

Format no switchport native vlan all

Mode Global Config

5.2.4.19. switchport allowed vlan

This command configures the degree of participation for a specific interface in a VLAN. The ID is a valid VLAN identification number, and the interface is a valid interface number.

Format switchport allowed vlan {add [tagged | untagged] | remove} <vlan-list>

Mode Interface Config

5.2.4.20. switchport allowed vlan all

This command configures the degree of participation for all interfaces in a VLAN. The ID is a valid VLAN identification number.

Format switchport allowed vlan {add {tagged | untagged} | remove} all <1-4093>

Mode Global Config

5.2.4.21. switchport tagging

This command configures the tagging behavior for a specific interface in a VLAN to enable. 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 switchport tagging <vlan-list>

Default Disable

Mode Interface Config

5.2.4.22. no switchport tagging

This command configures the tagging behavior for a specific interface 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 switchport tagging <vlan-list>

Mode Interface Config

5.2.4.23. switchport tagging all

This command configures the tagging behavior for all interfaces in a VLAN to be 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 switchport tagging all <1-4093>

Default Disable

Mode Global Config

5.2.4.24. no switchport 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 switchport tagging all <1-4093>

Mode Global Config

5.2.4.25. show vlan

This command displays brief information on a list of all configured VLANs.

Format show vlan

Mode Privileged EXEC

User EXEC

Display Message

Term	Definition
VLAN ID	There is a VLAN Identifier (vlanid) associated with each VLAN. The range of the VLAN ID is 1 to 4093.
VLAN Name	A string associated with this VLAN as a convenience. It can be up to 16 alphanumeric characters, including blanks. The default is blank. VLAN ID 1 is always named `Default`. This field is optional.
VLAN Type	Type of VLAN, which can be Default, (VLAN ID = 1), can be static (one that is configured and permanently defined), or Dynamic (one that is created by GVRP registration).
Interface(s)	Indicates by slot id and port number which port belongs to this VLAN.

5.2.4.26. show vlan id

This command displays detailed information, including interface information, for a specific VLAN.

Format show vlan {id <1-4093> | name <vlanname>}

Mode Privileged EXEC

User EXEC

Display Message

Term	Definition
VLAN ID	There is a VLAN Identifier (VID) associated with each VLAN. The range of the VLAN ID is 1 to 4093.
VLAN Name	A string associated with this VLAN as a convenience. It can be up to 32 alphanumeric characters, including blanks. The default is blank. VLAN ID 1 is always named `Default`. This field is optional.

VLAN Type	Type of VLAN, which can be Default, (VLAN ID = 1), can be static (one that is configured and permanently defined), or Dynamic (one that is created by GVRP registration).
Interface	Indicates by slot id and port number which port is controlled by the fields on this line.
Current: • **Include** • **Exclude** • **Autodetect**	Determines the degree of participation of this port in this VLAN. The permissible values are: • This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard. • This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. • Specifies 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: • **Include** • **Exclude** • **Autodetect**	Determines the configured degree of participation of this port in this VLAN. The permissible values are: • This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard. • This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. • Specifies 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: • **Tagged** • **Untagged**	Select the tagging behavior for this port in this VLAN: • Specifies to transmit traffic for this VLAN as tagged frames. • Specifies to transmit traffic for this VLAN as untagged frames.

5.2.4.27. 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

Display Message

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.

5.2.4.28. show interface switchport

This command displays VLAN port information.

Format show interface switchport {<slot/port> | port-channel <1-64>}

Mode Privileged EXEC
User EXEC

Display Message

Term	Definition
Interface	Indicates by slot id and port number which port is controlled by the fields on this line. It is possible to set the parameters for all ports by using the selectors on the top line.
Native VLAN	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.
Mode	Indicates this interface is operating on Access mode or General mode.
Ingress Filtering	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.

Term	Definition
Acceptable Frame Type	Specifies 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.

5.2.4.29. show vlan private-vlan

This command displays private vlan information.

Format show vlan private-vlan [type]

Mode Privileged Exec

5.2.4.30. show vlan remote-span

This command displays remote-span information.

Format **s**how vlan private-vlan

Mode Privileged Exec

5.2.5. 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.

5.2.5.1. 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>}

Parameter	Definition
host-association	Defines the VLAN association for community or host ports.
mapping	Defines the private VLAN mapping for promiscuous ports.
primary-vlan-id	Primary VLAN ID of a private VLAN.
secondary-vlanid	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-vlanlist	A list of secondary VLANs to be mapped to a primary VLAN.

Mode Interface Config

5.2.5.2. no switchport private-vlan

This command removes the private-VLAN association or mapping from the port.

Format no switchport private-vlan {host-association|mapping}

Mode Interface Config

5.2.5.3. 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.

Format switchport mode private-vlan {host|promiscuous}

Parameter	Definition
host	Configures an interface as a private VLAN host port. It can be either 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.

Default general

Mode Interface Config

5.2.5.4. 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

5.2.5.5. 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-vlanlist> | community | isolated | primary}

Parameter	Definition
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.

Mode VLAN Config

5.2.5.6. no private-vlan

This command restores normal VLAN configuration.

Format no private-vlan [association]

Mode VLAN Config

5.2.6. Switch Ports

This section describes the commands used for switch port mode.

5.2.6.1. switchport mode

This command configures an interface to be operated on VLAN access mode. In this mode, only one VLAN could be assigned to this interface. Use 'switchport access vlan <vlan-id>' to configure the access VLAN. In VLAN access mode, only the untagged packets are handled.

Format switchport mode <access | general | trunk>

Default General Mode

Mode Interface Config

5.2.6.2. no switchport mode

This command sets the mode to General.

Format no switchport mode

Mode Interface Config

5.2.6.3. 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 choosen, 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.

Format switchport trunk allowed vlan {<vlan-list> | all | add <vlan-list> | remove <vlan-list> | except <vlan-list>}

Parameter	Definition
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 XY 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.

Default All

Mode Interface Config

5.2.6.4. 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

5.2.6.5. 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.

Format switchport trunk native vlan <vlan-id>

Default 1 (Default VLAN)

Mode Interface Config

5.2.6.6. 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

5.2.6.7. 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.

Format switchport access vlan <vlan-id>

Default 1 (Default VLAN)

Mode Interface Config

5.2.6.8. no switchport access vlan

This command sets the access VLAN ID to 1.

Format no switchport access vlan

Mode Interface Config

5.2.6.9. show interfaces switchport

Use this command to display the switchport status for all interfaces or a specified interface.

Format show interfaces switchport [<slot/port> | port-channel <trunk-id>]

Mode Privileged EXEC

5.2.7. 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.

5.2.7.1. dvlan-tunnel ethertype

This command configures the ethertype for the all interfaces. 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.

Format dvlan-tunnel ethertype {802.1Q | vman | custom <1–65535>}

Parameter	Definition
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.

Mode Global Config

5.2.7.2. no dvlan-tunnel ethertype

Use the no form of the command to disassociate globally defined TPID(s) to all interfaces.

Format no dvlan-tunnel ethertype

Mode Global Config

5.2.7.3. dot1q-tunnel ethertype

This command configures the ethertype for the all interfaces. 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.

Format dot1q-tunnel ethertype {802.1Q | vman | custom <1–65535>}

Mode Global Config

5.2.7.4. no dot1q-tunnel ethertype

Use the no form of the command to disassociate globally defined TPID(s) to all interfaces.

Format no dot1q-tunnel ethertype

Mode Global Config

5.2.7.5. mode dot1q-tunnel

This command is used to enable Double VLAN Tunneling on the specified interface.

Format mode dot1q-tunnel

Default disabled

Mode Interface Config

5.2.7.6. 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

5.2.7.7. 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.

Format mode dvlan-tunnel

Default disabled

Mode Interface Config

5.2.7.8. 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

5.2.7.9. show dot1q-tunnel

Use this command with the optional parameter interface 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.

Format show dot1q-tunnel [interface [{<slot/port> | port-channel <port-channel-id >}]]

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.

Mode Privileged EXEC

User EXEC

Example: The following shows examples of the CLI display output for the commands *show dot1q-tunnel*.

```
(M4500-32C) #show dot1q-tunnel


Ethertype..................................... 0x8100

Interfaces Enabled for DVLAN Tunneling......... None


(M4500-32C) #show dvlan-tunnel interface port-channel 1

Interface     Mode           EtherType
------------  ------------   ---------------
ch1           Disable        0x8100
```

5.2.7.10. show dvlan-tunnel

Use this command with the optional parameter interface 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.

Format show dvlan-tunnel [interface [{<slot/port> | port-channel <portchannel-id >}]]

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.

Mode Privileged EXEC

User EXEC

Example: The following shows examples of the CLI display output for the commands *show dvlan-tunnel*.

```
(M4500-32C) #show dvlan-tunnel

Ethertype..................................... 0x8100

Interfaces Enabled for DVLAN Tunneling......... None


(M4500-32C) #show dvlan-tunnel interface port-channel 1


Interface      Mode          EtherType
-------------  ------------  ---------------
ch1            Disable       0x8100
```

5.2.8. IGMP snooping commands

This section describes the commands which are used to configure IGMP Snooping.

IGMP snooping is designed to prevent flooding multicast traffic which can cause unnecessary load on host devices.

Note: IGMP Snooping can be enabled with MLAG. The configuration of IGMP Snooping on peers of MLAG must be the same to guarantee that MLAG can work correctly.

5.2.8.1. ip igmp snooping

Use this command to enable IGMP snooping globally.

Format ip igmp snooping

Default Disable

Mode Global Config

5.2.8.2. no ip igmp snooping

Use this command to disable IGMP snooping globally.

Format no ip igmp snooping

Mode Global Config

5.2.8.3. clear igmp snooping

Use this command to delete all dynamic entries in Multicast Forwarding Database which is managed by the IGMP Snooping.

Format clear igmp snooping

Default None

Mode Privileged Exec

5.2.8.4. ip igmp snooping interfacemode

Use this command to enable IGMP snooping on one particular interface.

Format ip igmp snooping interfacemode

Default Disable

Mode Interface Config

5.2.8.5. no ip igmp snooping interfacemode

Use this command to disable IGMP snooping on one particular interface.

Format no ip igmp snooping interfacemode

Mode Interface Config

5.2.8.6. ip igmp snooping interfacemode all

Use this command to enable IGMP snooping on all interfaces.

Format ip igmp snooping interfacemode all

Default Disable

Mode Global Config

5.2.8.7. no ip igmp snooping interfacemode all

Use this command to disable IGMP snooping on all interfaces.

Format no ip igmp snooping interfacemode all

Mode Global Config

5.2.8.8. ip igmp snooping fast-leave

Use this command to enable IGMP snooping fast-leave admin mode on one particular interface or all interfaces.

Format ip igmp snooping fast-leave

Default Disable

Mode Global Config
Interface Config

5.2.8.9. no ip igmp snooping fast-leave

Use this command to disable IGMP snooping fast-leave admin mode on one particular interface or all interfaces.

Format no ip igmp snooping fast-leave

Mode Global Config
Interface Config

5.2.8.10. ip igmp snooping groupmembershipinterval

Use this command to configure IGMP Group Membership Interval time on one particular interface or all interfaces.

Format ip igmp snooping groupmembershipinterval <2-3600>

Default 600 seconds

Mode Global Config
Interface Config

5.2.8.11. no ip igmp snooping groupmembershipinterval

Use this command to restore IGMP Group Membership Interval time to default value.

Format no ip igmp snooping groupmembershipinterval

Mode Global Config
Interface Config

5.2.8.12. ip igmp snooping mcrtrexpiretime

Use this command to configure Multicast Router Present Expiration time globally or on one particular interface.

Format ip igmp snooping mcrtrexpiretime <0-3600>

Default 300 seconds

Mode Global Config
Interface Config

5.2.8.13. no ip igmp snooping mcrtrexpiretime

Use this command to restore Multicast Router Present Expiration time to default value.

Format no ip igmp snooping mcrtrexpiretime

Mode Global Config
Interface Config

5.2.8.14. ip igmp snooping mrouter

Use this command to configure one particular interface as a multicast router-attached interface or configure the VLAN ID for the VLAN that has the multicast router attached mode enabled.

Format ip igmp snooping mrouter {interface | <vlan-id>}

Default Disable

Mode Interface Config

5.2.8.15. no ip igmp snooping mrouter

Use this command to disable multicast router attached mode for one particular interface or a VLAN.

Format no ip igmp snooping mrouter {interface | <vlan-id>}

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode Interface Config

5.2.8.16. set igmp

Use this command to enable IGMP Snooping on a particular VLAN.

Format set igmp <vlan-id>

Default Disable

Mode VLAN database

5.2.8.17. no set igmp

Use this command to disable IGMP Snooping on a particular VLAN.

Format no set igmp <vlan-id>

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode VLAN database

5.2.8.18. set igmp fast-leave

Use this command to enable IGMP Snooping fast-leave admin mode on a particular VLAN.

Format set igmp fast-leave <vlan-id>

Default Disable

Mode VLAN database

5.2.8.19. no set igmp fast-leave

Use this command to disable IGMP Snooping fast-leave admin mode on a particular VLAN.

Format no set igmp fast-leave <vlan-id>

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode VLAN database

5.2.8.20. set igmp groupmembership-interval

Use this command to configure IGMP Group Membership Interval time on a particular VLAN.

Format set igmp groupmembership-interval <vlan-id> <2-3600>

Default 600 seconds

Mode VLAN database

5.2.8.21. no set igmp groupmembership-interval

Use this command to restore IGMP Group Membership Interval time on a particular VLAN to default value.

Format no set igmp groupmembership-interval <vlan-id>

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode VLAN database

5.2.8.22. set igmp maxresponse

Use this command to configure IGMP Maximum Response time on a particular VLAN when the **igmp-plus** command is not enabled.

Format set igmp maxresponse <vlan-id> <1-300>

Default 120

Mode VLAN database

5.2.8.23. no set igmp maxresponse

Use this command to restore IGMP Maximum Response time on a particular VLAN to default value.

Format no set igmp maxresponse <vlan-id>

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode VLAN database

5.2.8.24. set igmp mcrtrexpiretime

Use this command to configure Multicast Router Present Expiration time on a particular VLAN.

Format set igmp mcrtrexpiretime <vlan-id> <0-3600>

Default 300

Mode VLAN database

5.2.8.25. no set igmp mcrtrexpiretime

Use this command to restore Multicast Router Present Expiration time on a particular VLAN to default value.

Format no set igmp mcrtrexpiretime <vlan-id>

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode VLAN database

5.2.8.26. set igmp report-suppression

Use this command to enable Report Suppression one a particular VLAN.

Format set igmp report-suppression <vlan-id>

Default Disable

Mode VLAN database

5.2.8.27. no set igmp report-suppression

Use this command to disable Report Suppression on a particular VLAN.

Format no set igmp report-suppression <vlan-id>

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode VLAN database

5.2.8.28. set snoop-vlan-block

Use this command to enable Snooping Vlan Block mode for a list of VLAN.

Format set snoop-vlan-block <vlan-list>

Default None

Mode VLAN database

5.2.8.29. no set snoop-vlan-block

Use this command to disable Snooping Vlan Block mode for a list of VLAN.

Format no set snoop-vlan-block <vlan-list>

Parameter	Description
vlan-list	The VLANs which apply this command.

Mode VLAN database

5.2.8.30. ip igmp snooping static

Use this command to add an interface to a multicast group.

Format ip igmp snooping static <macaddr> vlan <vlan-id> [interface {<slot/port> | port-channel <portchannel-id>}]

Default None

Mode Global Config

5.2.8.31. no ip igmp snooping static

Use this command to remove an interface from a multicast group.

Format no ip igmp snooping static <macaddr> vlan <vlan-id> interface {<slot/port> | port-channel <portchannel-id>}

Parameter	Description
vlan-id	The VLAN ID. (Range: 1-4093)
macaddr	Multicast Group MAC address
slot/port	Interface number
portchannel-id	Port-channel interface number. The range of port-channel ID is 1 to 64.

Mode Global Config

5.2.8.32. ip igmp snooping router-alert-check

Use this command to enable Router-Alert validation for IGMP packets.

Format ip igmp snooping router-alert-check

Default Disable

Mode Global Config

5.2.8.33. no ip igmp snooping router-alert-check

Use this command to disable Router-Alert validation for IGMP packets.

Format no ip igmp snooping router-alert-check

Mode Global Config

5.2.8.34. show ip igmp snooping

Use this command to display IGMP snooping information.

Format show ip igmp snooping [interface {<slot/port> | vlan <vlan-id> | port-channel <portchannel-id>}]

Parameter	Description
vlan-id	The VLAN ID. (Range: 1-4093)
slot/port	Interface number
portchannel-id	Port-channel interface number. The range of port-channel ID is 1 to 64.

Mode Privilege Exec

Display Message

If no parameters are specified, this command displays the following information:

Term	Definition
Admin Mode	Indicates whether or not IGMP Snooping is enabled on the switch.
Operation Mode	Indicates whether or not IGMP Snooping is active on the switch.
Multicast Control Frame Count	Displays the number of IGMP Control frames that are processed by the CPU.
IGMP Snooping Router-Alert check	Indicates whether or not Router-Alert Validation is active on the switch.
Interfaces Enabled for IGMP Snooping	Interfaces on which IGMP Snooping is enabled.
VLANs enabled for IGMP snooping	VLANs on which IGMP Snooping is enabled.
VLANs Block enabled for snooping	VLANs on which IGMP Snooping is disabled.

If parameter <slot/port> or <portchannel-id> is specified, the following information is displayed:

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	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 on the interface, before deleting the interface from the entry. This value may be configured.
Max Response Time	Shows the amount of time in seconds that a switch will wait after receiving an IGMP Leave Packet.
Multicast Router Expiry Time	Displays the amount of time to wait before removing an interface that is participating on the 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.

If parameter <vlan-id> is specified, the following information appears:

Term	Definition
VLAN ID	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.
Flood IGMP Report and Leave PDU	Indicates whether IGMP report and leave PDUs are flooded 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	Shows the amount of time in seconds that a switch will wait after receiving an IGMP Leave Packet.
Multicast Router Block Mode	Indicates whether the Multicast Router Block mode is enabled or disabled on the VLAN.
Multicast Router Expiry 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.
Report Suppression Mode	Indicate whether Report Suppression mode is active on the VLAN.
Vlan Block Mode	Indicate whether Vlan Block Mode is active on the VLAN.

5.2.8.35. show ip igmp snooping mrouter interface

Use this command to display information about dynamically learned or statically configured multicast router-attached interfaces.

Format show ip igmp snooping mrouter interface {<slot/port> | port-channel <portchannel-id>}

Parameter	Description
slot/port	Interface number
portchannel-id	Port-channel interface number. The range of port-channel ID is 1 to 64.

Mode Privilege Exec

Display Message

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.

5.2.8.36. show ip igmp snooping mrouter vlan

Use this command to display information about dynamically learned or statically configured multicast router-attached VLAN interfaces.

Format show ip igmp snooping mrouter vlan {<slot/port> | port-channel <portchannel-id>}

Parameter	Description
slot/port	Interface number
portchannel-id	Port-channel interface number. The range of port-channel ID is 1 to 64.

Mode Privilege Exec

Display Message

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.

5.2.8.37. show ip igmp snooping static

Use this command to display IGMP snooping static information.

Format show ip igmp snooping static

Mode Privilege Exec

Display Message

Term	Definition
VLAN	The VLAN ID used with the MAC address to fully identify the L2Mcast Group packets
MAC Address	The MAC address of the L2Mcast Group in the format 01:00:5e:xx:xx:xx.
Port	List the ports you want included into L2Mcast Group.
State	The active interface number belongs to this Multicast Group.

5.2.8.38. show mac-address-table igmpsnooping

Use this command to display the IGMP Snooping entries in the Multicast Forwarding Database (MFDB) table.

Format show mac-address-table igmpsnooping

Mode Privilege Exec

Display Message

Term	Definition
VLAN ID	The VLAN ID used with the MAC address to fully identify the L2Mcast Group packets
MAC Address	A multicast MAC address for which the switch has forwarding or filtering interfaces. The format is 01:00:5e:xx:xx:xx.
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:).

5.2.8.39. show ip igmp snooping ssm entries

Use this command to display IGMP source specific multicast forwarding database.

Format show ip igmp snooping ssm entries

Mode Privilege Exec

Display Message

Term	Definition
VLAN ID	VLAN ID
Group	Multicast Group IP address
Source IP	Source IP address
Source Filter Mode	Source filter mode (Include or Exclude) for the specified group on the specified interface and VLAN
Interfaces	The list of interfaces which are included or excluded for specified group, VLAN and source address.

5.2.8.40. show ip igmp snooping ssm groups

Use this command to display IGMP SSM group membership information.

Format show ip igmp snooping ssm groups

Mode Privilege Exec

Display Message

Term	Definition
VLAN ID	VLAN ID
Group	Multicast Group IP address
Interface	Interface which is included or excluded for specified group, VLAN and source address.
Reporter	IP Address of the source of last membership report received for the specified group address on the specified interface and VLAN
Source Filter Mode	Source filter mode (Include or Exclude) for the specified group on the specified interface and VLAN
Source Address List	Source List Entry for the specified group address, interface and VLAN

5.2.8.41. show ip igmp snooping ssm stats

Use this command to display statistics of IGMP snooping SSMFDB.

Format show ip igmp snooping ssm stats

Mode Privilege Exec

Display Message

Term	Definition
Total Entries	Maximum number of entries that the SSM MFDB table can hold for IGMP snooping.
Most SSM FDB Entries Ever Used	Most number of entries ever used in the IGMP snooping SSM MFDB table.
Current Entries	Current number of entries in the IGMP snooping SSM MFDB table.

5.2.8.42. ip igmp snooping maxresponse

Use this command to configure the IGMP Maximum Response time on a particular interface when the **igmp-plus** command is not enabled. The range is 1 to 300 seconds.

Format ip igmp snooping maxresponse <1-300>

Default 120

Mode Interface Config

5.2.8.43. no ip igmp snooping maxresponse

Use this command to restore the IGMP Maximum Response time on a particular interface to default value.

Format no ip igmp snooping maxresponse

Mode Interface Config

5.2.9. IGMP snooping querier commands

This section describes the commands which are used to configure IGMP Snooping querier.

Note: If you configure the specific IP address as the IGMP snooping querier address, the querier IP address assigned for a VLAN takes precedence over the global querier IP address. If the VLAN is a routing interface with an IP address, this IP address takes precedence over the querier IP address assigned for that VLAN.

5.2.9.1. ip igmp snooping querier

Use this command to enable IGMP snooping querier admin mode.

Format ip igmp snooping querier

Default Disable

Mode Global Config

5.2.9.2. no ip igmp snooping querier

Use this command to disable IGMP snooping querier admin mode.

Format no ip igmp snooping querier

Mode Global Config

5.2.9.3. ip igmp snooping querier address

Use this command to configure IGMP snooping querier address.

Format ip igmp snooping querier address <ip-address>

Default 0.0.0.0

Mode Global Config

5.2.9.4. no ip igmp snooping querier address

Use this command to restore IGMP snooping querier address to default value.

Format no ip igmp snooping querier address

Mode Global Config

5.2.9.5. ip igmp snooping querier query-interval

Use this command to configure IGMP snooping querier query interval.

Format ip igmp snooping querier query-interval <1-1800>

Default 60

Mode Global Config

5.2.9.6. no ip igmp snooping querier query-interval

Use this command to restore IGMP snooping querier query interval to default value.

Format no ip igmp snooping querier query-interval

Mode Global Config

5.2.9.7. ip igmp snooping querier querier-expiry-interval

Use this command to configure IGMP snooping querier querier expiry interval.

Format ip igmp snooping querier querier-expiry-interval <60-300>

Default 180

Mode Global Config

5.2.9.8. no ip igmp snooping querier querier-expiry-interval

Use this command to restore IGMP snooping querier querier expiry interval to default value.

Format no ip igmp snooping querier querier-expiry-interval

Mode Global Config

5.2.9.9. ip igmp snooping querier version

Use this command to configure IGMP snooping querier version.

Format ip igmp snooping querier version <1-2>

Default 2

Mode Global Config

5.2.9.10. no ip igmp snooping querier version

Use this command to restore IGMP snooping querier version to default value.

Format no ip igmp snooping querier version

Mode Global Config

5.2.9.11. ip igmp snooping querier vlan

Use this command to enable IGMP snooping querier vlan admin mode.

Format ip igmp snooping querier vlan <vlan-id>

Default Disable

Mode Global Config

5.2.9.12. no ip igmp snooping querier vlan <vlan-id>

Use this command to disable IGMP snooping querier vlan admin mode.

Format no ip igmp snooping querier vlan <vlan-id>

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode Global Config

5.2.9.13. ip igmp snooping querier vlan address

Use this command to configure IGMP snooping querier vlan address.

Format ip igmp snooping querier vlan <vlan-id> address <ip-address>

Default 0.0.0.0

Mode Global Config

5.2.9.14. no ip igmp snooping querier vlan address

Use this command to restore IGMP snooping querier vlan address to default value.

Format no ip igmp snooping querier vlan <vlan-id> address

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode Global Config

5.2.9.15. ip igmp snooping querier vlan election participate

Use this command to enable IGMP snooping querier vlan election participate mode.

Format ip igmp snooping querier vlan election participate <vlan-id>

Default Disable

Mode Global Config

5.2.9.16. no ip igmp snooping querier vlan election participate

Use this command to disable IGMP snooping querier vlan election participate mode.

Format no ip igmp snooping querier vlan election participate <vlan-id>

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode Global Config

5.2.9.17. show ip igmp snooping querier

Use this command to display IGMP snooping querier global information.

Format show ip igmp snooping querier

Display Message

Term	Definition
IGMP Snooping Querier Mode	Administrative mode for IGMP Snooping. The default is disable.
Querier Address	Specify the Snooping Querier Address to be used as source address in periodic IGMP queries. This address is used when no address is configured on the VLAN on which query is being sent.
IGMP Version	Specify the IGMP protocol version used in periodic IGMP queries.
Querier Query Interval	Specify the time interval in seconds between periodic queries sent by the snooping querier. The Query Interval must be a value in the range of 1 and 1800. The default value is 60.
Querier Expiry Interval	Specify the time interval in seconds after which the last querier information is removed. The Querier Expiry Interval must be a value in the range of 60 and 300. The default value is 120.

Mode Privilege Exec

5.2.9.18. show ip igmp snooping querier vlan

Use this command to display IGMP snooping querier vlan information.

Format show ip igmp snooping querier vlan <vlan-id>

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode Privilege Exec

Display Message

Term	Definition
IGMP Snooping Querier Vlan Mode	Display the administrative mode for IGMP Snooping for the switch.
Querier Election Participation Mode	Displays the querier election participate mode on the VLAN. When this mode is disabled, up on seeing a query of the same version in the vlan, the snooping

	querier move to non querier state. Only when this mode is enabled, the snooping querier will participate in querier election where in the least ip address will win the querier election and operates as the querier in that VLAN. The other querier moves to non-querier state.
Querier Vlan Address	Displays the Snooping Querier Address to be used as source address in periodic IGMP queries sent on the specified VLAN.
Operational State	Displays the operational state of the IGMP Snooping Querier on a VLAN.
Operational Version	Displays the operational IGMP protocol version of the querier.
Operational Max Resp Time	Displays the operational IGMP maximum response time of the querier.

5.2.9.19. show ip igmp snooping querier detail

Use this command to display all of the IGMP snooping querier information.

Format show ip igmp snooping querier detail

Display Message

Last Querier

Term	Definition
VLAN ID	Indicate the VLAN on which the Querier exists.
Address	Indicate the IP address of the most recent Querier from which a Query was received on this VLAN.
IGMP Version	Indicate the IGMP protocol version of the most recent Querier from which a Query was received on this VLAN.

Global IGMP Snooping querier status

Term	Definition
IGMP Snooping Querier Mode	Administrative mode for IGMP Snooping. The default is disable.
Querier Address	Specify the Snooping Querier Address to be used as source address in periodic IGMP queries. This address is used when no address is configured on the VLAN on which query is being sent.
IGMP Version	Specify the IGMP protocol version used in periodic IGMP queries.
Querier Query Interval	Specify the time interval in seconds between periodic queries sent by the snooping querier. The Query Interval must be a value in the range of 1 and 1800. The default value is 60.
Querier Expiry Interval	Specify the time interval in seconds after which the last querier information is removed. The Querier Expiry Interval must be a value in the range of 60 and 300. The default value is 120.

Mode Privilege Exec

5.2.10. MLD Snooping Commands

5.2.10.1. show ipv6 mld snooping

Use this command to display mld snooping information.

Format show ipv6 mld snooping [interface {<slot/port> | vlan <vlan-id> | port-channel <portchannel-id>}]

Parameter	Description
vlan-id	The VLAN ID. (Range: 1-4093)
slot/port	Interface number
portchannel-id	Port-channel interface number. The range of port-channel ID is 1 to 64.

Mode Privilege Exec

Display Message

If no parameters are specified, following information is displayed.

Term	Definition
Admin Mode	Indicates whether or not MLD Snooping is enabled on the switch.
Operational Mode	Indicates whether or not MLD Snooping is active on the switch.
Multicast Control Frame Count	Displays the number of MLD Control frames that are processed by the CPU.
Interfaces Enabled for MLD Snooping	Interfaces on which MLD Snooping is enabled.
VLANs enabled for MLD snooping	VLANs on which MLD Snooping is enabled.
VLANs Block enabled for snooping	VLANs on which MLD Snooping is disabled.

If parameter <slot/port> or <portchannel-id> is specified, following information is displayed.

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 interface.
Group Membership Interval	Shows the p in seconds that a switch will wait for a report from a particular group on a particular interface, which is participating on the interface, 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 in 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	Displays the amount of time to wait before removing an interface that is participating on the 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.

If parameter <vlan-id> is specified, following information appears.

Term	Definition

VLAN ID	VLAN ID.
MLD Snooping Admin Mode	Indicates whether MLD Snooping is active on the VLAN.
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	Shows the amount of time in seconds that a switch will wait after receiving an MLD Leave Packet.
Multicast Router Expiry 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.
Vlan Block Mode	Indicate whether Vlan Block Mode is active on the VLAN.

5.2.10.2. show ipv6 mld snooping mrouter interface

Use this command to display information about statically configured multicast router-attached interfaces.

Format show ipv6 mld snooping mrouter interface {<slot/port> | port-channel <portchannel-id>}

Parameter	Description
slot/port	Interface number
portchannel-id	Port-channel interface number. The range of port-channel ID is 1 to 64.

Mode Privilege Exec

Display Message

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.

5.2.10.3. show ipv6 mld snooping mrouter vlan

Use this command to display information about statically configured multicast router-attached interfaces.

Format show ipv6 mld snooping mrouter vlan {<slot/port> | port-channel <portchannel-id>}

Parameter	Description
slot/port	Interface number
portchannel-id	Port-channel interface number. The range of port-channel ID is 1 to 64.

Mode Privilege Exec

Display Message

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.

5.2.10.4. show ipv6 mld snooping static

Use this command to display MLD snooping static information.

Format show ipv6 mld snooping static

Mode Privilege Exec

Display Message

Term	Definition
VLAN	The VLAN ID used with the MAC address to fully identify packets you want L2Mcast Group
MAC Address	The MAC address of the L2Mcast Group in the format 33:33:xx:xx:xx:xx.
Port	List the ports you want included into L2Mcast Group
State	The active interface number belongs to this Multicast Group.

5.2.10.5. 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 Privilege Exec

Display Message

Term	Definition
VLAN ID	VLAN ID number
MAC Address	A multicast MAC address for which the switch has forwarding or filtering information. The format is twodigit hexadecimal numbers that are separated by colons, for example 33:33:45:67:89: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:).

5.2.10.6. show ipv6 mld snooping ssm entries

Use this command to display MLD source specific multicast forwarding database.

Format show ipv6 mld snooping ssm entries

Mode Privilege Exec

Display Message

Term	Definition
VLAN ID	VLAN ID

Group	Multicast Group IP address
Source IP	Source IP address
Source Filter Mode	Source filter mode (Include or Exclude) for the specified group on the specified interface and VLAN
Interfaces	The list of interfaces which are included or excluded for specified group, VLAN and source address.

5.2.10.7. show ipv6 mld snooping ssm groups

Use this command to display MLD SSM group membership information.

Format show ipv6 mld snooping ssm groups

Mode Privilege Exec

Display Message

Term	Definition
VLAN ID	VLAN ID
Group	Multicast Group IP address
Interface	Interface which is included or excluded for specified group, VLAN and source address.
Reporter	IP Address of the source of last membership report received for the specified group address on the specified interface and VLAN
Source Filter Mode	Source filter mode (Include or Exclude) for the specified group on the specified interface and VLAN
Source Address List	Source List Entry for the specified group address, interface and VLAN

5.2.10.8. show ipv6 mld snooping ssm stats

Use this command to display statistics of MLD snooping SSMFDB.

Format show ipv6 mld snooping ssm stats

Mode Privilege Exec

Display Message

Term	Definition
Total Entries	Maximum number of entries that the SSM MFDB table can hold for MLD snooping.
Most SSM FDB Entries Ever Used	Most number of entries ever used in the MLD snooping SSM MFDB table.
Current Entries	Current number of entries in the MLD snooping SSM MFDB table.

5.2.10.9. ipv6 mld snooping

Use this command to enable MLD Snooping globally.

Format ipv6 mld snooping

Default Disable

Mode Global Config

5.2.10.10. no ipv6 mld snooping

Use this command to disable MLD Snooping globally.

Format no ipv6 mld snooping

Mode Global Config

5.2.10.11. clear mld snooping

Use this command to delete all dynamic entries in Multicast Forwarding Database which is managed by the MLD Snooping.

Format clear mld snooping

Default None

Mode Privilege Exec

5.2.10.12. ipv6 mld snooping interfacemode

Use this command to enable MLD Snooping on a particular interface.

Format ipv6 mld snooping interfacemode

Default Disable

Mode Interface Config

5.2.10.13. no ipv6 mld snooping interfacemode

Use this command to disable MLD Snooping on a particular interface.

Format no ipv6 mld snooping interfacemode

Mode Interface Config

5.2.10.14. ipv6 mld snooping interfacemode all

Use this command to enable MLD Snooping on all interfaces.

Format ipv6 mld snooping interfacemode all

Default Disable

Mode Global Config

5.2.10.15. no ipv6 mld snooping interfacemode all

Use this command to disable MLD Snooping on all interfaces.

Format no ipv6 mld snooping interfacemode all

Mode Global Config

5.2.10.16. ipv6 mld snooping fast-leave

Use this command to enable MLD Snooping fast-leave admin mode on a particular interface or all interfaces.

Format ipv6 mld snooping fast-leave

Default Disable

Mode Global Config
Interface Config

5.2.10.17. no ipv6 mld snooping fast-leave

Use this command to disable MLD Snooping fast-leave admin mode on a particular interface or all interfaces.

Format no ipv6 mld snooping fast-leave

Mode Global Config
Interface Config

5.2.10.18. ipv6 mld snooping groupmembershipinterval

Use this command to configure the MLD Group Membership Interval time on a particular interface or all interfaces.

Format ipv6 mld snooping groupmembershipinterval <2-3600>

Default 260

Mode Global Config
Interface Config

5.2.10.19. no ipv6 mld snooping groupmembershipinterval

Use this command to restore the MLD Group Membership Interval time to default value.

Format no ipv6 mld snooping groupmembershipinterval

Mode Global Config
Interface Config

5.2.10.20. ipv6 mld snooping mcrtrexpiretime

Use this command to configure the Multicast Router Present Expiration time for the system or on a particular interface.

Format ipv6 mld snooping mcrtrexpiretime <0-3600>

Default 300 seconds

Mode Global Config
Interface Config

5.2.10.21. no ipv6 mld snooping mcrtrexpiretime

Use this command to restore the Multicast Router Present Expiration time to default value.

Format no ipv6 mld snooping mcrtrexpiretime

Mode Global Config
Interface Config

5.2.10.22. ipv6 mld snooping mrouter

Use this command to configure the interface as a multicast router-attached interface or configure the VLAN ID for the VLAN that has the multicast router attached mode enabled.

Format ipv6 mld snooping mrouter {interface |<vlan-id>}

Default None

Mode Interface Config

5.2.10.23. no ipv6 mld snooping mrouter

Use this command to disable multicast router attached mode for the interface or a VLAN.

Format no ipv6 mld snooping mrouter {interface|<vlan-id>}

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode Interface Config

5.2.10.24. ipv6 mld snooping static

Use this command to add an interface to ipv6 multicast group.

Format ipv6 mld snooping static <macaddr> vlan <vlan-id> [interface {<slot/port> | port-channel <portchannel-id>}]

Default None

Mode Global Config

5.2.10.25. no ipv6 mld snooping static

Use this command to remove an interface from ipv6 multicast group.

Format no ipv6 mld snooping static <macaddr> vlan <vlan-id> interface {<slot/port> | port-channel <portchannel-id>}

Parameter	Description
vlan-id	The VLAN ID. (Range: 1-4093)
macaddr	Multicast Group MAC address
slot/port	Interface number
portchannel-id	Port-channel interface number. The range of port-channel ID is 1 to 64.

Mode Global Config

5.2.10.26. set mld

Use this command to enable MLD Snooping on a particular VLAN.

Format set mld <vlan-id>

Default Disable

Mode VLAN database

5.2.10.27. no set mld

Use this command to disable MLD Snooping on a particular VLAN.

Format no set mld <vlan-id>

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode VLAN database

5.2.10.28. set mld fast-leave

Use this command to enable MLD Snooping fast-leave admin mode on a particular VLAN.

Format set mld fast-leave <vlan-id>

Default Disable

Mode VLAN database

5.2.10.29. no set mld fast-leave

Use this command to disable MLD Snooping fast-leave admin mode on a particular VLAN.

Format no set mld fast-leave <vlan-id>

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode VLAN database

5.2.10.30. set mld groupmembership-interval

Use this command to configure the MLD Group Membership Interval time on a particular VLAN.

Format set mld groupmembership-interval <vlan-id> <2-3600>

Default 260

Mode VLAN database

5.2.10.31. no set mld groupmembership-interval

Use this command to restore the MLD Group Membership Interval time on a particular VLAN to default value.

Format no set mld groupmembership-interval <vlan-id>

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode VLAN database

5.2.10.32. set mld maxresponse

Use this command to configure the MLD Maximum Response time on a particular VLAN.

Format set mld maxresponse <vlan-id> <1-65>

Default 10

Mode VLAN database

5.2.10.33. no set mld maxresponse

Use this command to restore the MLD Maximum Response time on a particular VLAN to default value.

Format no set mld maxresponse <vlan-id>

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode VLAN database

5.2.10.34. set mld mcrtrexpiretime

Use this command to configure the Multicast Router Present Expiration time on a particular VLAN.

Format set mld mcrtrexpiretime <vlan-id> <0-3600>

Default 300 seconds

Mode VLAN database

5.2.10.35. no set mld mcrtrexpiretime

Use this command to restore the Multicast Router Present Expiration time on a particular VLAN to default value.

Format no set mld mcrtrexpiretime <vlan-id>

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode VLAN database

5.2.11. MLD Snooping Querier Commands

This section describes the commands which are used to configure MLD Snooping querier.

5.2.11.1. show ipv6 mld snooing querier

Use this command to display MLD snooping querier global information.

Format show ipv6 mld snooping querier

Mode Privileged Exec

Display Message

Term	Definition
MLD Snooping Querier Mode	Specify the Snooping Querier Address to be used as source address in periodic MLD queries. This address is used when no address is configured on the VLAN on which query is being sent.
Querier Address	Specify the Snooping Querier Address to be used as source address in periodic MLD queries. This address is used when no address is configured on the VLAN on which query is being sent.
MLD Version	Specify the MLD protocol version used in periodic MLD queries.
Querier Query Interval	Specify the time interval in seconds between periodic queries sent by the snooping querier. The Query Interval must be a value in the range of 1 and 1800. The default value is 60.

Querier Expiry Interval	Specify the time interval in seconds after which the last querier information is removed. The Querier Expiry Interval must be a value in the range of 60 and 300. The default value is 120.

5.2.11.2. show ipv6 mld snooping querier vlan

Use this command to display MLD snooping querier vlan information.

Format show ipv6 mld snooping querier vlan <vlan-id>

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode Privileged Exec

Display Message

Term	Definition
MLD Snooping Querier Vlan Mode	Displays the querier election participate mode on the VLAN. When this mode is disabled, up on seeing a query of the same version in the vlan, the snooping querier move to non querier state. Only when this mode is enabled, the snooping querier will participate in querier election where in the least ip address will win the querier election and operates as the querier in that VLAN. The other querier moves to non-querier state.
Querier Election Participation Mode	Displays the querier election participate mode on the VLAN. When this mode is disabled, up on seeing a query of the same version in the vlan, the snooping querier move to non querier state. Only when this mode is enabled, the snooping querier will participate in querier election where in the least ip address will win the querier election and operates as the querier in that VLAN. The other querier moves to non-querier state.
Querier Vlan Address	Displays the Snooping Querier Address to be used as source address in periodic MLD queries sent on the specified VLAN.
Operational State	Specifies the operational state of the MLD Snooping Querier on a VLAN.
Operational Version	Displays the operational MLD protocol version of the querier.

5.2.11.3. show ipv6 mld snooping querier detail

Use this command to display MLD snooping querier global information.

Format show ipv6 mld snooping querier detail

Mode Privileged Exec

Display Message

Term	Definition
VLAN ID	Specify the VLAN ID on which the MLD snooping querier is enabled.

Last Querier Address	Specify the IP address of the most recent Querier from which a Query was received.
MLD Snooping Querier Mode	Specify the Snooping Querier Address to be used as source address in periodic MLD queries. This address is used when no address is configured on the VLAN on which query is being sent.
Querier Address	Specify the Snooping Querier Address to be used as source address in periodic MLD queries. This address is used when no address is configured on the VLAN on which query is being sent.
MLD Version	Specify the MLD protocol version used in periodic MLD queries.
Querier Query Interval	Specify the time interval in seconds between periodic queries sent by the snooping querier. The Query Interval must be a value in the range of 1 and 1800. The default value is 60.
Querier Expiry Interval	Specify the time interval in seconds after which the last querier information is removed. The Querier Expiry Interval must be a value in the range of 60 and 300. The default value is 120.

5.2.11.4. ipv6 mld snooping querier

Use this command to enable MLD snooping querier admin mode.

Format ipv6 mld snooping querier

Default Disable

Mode Global Config

5.2.11.5. no ipv6 mld snooping querier

Use this command to disable MLD snooping querier admin mode.

Format no ipv6 mld snooping querier

Mode Global Config

5.2.11.6. ipv6 mld snooping querier address

Use this command to configure MLD snooping querier address.

Format ipv6 mld snooping querier address <ipv6-address>

Default 0

Mode Global Config

5.2.11.7. no ipv6 mld snooping querier address

Use this command to restore MLD snooping querier address to default value.

Format no ipv6 mld snooping querier address

Mode Global Config

5.2.11.8. ipv6 mld snooping querier query-interval

Use this command to configure MLD snooping querier querier interval.

Format ipv6 mld snooping querier query-interval <1-1800>

Default 60

Mode Global Config

5.2.11.9. no ipv6 mld snooping querier querier-interval

Format no ipv6 mld snooping querier query-interval

Mode Global Config

5.2.11.10. ipv6 mld snooping querier querier-expiry-interval

Use this command to configure MLD snooping querier querier expiry interval.

Format ipv6 mld snooping querier querier-expiry-interval <60-300>

Default 125

Mode Global Config

5.2.11.11. no ipv6 mld snooping querier querier-expiry-interval

Use this command to restore MLD snooping querier querier expiry interval to default value.

Format no ipv6 mld snooping querier querier-expiry-interval

Mode Global Config

5.2.11.12. ipv6 mld snooping querier vlan

Use this command to enable MLD snooping querier vlan admin mode.

Format ipv6 mld snooping querier vlan <vlan-id>

Default Disable

Mode Global Config

5.2.11.13. no ipv6 mld snooping querier vlan

Use this command to disable MLD snooping querier vlan admin mode.

Format no ipv6 mld snooping querier vlan <vlan-id>

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode Global Config

5.2.11.14. ipv6 mld snooping querier vlan address

Use this command to configure MLD snooping querier vlan address.

Format ipv6 mld snooping querier vlan <vlan-id> address <ipv6-address>

Default 0

Mode Global Config

5.2.11.15. no ipv6 mld snooping querier vlan address

Format no ipv6 mld snooping querier vlan <vlan-id> address

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode Global Config

5.2.11.16. ipv6 mld snooping querier vlan election participate

Use this command to enable MLD snooping querier vlan election participate mode.

Format ipv6 mld snooping querier vlan election participate <vlan-id>

Default Disable

Mode Global Config

5.2.11.17. no ipv6 mld snooping querier vlan election participate

Use this command to disable MLD snooping querier vlan election participate mode.

Format no ipv6 mld snooping querier vlan election participate <vlan-id>

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode Global Config

5.2.12. 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.

5.2.12.1. show interface port-channel brief

This command displays the capability of all port-channels (LAGs) on the device as well as a summary of individual port-channels.

Format show interface port-channel brief

Mode Privileged EXEC
User EXEC

For each port-channel the following information is displayed:

Parameter	Definition
Channel ID	The field displays the port-channel's ID.
Port-Channel Name	This field displays the name of the port-channel.
Min-links	This field displays the minimum links value of the port-channel.
Link State	This field indicates whether the link is up or down.
Trap Flag	This object determines whether or not to send a trap when link status changes. The factory default is enabled.
Type	This field displays the status designating whether a particular port-channel (LAG) is statically or dynamically maintained. The possible values of this field are Static, indicating that the port-channel is statically maintained; and Dynamic, indicating that the port-channel is dynamically maintained.
Mbr Ports	This field lists the ports that are members of this port-channel, in slot/port notation.
Active Ports	This field lists the ports that are actively participating in this port-channel.

Example: The following example displays the interface port-channel brief configurations.

```
(M4500-48XF8C) #show interface port-channel brief

 Channel  Port-Channel Name Min Link State Trap     Type    Mbr Ports  Active Ports

   ID                                    Flag

--------- ----------------- --- ---------- -------- ------- ---------  ------------

1         ch1               1   Down       Disabled Static

2         ch2               1   Down       Disabled Static

3         ch3               1   Down       Disabled Static

4         ch4               1   Down       Disabled Static
```

```
5          ch5                1    Down       Disabled Static

6          ch6                1    Down       Disabled Static

7          ch7                1    Down       Disabled Static

8          ch8                1    Down       Disabled Static

9          ch9                1    Down       Disabled Static

10         ch10               1    Down       Disabled Static

11         ch11               1    Down       Disabled Static

12         ch12               1    Down       Disabled Static

13         ch13               1    Down       Disabled Static

14         ch14               1    Down       Disabled Static

15         ch15               1    Down       Disabled Static

16         ch16               1    Down       Disabled Static

17         ch17               1    Down       Disabled Static

18         ch18               1    Down       Disabled Static

19         ch19               1    Down       Disabled Static
```

5.2.12.2. show interface port-channel

This command displays an overview of all port-channels (LAGs) or a specific port-channel on the switch.

Format show interface port-channel [<ID>]

Mode Privileged EXEC
User EXEC

If you do not use the optional parameters *ID*, the command displays following information for all port-channels:

Parameter	Definition
Channel ID	The field displays the port-channel's ID.
Channel Name	This field displays the name of the port-channel.
Min	This field displays the minimum links value of the port-channel.
Link	This field indicates whether the link is up or down.
Admin Mode	May be enabled or disabled. The factory default is enabled.
Link Trap	This object determines whether or not to send a trap when link status changes.

	The factory default is enabled
STP Mode	This field displays the MSTP administrative bridge port state.
Type	This field displays the status designating whether a particular port-channel (LAG) is statically or dynamically maintained. The possible values of this field are Static, indicating that the port-channel is statically maintained; and Dynamic, indicating that the port-channel is dynamically maintained.
Mbr Ports	This field lists the ports that are members of this port-channel, in slot/port notation.
Device Timeout	This field displays the device timeout value of actor and partner. The value of device timeout should be short(1 second) or long(30 seconds).
Port Speed	Speed of the port-channel port.
Active Ports	This field lists the ports that are actively participating in the port-channel (LAG).

Example: The following example displays the interface port-channel configurations.

```
M4500-48XF8C) #show  interface port-channel

Channel    Channel                Adm. Link STP         Mbr    Device/       Port      Port

  ID        Name       Min  Link   Mode Trap Mode   Type Ports  Timeout       Speed     Active

------- -------------- ---- ------ ---- ---- ------ ---- ------ ------------- --------- -------

1       ch1            3    Down   En.  Dis. En.    Stat

2       ch2            1    Down   En.  Dis. En.    Stat

3       ch3            1    Down   En.  Dis. En.    Stat

4       ch4            1    Down   En.  Dis. En.    Stat

5       ch5            1    Down   En.  Dis. En.    Stat

6       ch6            1    Down   En.  Dis. En.    Stat

7       ch7            1    Down   En.  Dis. En.    Stat

8       ch8            1    Down   En.  Dis. En.    Stat
```

```
9       ch9             1    Down   En.  Dis. En.    Stat

10      ch10            1    Down   En.  Dis. En.    Stat

11      ch11            1    Down   En.  Dis. En.    Stat

12      ch12            1    Down   En.  Dis. En.    Stat

13      ch13            1    Down   En.  Dis. En.    Stat

14      ch14            1    Down   En.  Dis. En.    Stat

15      ch15            1    Down   En.  Dis. En.    Stat
```

If you use the optional parameters *ID*, the command displays following information for the specific port-channel:

Parameter	Definition
Port Channel ID	The field displays the port-channel's ID.
Channel Name	This field displays the name of the port-channel.
Link State	This field indicates whether the link is up or down.
Admin Mode	May be enabled or disabled. The factory default is enabled.
Link Trap Mode	This object determines whether or not to send a trap when link status changes. The factory default is enabled
STP Mode	This field displays the MSTP administrative bridge port state.
Type	This field displays the status designating whether a particular port-channel (LAG) is statically or dynamically maintained. The possible values of this field are Static, indicating that the port-channel is statically maintained; and Dynamic, indicating that the port-channel is dynamically maintained.
Port-channel Min-links	This field displays the minimum links value of the port-channel.
Load Balance Option (Src/Dest MAC, VLAN, EType, incoming port)	The load balance option associated with the port-channel..
LACP Fallback Mode	May be enabled or disabled. The factory default is disabled.
LACP Fallback Timeout	This field displays the LACP fallback timeout, the timeout default is 5sec.
Mbr Ports	This field lists the ports that are members of this port-channel, in slot/port notation.

Device Timeout	This field displays the device timeout value of actor and partner. The value of device timeout should be short(1 second) or long(30 seconds).
Port Speed	Speed of the port-channel port.
Active Ports	This field lists the ports that are actively participating in the port-channel (LAG).

Example: The following example displays the interface port-channel configurations.

```
M4500-48XF8C) #show interface port-channel 1

Port Channel ID.............................. 1

Channel Name................................. ch1

Link State................................... Down

Admin Mode................................... Enabled

Admin Key.................................... 354

Link Trap Mode............................... Disabled

STP Mode..................................... Enabled

Type......................................... Static

Port-channel Min-links....................... 1

Load Balance Option.......................... 3

(Src/Dest MAC, VLAN, EType, incoming port)

LACP Fallback Mode........................... Disabled

LACP Fallback Timeout........................ 5


Mbr    Device/       Port      Port    Fallback

Ports  Timeout       Speed     Active

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

5.2.12.3. show interface port-channel system priority

This command displays the port-channel system priority.

Format show interface port-channel system priority

Mode Privileged EXEC
User EXEC

5.2.12.4. show lacp actor

This command displays LACP actor attributes.

Format show lacp actor [slot/port]

Mode Privileged EXEC
User EXEC

Display Message

Parameter	Description
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 LACPUDs

5.2.12.5. show lacp interface

This command displays LACP status for interface.

Format show lacp interface [slot/port]

Mode Privileged EXEC
User EXEC

5.2.12.6. interface port-channel

This command configures a new port-channel (LAG) with the specified ID. Display the information of this port-channel using the **show interface port-channel <portchannel-id>.**

Note: Before including a port in a port-channel, set the port physical mode. For more information, see **speed-duplex** command

Format interface port-channel <portchannel-id>

Mode Global Config

5.2.12.7. staticcapability

This command enables the static function to support on specific port-channels (static link aggregations - LAGs) on the device.

Format staticcapability

Default Disabled

Mode Interface Config

5.2.12.8. no staticcapability

This command disables the static function to support on specific port-channels (static link aggregations - LAGs) on the device.

Format no staticcapability

Mode Interface Config

5.2.12.9. port-channel linktrap

This command enables link trap notifications for the port-channel (LAG). The interface is an ID for a configured port-channel. The option **all** sets every configured port-channel with the same administrative mode setting.

Format port-channel linktrap {<ID> | all}

Default Enabled

Mode Global Config

5.2.12.10. no port-channel linktrap

This command disables link trap notifications for the port-channel (LAG). The interface is a ID for a configured port-channel. The option **all** sets every configured port-channel with the same administrative mode setting.

Format no port-channel linktrap {<ID> | all}

Mode Global Config

5.2.12.11. 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 form selected fields in a packet, and associating that pattern with a particular link.

This command can be configured for a single interface, a range of interfaces, or all interfaces.

Format port-channel load-balance {src-mac | dst-mac | src-dst-mac | src-ip | dst-ip | src-dst-ip }

Parameter	Definition
src-mac	Sets the mode on the source MAC address.
dst-mac	Sets the mode on the destination MAC address.
src-dst-mac	Sets the mode on the source and destination MAC addresses.
src-ip	Sets the mode on the source IP address.
dst-ip	Sets the mode on the destination IP addresses.
src-dst-ip	Sets the mode on the source and destination IP addresses.
enhanced	Set the mode on the source and destination MAC addresses if it is a L2 packet or on the source and destination IP addresses if it is a IP packet.
<ID> | all	Global Config Mode only: The interface is an identifier of a configured port-channel. A**ll** applies the command to every configured port-channel.

Default src-dst-mac

Mode Global Config

5.2.12.12. no port-channel load-balance

This command reverts to the default load balancing configuration.

Format no port-channel load-balance {<ID> | all}

Mode Global Config

5.2.12.13. 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 form selected fields in a packet, and associating that pattern with a particular link.

Format load-balance {src-mac | dst-mac | dst-src-mac | src-ip | dst-ip | dst-src-ip | enhanced}

Parameter	Definition
src-mac	Sets the mode on the source MAC address.
dst-mac	Sets the mode on the destination MAC address.
src-dst-mac	Sets the mode on the source and destination MAC addresses.
src-ip	Sets the mode on the source IP address.
dst-ip	Sets the mode on the destination IP addresses.
src-dst-ip	Sets the mode on the source and destination IP addresses.
enhanced	Set the mode on the source and destination MAC addresses if it is a L2 packet or on the source and destination IP addresses if it is a IP packet.

Default src-dst-mac

Mode Interface Config

5.2.12.14. no load-balance

This command reverts to the default load balancing configuration.

Format no load-balance

Mode Interface Config

5.2.12.15. port-channel system priority

This command configures port-channel system priority. The value range of priority is 0-65535.

Format port-channel system priority <priority-value>

Default 32768 (0x8000)

Mode Global Config

5.2.12.16. no port-channel system priorty

This command configures the default port-channel system priority vlaue.

Format no port-channel system priority

Mode Global Config

5.2.12.17. lacp

This command enables Link Aggregation Control Protocol (LACP) on a port or a range of interfaces.

Format lacp

Default Enabled

Mode Interface Config

5.2.12.18. no lacp

This command disables Link Aggregation Control Protocol (LACP) on a port or a range of interfaces.

Format no lacp

Mode Interface Config

5.2.12.19. lacp all

This command enables Link Aggregation Control Protocol (LACP) on all ports.

Format lacp all

Default Enabled

Mode Global Config

5.2.12.20. no lacp

This command disables Link Aggregation Control Protocol (LACP) on all ports.

Format no lacp all

Mode Global Config

5.2.12.21. lacp admin key

This command configures the administrative value of the key for the port-channel. This command can be used to configure a single interface or a range of interfaces.

Note: This command is applicable only to port-channel interfaces

Format lacp admin key <0-65535>

Default Internal interface number of this port-channel

Mode Interface Config

5.2.12.22. no lacp admin key

This command configures the default administrative value of the key for the port-channel.

Format no lacp admin key

Mode Interface Config

5.2.12.23. lacp actor admin key

This command configures the administrative value of the LACP actor admin key on an interface or a range of interfaces. “0” means that this value is not configured yet and the key value of the physical interfaces will be adjusted to the internal interface number of the port-channel that this physical interface is going to join to.

Note: This command is applicable only to physical interfaces

Format lacp actor admin key <0-65535>

Default 0

Mode Interface Config

5.2.12.24. no lacp actor admin key

This command configures the default administrative value of the key.

Format no lacp actor admin key

Mode Interface Config

5.2.12.25. lacp actor admin state

This command configures the administrative value of the actor state as transmitted by the Actor in LACPUDs. This command can be used to configure a single interface or a range of interfaces.

Note: This command is applicable only to physical interfaces

Format lacp actor admin state <individual | longtimeout | passive>

Default no lndividual (aggregation)
longtimeout (no shorttimeout)
no passive (active)

Mode Interface Config

5.2.12.26. no lacp actor admin state

This command configures the default administrative value of actor state as transmitted by the Actor in LACPDUs.

Note: Both the **no port lacptimeout** and the **no lacp actor admin state** commands set the values back to default, regardless of the command used to configure the ports.

Format no lacp actor admin state <individual | longtimeout | passive>

Mode Interface Config

5.2.12.27. lacp actor port priority

This command configures the priority value assigned to the Aggregation Port for an interface or a range of interfaces.

Note: This command is applicable only to physical interfaces

Format lacp actor port priority <0-65535>

Default 128 (0x80)

Mode Interface Config

5.2.12.28. no lacp actor port priority

This command configures the default priority value assigned to the Aggregation Port.

Format no lacp actor port priority

Mode Interface Config

5.2.12.29. min-links

This command configures the minimum links for port-channel interfaces. The maximum number of members for each port-channel is 32. For T1048-LB9/T1048-LB9A, the maximum number of members is 8.

Note: This command is applicable only to port-channel interfaces

Format min-links <1-*max number*>

Default 1

Mode Interface Config

5.2.12.30. no min-links

This command configures the default minimum links for port-channel interfaces.

Format no min-links

Mode Interface Config

5.2.12.31. lacp fallback

This command configures the fallback feature for Link Aggregation.

Note: This command is applicable only to port-channel interfaces

Format lacp fallback

Default Disabled

Mode Interface Config

5.2.12.32. no lacp fallback

This command restores the fallback feature to default value.

Format no lacp fallback

Mode Interface Config

5.2.12.33. lacp fallback timeout

This command configures the fallback timeout value for Link Aggregation.

Note: This command is applicable only to port-channel interfaces

Format lacp fallback timeout <1-100>

Default 5

Mode Interface Config

5.2.12.34. no lacp fallback timeout

This command restores the fallback feature to default timeout value.

Format no lacp fallback timeout

Mode Interface Config

5.2.12.35. channel-group

This command assigns and configures an interface to a port-channel (LAG) group. The interface is an ID of a configured port-channel.

Note: Before adding a port to a port-channel, set the physical mode of the port. See 'port-mode' command.

You can change the mode for an interface only if it is the only interface designated to the specified channel group. If you enter this command on an interface that is added to a channel with a different protocol (than the protocol you are entering), the command is rejected.

Format channel-group <ID> mode {active | on}

Parameter	Definition
active	Enables LACP unconditionally.

on	Enables static mode (Cisco EtherChannel-like).

Default None

Mode Interface Config

5.2.12.36. no channel-group

This command removes the interface from the specified channel group.

Format no channel-group <ID>

Mode Interface Config

5.2.12.37. delete-channel-group

This command deletes all configured ports from the port-channel (LAG). The interface is an ID of a configured port-channel.

Note: This command is applicable only to port-channel interfaces

Format delete-channel-group <ID> all

Default None

Mode Global Config

5.2.12.38. port lacpmode enable all

This command enables Link Aggregation Control Protocol (LACP) on all ports.

Format port lacpmode enable all

no port lacpmode enable all

Mode Global Config

5.2.12.39. port lacptimeout

This command sets the timeout for all interfaces of a particular device type (actor or partner) to either long or short timeout.

Format port lacptimeout {actor | partner} {long | short}

no port lacptimeout {actor | partner}

Default long

Mode Global Config

5.2.13. Storm Control

This section describes the commands you use to configure storm control or display storm control 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.

5.2.13.1. 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.

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 [{ <slot/port> | all | port-channel <id> }]

Parameter	Definition
<slot/port>	Specifies a valid slot number and port number for the system.
all	Indicates to display the configuration parameters for all ports.
id	Specifies the port channel ID

Mode Privileged EXEC, Global Config, Interface Config

The following is the display format for the command without any optional parameter.

Display Message

Fields	Definition
Broadcast Storm Control Mode	The storm-control configuration mode for broadcast traffic.
Broadcast Storm Control Level	The storm-control speed threshold for broadcast traffic.

Broadcast Storm Control Action	The storm-control action for broadcast traffic.
Multicast Storm Control Mode	The storm-control configuration mode for multicast traffic.
Multicast Storm Control Level	The storm-control speed threshold for multicast traffic.
Multicast Storm Control Action	The storm-control action for multicast traffic.
Unicast Storm Control Mode	The storm-control configuration mode for unicast traffic.
Unicast Storm Control Level	The storm-control speed threshold for unicast traffic.
Unicast Storm Control Action	The storm-control action for unicast traffic.

The following is the display format for the command with a specific parameter.

Display Message

Fields	Definition
Intf	The interface number.
Bcast Mode	The storm-control configuration mode for broadcast traffic.
Bcast Level	The storm-control speed threshold for broadcast traffic.
Bcast Action	The storm-control action for broadcast traffic.
Mcast Mode	The storm-control configuration mode for multicast traffic.
Mcast Level	The storm-control speed threshold for multicast traffic.
Mcast Action	The storm-control action for multicast traffic.
Ucast Mode	The storm-control configuration mode for unicast traffic.
Ucast Level	The storm-control speed threshold for unicast traffic.
Ucast Action	The storm-control action for unicast traffic.
Flow Mode	The storm-control speed threshold for unicast traffic.

5.2.13.2. storm-control Configuration

Use this command to enable storm control on each port or all ports.

Format storm-control {broadcast | multicast | unicast} [{action { shutdown| trap} | level <0-100>| rate <0-14880000>}]

Parameter	Definition
broadcast | multicast | unicast	Specifies to enable one of storm control modes for an interface or all interfaces.
action shutdown | trap	Indicates the action to be taken if the storm occurs. Shutdown is to disable the interface. Trap is to send SNMP trap.
level <0-100>	Specifies a threshold level (a percentage of link speed) for all interfaces or one interface. The default is 5.
rate <0-14880000>	Specifies a threshold rate(in packets per second) for all interfaces or one interface. The default is 0.

Default disabled

Mode Global Config

Interface Config

5.2.13.3. storm-control broadcast

Use this command to enable broadcast storm control 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.

Format storm-control broadcast

Default disabled

Mode Global Config

Interface Config

5.2.13.4. no storm-control broadcast

This command disables broadcast storm control for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format no storm-control broadcast

Mode Global Config
Interface Config

5.2.13.5. 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.

Format storm-control broadcast action { shutdown | trap }

Default None

Mode Global Config
Interface Config

5.2.13.6. 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

5.2.13.7. 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.

Format storm-control broadcast rate <0-14880000>

Default 0

Mode Global Config
Interface Config

5.2.13.8. 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

5.2.13.9. 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.

Format storm-control broadcast level <0-100>

Default 5

Mode Global Config
Interface Config

5.2.13.10. 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

5.2.13.11. 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.

Format storm-control multicast

Default disabled

Mode Global Config
Interface Config

5.2.13.12. 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

5.2.13.13. 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

Format storm-control multicast action {shutdown | trap}

Default None

Mode Global Config
Interface Config

5.2.13.14. 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

5.2.13.15. 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

Format storm-control multicast level <0-100>

Default 5

Mode Global Config
Interface Config

5.2.13.16. 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

Mode Global Config
Interface Config

5.2.13.17. 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.

Format storm-control multicast rate <0-14880000>

Default 0

Mode Global Config
Interface Config

5.2.13.18. 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

5.2.13.19. 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.

Format storm-control unicast

Default disabled

Mode Global Config
Interface Config

5.2.13.20. 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

5.2.13.21. 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.

Format storm-control unicast action { shutdown | trap }

Default None

Mode Global Config
Interface Config

5.2.13.22. no storm-control unicast action

This command returns the unicast storm recovery action option to the default value for all interfaces (GlobalConfig mode) or one or more interfaces (Interface Config mode).

Format no storm-control unicast action

Mode Global Config
Interface Config

5.2.13.23. 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.

Format storm-control unicast level <0-100>

Default 5

Mode Global Config
Interface Config

5.2.13.24. 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 multicast level

Mode Global Config
Interface Config

5.2.13.25. 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.

Format storm-control unicast rate <0-14880000>

Default 0

Mode Global Config
Interface Config

5.2.13.26. 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

5.2.14. Port Mirror Commands

This section describes the commands you use to select network traffic that you can analyze with a network analyzer.

Note: On LY4R, one port cannot join more than one port-monitor session regardless of source port or destination port due to the HW limitation.

5.2.14.1. show port-mirror session

Use this command to display the port monitoring information for the specified session.

Format show port-monitor session { <1-4> | all }

Parameter	Definition
<1-4>	An integer value used to identify the session.Its value can be anything between 1 and the maximum number of mirroring sessions(4) allowed on the platform.
all	Displays the all sessions

Mode Privileged EXEC

Display Message

Fields	Definition
Session ID	The session ID. The range of session ID is 1 to 4.
Admin Mode	Indicates whether the Port Monitoring feature is enabled or disabled. 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.
Src VLAN	All member ports of this VLAN are mirrored. If the source VLAN is not configured, this field is blank.
Mirrored Port	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.
Ref. Port	This port carries all the mirrored traffic at the source switch.
Src RVLAN	The source VLAN is configured at the destination switch. If the remote VLAN is not configured, this field is blank.
Dst RVLAN	The destination VLAN is configured at the source switch. If the remote VLAN is not configured, this field is blank.

Type	Direction in which source port configured for port mirroring. Types are tx for transmitted packets and rx for receiving packets.
IP ACL	The IP access-list id or name attached to the port mirroring session.
MAC ACL	The MAC access-list id or name attached to the port mirroring session.

5.2.14.2. port-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. On LY4R, one port cannot join more than one port-monitor session regardless of source port or destination port due to the HW limitation.

Format port-monitor session <1-4> source {interface {<port-list> | <slot/port> | cpu | port-channel {<1-64> | <chId-list>}} [{rx | tx}] | remote vlan <1-4093>| vlan <1-4093>}

no port-monitor [session <1-4> [source {interface {<port-list> | <slot/port> | cpu | port-channel {<1-64> | <chId-list>}} | remote vlan | vlan}]]

Parameter	Definition
<1-4>	The session ID, which can be 1, 2, 3, or 4.
<port-list>	The physical-port IDs in range from 1 to 48. Use '-' to specify a range, or ',' to separate physical port IDs in a list. Spaces and zeros are not permitted.
<slot/port>	The interface number.
port-channel <1-64>	The port-channel interface number. The range of the port-channel ID is from 1 to 64.
port-channel <chId-list>	The channel IDs in range <1-64>. Use '-' to specify a range, or ',' to separate physical-port IDs in a list. Spaces and zeros are not permitted.
rx | tx	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.
remote vlan <1-4093>	The VLAN ID to be monitored on the remote switch. The range is 1 to 4093.
vlan <1-4093>	The VLAN ID to be monitored. The range is 1 to 4093.

Default None

Mode Global Config

5.2.14.3. no port-monitor session source

Use this command to remove the specified mirrored port from the selected port mirroring session.

Format no port-monitor session <session-id> source { interface {<slot/port> | cpu | port-channel } [{rx | tx} } | remote vlan <vlan-id>| vlan <vlan-id> }

Default None

Mode Global Config

5.2.14.4. port-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. On LY4R, one port cannot join more than one port-monitor session regardless of source port or destination port due to the HW limitation.

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.

Format port-monitor session <1-4> destination { interface <slot/port> | remote vlan <1-4093> reflector-port <slot/port> }

Parameter	Definition
<1-4>	Session number. The range of session id is 1 to 4
interface <slot/port>	The Interface number .
remote vlan <1-4093>	The VLAN ID to be monitored on the remote switch. The range is 1 to 4093.
reflector-port <slot/port>	The Interface number for reflector-port.

Default None

Mode Global Config

5.2.14.5. no port-monitor session destination

Use this command to remove the specified probe port from the selected port mirroring session.

Format no port-monitor session <session-id> destination { interface <slot/port> | remote vlan <vlan-id> reflector-port <slot/port> }

Default None

Mode Global Config

5.2.14.6. port-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.

Note: 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.

Format port-monitor session <1-4> filter { ip | mac } access-group <aclid | ip-acl-name>

Parameter	Definition
<1-4>	Session number. The range of session id is 1 to 4
ip | mac	Indicates IP or MAC ACLs will be attached to the session.
<aclid>	Enter an integer specifying an IP ACL number.
<ip-acl-name>	Enter access-list name up to 31 characters in length .

Default None

Mode Global Config

5.2.14.7. no port-monitor session filter

Use this command to remove the specified IP/MAC ACL from the selected monitoring session.

Format no port-monitor session <session-id> filter { ip | mac } access-group

Default None

Mode Global Config

5.2.14.8. port-monitor session mode

Use this command to configure the mode parameters to enable the administrative mode of the selected port mirroring session. If enabled, the probe port monitors all the traffic received and transmitted on the physical monitored port.

Format port-monitor session <1-4> mode

Parameter	Definition
<1-4>	Session number. The range of session id is 1 to 4

Default None

Mode Global Config

5.2.14.9. no port-monitor session mode

The command disables port-monitoring function for the selected port monitoring session.

Format no port-monitor session <session-id> mode

Default None

Mode Global Config

5.2.14.10. no port-monitor session

Use this command without optional parameters to remove the monitor session (port monitoring) destination 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.

Format no port-monitor session <session-id>

Parameter	Definition
<1-4>	Session number. The range of session id is 1 to 4

Default None

Mode Global Config

5.2.14.11. no port-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.

Format no port-monitor

Default enabled

Mode Global Config

5.2.15. Link State

5.2.15.1. show link state

Show link state information.

Format show link state group [<1-48>]

Parameter	Description
<1-48>	The range of group id is 1 to 48.

Default None

Mode Global Config

Display Message

Fields	Definition
Group ID	The group ID for each displayed row.
DownStream	Display such port was included to DownStream set.
UpStream	Display such port was included to UpStream set.

Link Action	This group was set which action
Group State	The state of this group

5.2.15.2. link state group action

This command is used to Link DOWN the group downstream interface list when upstream link goes down (link is up othewise) or Link UP the group downstream interface list when upstream link goes down (link is down otherwise).

Format link state group <1-48> action {down | up}

no link state group <1-48>

Parameter	Description
<1-48>	The range of group id is 1 to 48.
no	Disable the group action

Default None

Mode Global Config

5.2.15.3. link state group

This command is used to add interface to the downstream/upstream interface list.

Format link state group <1-48> {downstream| upstream}

no link state group <1-48> {downstream| upstream}

Parameter	Description
<1-48>	The range of group id is 1 to 48.
no	Remove the selected interface from downstream/upstream list.

Default None

Mode Interface Config

5.2.16. Port-backup Commands

This section describes commands you use to configure port-backup group. Port- backup group consists of two ports, one port is used under normal condition and treated as an “active port”, the other port is NOT used while the other port is active mode and it is treated as a “Backup (Stand-by) port”.

5.2.16.1. show port-backup

This command displays information about port-backup group.

Format show port-backup

Mode Privileged EXEC

The following example shows the CLI display output for the command *show port-backup*.

```
(M4500-32C) #show port-backup

Admin Mode: Enable

Group  Mode  MAC Update  Failback  Active Port   Backup Port  Current Active Port

-----  ----  ----------  --------  ------------  -----------  -------------------

1      En.   Enable      60(sec)   0/1           0/2
```

5.2.16.2. port-backup

Use this command to enable port-backup admin mode.

Format port-backup

Default Disable

Mode Global Config

5.2.16.3. no port-backup

Use this command to disable port-backup admin mode.

Format no port-backup

Mode Global Config

5.2.16.4. port-backup group

Use this command to create the port backup group.

Format port-backup group [<group id>]

Default NA

Mode Global Config

5.2.16.5. no port-backup group

Use this command to destroy the port-backup group.

Format no port-backup group <group id>

Mode Global Config

5.2.16.6. port-backup group active

Use this command to set active port for a port-backup group.

Format port-backup group <group id> active

Default NA

Mode Interface Config

5.2.16.7. no port-backup group active

Use this command to reset active port for a port-backup group.

Format no port-backup group <group id> active

Mode Interface Config

5.2.16.8. port-backup group backup

Use this command to set backup port for a port-backup group.

Format port-backup group <group id> backup

Default NA

Mode Interface Config

5.2.16.9. no port-backup group backup

Use this command to reset backup port for a port-backup group.

Format no port-backup group <group id> backup

Mode Interface Config

5.2.16.10. port-backup group enable

Use this command to enable a port-backup group.

Format port-backup group enable <group id>

Default Disable

Mode Global Config

5.2.16.11. port-backup group mac-move-update

Use this command to enable the MAC address-table move update feature for a port-backup group.

Format port-backup group <group id> mac-move-update

Default Disable

Mode Global Config

5.2.16.12. no port-backup group mac-move-update

Use this command to disable the MAC address-table move update feature for a port-backup group.

Format no port-backup group <group id> mac-move-update

Mode Global Config

5.2.16.13. port-backup group failback-time

Use this command to set auto-failback time for a port-backup group. Setting the value to 0 means that auto-failback time feature is disabled.

Format port-backup group <group id> failback-time 0

port-backup group <group id> failback-time <10-60>

Default 60s

Mode Global Config

5.2.16.14. no port-backup group failback-time

Use this command to reset auto-failback time for a port-backup group.

Format no port-backup group <group id> failback-time

Mode Global Config

5.3. Provisioning (IEEE 802.1p) Commands

This section describes the commands you use to configure provisioning (IEEE 802.1p,) which allows you to prioritize ports.

5.3.1. switchport priority all

This command configures the port priority assigned for untagged packets for all ports presently plugged into the device. Any subsequent per port configuration will override this configuration setting.

Format switchport priority all <0-7>

Default 0

Mode Global Config

5.3.2. no switchport priority all

This command restores the priority value to default value for all interfaces.

Format no switchport priority all

Mode Global Config

5.3.3. switchport priority

This command configures the default 802.1p port priority assigned for untagged packets for a specific interface.

Format switchport priority <0-7>

Default 0

Mode Interface Config

5.3.4. no switchport priority

This command restores the priority configuration to default value.

Format no switchport priority

Mode Interface Config

5.4. Management Commands

5.4.1. Network Commands

5.4.1.1. show ip interface

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.

Format show ip interface

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
VLAN ID	Indicates whether the VLAN ID is used for this vlan interface.
Interface Status	Indicates whether the interface is up or down.
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
MAC Address	The MAC address used for in-band connectivity.
Network Configuration Protocol Current	Indicates which network protocol is being used. The options are bootp | dhcp | none.

5.4.1.2. show ip filter

This command displays management IP filter status and all designated management stations.

Format show ip filter

Default None

Mode Privileged Exec

5.4.1.3. 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.

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).

Format mtu <1518-9412>

Default 1518 (untagged)

Mode Interface Config

5.4.1.4. no mtu

This command sets the default MTU size(in bytes) for the interface.

Format no mtu

Mode Interface Config

5.4.1.5. interface vlan

This command is used to create a vlan interface and enter Interface-vlan configuration mode.

Format interface vlan <vlan-id>

Parameter	Definition
<vlan-id>	VLAN ID (Range: 1 - 4093).

Default None

Mode Global Config

5.4.1.6. 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 "show ip interface".

Format ip address <ipaddr> {subnetmask | /prefix-length} [secondary]

Parameter	Definition
ipaddr	The IP address of the interface.
subnetmask	A 4-digit dotted-decimal number which represents the subnet mask of the interface.
masklen	Implements RFC 3021. Using the/notation of the subnet mask, this is and integer that indicates the length of subnet mask. Range is 5 to 32 bits.

Default IP address: 0.0.0.0

Subnet Mask: 0.0.0.0

Mode Interface-Vlan 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.

```
(M4500-32C) (if-vlan100)#ip address 192.168.10.2 255.255.255.254

(M4500-32C) (if-vlan100)#
```

5.4.1.7. no ip addess

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 | /prefix-length} [secondary]

Mode Interface-Vlan Config

5.4.1.8. ip default-gateway

This command sets the IP Address of the default gateway.

Format ip default-gateway <gateway-addr>

no ip default-gateway

Parameter	Definition
< gateway-addr >	IP address of the default gateway.

no	Restore the default IP address of the default gateway.

Default IP address: 0.0.0.0

Mode Global Config

5.4.1.9. 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.

Format ip address dhcp [{client-id | restart}]

Parameter	Definition
client-id	Enable the DHCP client to specify the unique client identifier (option 61).
restart	Restarts the DHCP process.

Default None

Mode Interface Config

5.4.1.10. no ip address dhcp

Use this command to release a leased address and disable DHCPv4 on an interface.

Format no ip address dhcp [client-id]

Mode Interface Config

5.4.1.11. ip filter

This command is used to enable the IP filter function.

Format ip filter

Default Disabled

Mode Global Config

5.4.1.12. no ip filter

Disable ip filter.

Format no ip filter

Mode Global Config

5.4.1.13. ip filter <name> {ipv4|ipv6}<ipAddr>[<mask>]

This command is used to set an IP address to be a filter.

Format ip filter <name> {ipv4 <ipAddr> [<mask>] | ipv6 <prefix/length>}
no ip filter <name>

Parameter	Definition
<name>	The name of the IP filter.
<ipAddr>	Specifies an IP address to the filter.
<mask>	Specifies the mask for a range filter.
<prefix/length>	Specifies an IPv6 prefix and prefix length.

Default None

Mode Global Config

5.4.1.14. no ip filter<name>

Remove this IP address from filter.

Format no ip filter <name>

Mode Global Config

5.4.2. Serial Interface Commands

5.4.2.1. show line console

This command displays serial communication settings for the switch.

Format show line console

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
Serial Port Login Timeout (minutes)	Specifies the time, in minutes, of inactivity on a Serial port connection, after which the Switch will close the connection. Any numeric value between 0 and 160 is allowed, the factory default is 5. A value of 0 disables the timeout.
Baud Rate	The default baud rate at which the serial port will try to connect. The available values are 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200 bauds.
Character Size	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.
Password Threshold	When the logon attempt threshold is reached on the console port, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the silent time command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface closes.
Silent Time (sec)	Use this command to set the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the password threshold command.
Terminal Length	The columns per page for terminal serial port.

5.4.2.2. line console

This command is used to enter Line configuration mode

Format line console

Default None

Mode Global Config

5.4.2.3. baudrate

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

Format baudrate {1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200}

Default 115200

Mode Line Config

5.4.2.4. no baudrate

This command sets the communication rate of the terminal interface to **115200**.

Format line console

Mode Line Config

5.4.2.5. exec-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.

Format exec-timeout <0-160>

Default 5

Mode Line Config

5.4.2.6. no exec-timeout

This command sets the maximum connect time (in minutes) without console activity to 5.

Format no exec-timeout

Mode Line Config

5.4.2.7. password-threshold

This command is used to set the password instruction threshold limiting the number of failed login attempts.

Format password-threshold <0-120>

Default 3

Mode Line Config

5.4.2.8. no password-threshold

This command sets the maximum value to the default.

Format no password-threshold

Mode Line Config

5.4.2.9. silent-time

This command uses to set the amount of time the management console is inaccessible after the number of unsuccessful logon tries exceeds the threshold value.

Format silent-time <0-65535>

Default 0

Mode Line Config

5.4.2.10. no silent-time

This command sets the maximum value to the default.

Format no silent-time

Mode Line Config

5.4.2.11. terminal length

This command uses to configure the columns per page for the management console.

Format terminal length <10-100>

Default 24

Mode Privileged Exec

5.4.2.12. line password

This command is used to specify the password for the line mode.

Format password [<password>]

Default None

Mode Line Config

no password (Line Config)

This command set the password for the line mode to default.

Format no password

Mode Line Config

5.4.3. Telnet Session Commands

5.4.3.1. telnet

This command establishes a new outbound telnet connection to a remote host.

Format telnet <ip-address|hostname> [port] [debug] [line]

Parameter	Definition
<ip-address|hostname>	A hostname or a valid IPv4 address.
port	A valid decimal integer in the range of 0 to 65535, where the default value is 23.
debug	Display current enabled telnet options.
line	Set the outbound telnet operational mode as 'linemode', where by default, the operational mode is 'character mode'.

Default None

Mode Privileged Exec
User Exec

5.4.3.2. show line vty

This command displays telnet settings.

Format show line vty

Default None

Mode Privileged Exec

Display Message

Parameter	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. A zero means there will be no timeout. May be specified as a number from 0 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	Indicates that new telnet sessions will not be allowed when set to no. The factory default value is yes.
Telnet Server Admin Mode	The telnet server admin mode status. The factory default is enable.
Telnet Server Port	The listen port number of Telnet service.
Password Threshold	When the logon attempt threshold is reached on the console port, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the silent time command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface closes.
Terminal Length	The columns per page for terminal vty port.

5.4.3.3. line vty

This command is used to enter vty (Telnet) configuration mode.

Format line vty

Default None

Mode Global Config

5.4.3.4. exec-timeout

This command sets the remote connection session timeout value, in minutes. A session is active as long as the session has been idle for the value set. A value of 0 indicates that a session remains active indefinitely. The time is a decimal value from 0 to 160.

i	Changing the timeout value for active sessions does not become effective until the session is reaccessed. Any keystroke will also activate the new timeout duration.

Format exec-timeout <1-160>

Default 5

Mode Line Vty

Example:

```
(M4500-32C) #configure

(M4500-32C) (Config)#line vty

(M4500-32C) (Config-vty)#exec-timeout 10
```

5.4.3.5. no exec-time out

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

Format no exec-timeout

Mode Line Vty

5.4.3.6. password-threshold

This command is used to set the password instruction threshold limited for the number of failed login attempts.

Format password-threshold <0-120>

Default 3

Mode Line Vty

Example:

```
(M4500-32C) #configure

(M4500-32C) (Config)#line vty

(M4500-32C) (Config-vty)#password-threshold 10
```

5.4.3.7. no password-threshold

This command sets the maximum value to the default

Format no password-threshold

Mode Line Vty

5.4.3.8. maxsessions

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

Format maxsessions <0-5>

Default 5

Mode Line Vty

Example:

```
(M4500-32C) #configure

(M4500-32C) (Config)#line vty

(M4500-32C) (Config-vty)#maxsessions 5
```

5.4.3.9. no maxsessions

This command sets the maximum value to be 5.

Format no maxsessions

Mode Line Vty

5.4.3.10. server enable

This command enables/disables telnet server. If telnet server is enabled, all telnet sessions can be established until there are no more sessions available. If telnet server is disabled, all telnet sessions are closed.

Format server enable

Default Enabled

Mode Line Vty

5.4.3.11. no server enable

This command disables telnet server. If telnet server is disabled, all telnet sessions are droped.

Format no server enable

Mode Line Vty

5.4.3.12. sessions

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

Format sessions

Default Enabled

Mode Line Vty

5.4.3.13. no sessions

This command disables telnet sessions. If sessions are disabled, no new telnet sessions are established.

Format no sessions

Mode Line Vty

5.4.3.14. telnet sessions

This command regulates new outbound telnet connections. If enabled, new outbound telnet sessions can be established until it reaches the maximum number of simultaneous outbound telnet sessions allowed. If disabled, no new outbound telnet session can be established. An established session remains active until the session is ended or an abnormal network error ends it.

Format telnet sessions

Default Enabled

Mode Global Config

5.4.3.15. no telnet sessions

This command disables new outbound telnet connections. If disabled, no new outbound telnet connection can be established.

Format no telnet sessions

Mode Global Config

5.4.3.16. telnet maxsessions

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

Format telnet maxsessions <0-5>

Default 5

Mode Global Config

5.4.3.17. no telnet maxsessions

This command sets the maximum value to be 5.

Format no telnet maxsessions

Mode Global Config

5.4.3.18. telnet exec-timeout

This command sets the outbound telnet session timeout value in minute.

i Changing the timeout value for active sessions does not become effective until the session is reaccessed. Any keystroke will also activate the new timeout duration.

Format telnet exec-timeout <1-160>

Default 5

Mode Global Config

5.4.3.19. no telnet exec-timeout

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

Format no telnet exec-timeout

Mode Global Config

5.4.3.20. show telnet

This command displays the current outbound telnet settings.

Format show telnet

Default None

Mode Privileged Exec
User Exec

Display Message

Parameter	Definition
Outbound Telnet Login Timeout (in minutes)	Indicates the number of minutes an outbound telnet session is allowed to remain inactive before being logged off. A value of 0, which is the default, results in no timeout.
Maximum Number of Outbound Telnet Sessions	Indicates the number of simultaneous outbound telnet connections allowed.
Allow New Outbound Telnet Sessions	Indicates whether outbound telnet sessions will be allowed.

5.4.4. SNMP Server Commands

5.4.4.1. show snmp

This command displays SNMP community information and SNMP trap/inform receivers. Trap/Inform messages are sent across a network to an SNMP Network Manager. These messages alert the manager to events occurring within the switc

h or on the network.

You can add, change, or delete communities. The switch does not have to be reset for changes to take effect.

The SNMP agent of the switch complies with SNMP versions 1, 2c, and 3 (for more about the SNMP specification, see the SNMP RFCs). The SNMP agent sends traps through TCP/IP to an external SNMP manager based on the SNMP configuration (the trap receiver and other SNMP community parameters).

Note: By default, no community strings such as 'private' or 'public' exist for SNMPv1 and SNMPv2. In addition, the MD5 authentication procotol is used for SNMPv3, and the 'None' authentication protocol is not allowed.

Format show snmp

Default None

Mode Privileged EXEC

Display Message

Parameter	Definition
Community-String	The community string to which this entry grants access. A valid entry is a case-sensitive alphanumeric string of up to 20 characters. Each row of this table must contain a unique community name.
Community-Access	The access level for this community string.
View Name	The view this community has access to.
IP Address	Access to this community is limited to this IP address.
Group Name	The community this mapping configures.
Target Address	An IP address (or portion thereof) from which this device will accept SNMP packets with the associated community.
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.
SNMP v1	Uses SNMP v1 to send traps to the receiver.
SNMP v2	Uses SNMP v2 to send traps to the receiver.
SNMP v3	Uses SNMP v3 to send traps to the receiver.
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.

Username	The user this mapping configures.
Security Level	The authentication and encryption level for snmpv3.
NoAuth-N	No authentication checksum and no encryption algorithm assigned.
Auth-NoP	Md5 or sha authentication checksum assigned and no encryption algorithm assigned.
Auth-Pri	Md5 or sha authentication checksum and des encryption algorithm assigned.

5.4.4.2. snmp-server sysname

This command sets the name of the switch. The range for name is from 1 to 64 alphanumeric characters.

Format snmp-server sysname <name>

Parameter	Definition
<name>	Range is from 1 to 64 alphanumeric characters.

Default None

Mode Global Config

5.4.4.3. snmp-server location

This command sets the physical location of the switch. The range for name is from 1 to 255 alphanumeric characters.

Format snmp-server location <loc>

Parameter	Definition
<loc>	Range is from 1 to 255 alphanumeric characters.

Default None

Mode Global Config

5.4.4.4. snmp-server contact

This command sets the name of the organization responsible for the network. The name can be from 1 to 255 alphanumeric characters.

Format snmp-server contact <name>

Parameter	Definition
<name>	The name can be from 1 to 255 alphanumeric characters.

Default None

Mode Global Config

5.4.4.5. snmp-server community

This command adds a new SNMP community, and optionally sets the access mode, allowed IP address, and creates a view for the community. The allowed IP address supports IPv4 and IPv6 address but does not support IP mask value to demote a range of IPv6 addresses.

Note: Community names in the SNMP community table must be unique. If you make multiple entries using the same community name, the first entry is kept and processed and all duplicate entries are ignored.

Format snmp-server community <community-string> [ipaddress <ipaddress> | ro | rw | su | view <viewname>]

Parameter	Definition
<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-name can be up to 20 case-sensitive characters.
ipaddress	The associated community SNMP packet sending address and is used along with the client IP mask value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 0.0.0.0 allows access from any IP address. Otherwise, this value is ANDed with the mask to determine the range of allowed client IP addresses.
ro | rw | su	The access mode of the SNMP community, which can be public (Read-Only/RO), private (Read-Write/RW), or Super User (SU).
<viewname>	The name of the view to create or update.

Default None

Mode Global Config

5.4.4.6. no snmp-server community <community-string>

This command deletes snmp community.

Format no snmp-server community <community-string>

Mode Global Config

5.4.4.7. 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 <ip-address>]

Parameter	Definition
<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.
<ip-address>	Optionally, the IPv4 address that the community may be accessed from.

Default None

Mode Global Config

5.4.4.8. no snmp-server community-group <community-string>

This command deletes snmp community group.

Format no snmp-server community-group <community-string>

Mode Global Config

5.4.4.9. show snmp engineid

This command displays the currently configured SNMP engineID.

Format show snmp engineid

Default None

Mode Privileged Exec

Display Message

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

Example: The following shows examples of the CLI display output for the commands.

```
(M4500-32C) (Config)#show snmp engineid

Local SNMP engineID : 80001c4c032c600c83ad47
```

5.4.4.10. snmp-server engineid

This command configures snmp engineID on the local device.

Note: Changing the engineID will invalidate all SNMP configuration that exists on the box.

Format snmp-server engineid local {<engine-id> | default}

Parameter	Definition
<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.

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

Mode Global Config

5.4.4.11. no snmp-server engineid

This command removes snmp engineID.

Format no snmp-server engineid local

Mode Global Config

5.4.4.12. show snmp filters

This command displays the configured filters used when sending traps.

Format show snmp filters [<filter-name>]

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
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.

Example: The following shows examples of the CLI display output for the commands.

```
(M4500-32C) (Config)#show snmp filters

Name                            OID Tree                        Type

------------------------------  ------------------------------ ----------

test                            fastPathSwitching               Included
```

5.4.4.13. snmp-server filter

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

Format snmp-server filter <filter-name> <oid-tree> [excluded | included]

Parameter	Definition
<filter-name>	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).
excluded	The tree is excluded from the filter.
included	The tree is included in the filter.

Default None

Mode Global Config

5.4.4.14. no snmp-server filter <filter-name> [<oid-tree >]

This command removes the specified filter.

Format no snmp-server filter <filter-name> [<oid-tree >]

Mode Global Config

5.4.4.15. show snmp user

This command displays the currently configured SNMPv3 users.

Format show snmp user [<username>]

Default None

Mode Privileged Exec

Display Message

Parameter	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.

Example: The following shows examples of the CLI display output for the commands.

```
(M4500-32C) (Config)#show snmp user

Name               Group Name              Auth     Priv
                                           Meth     Meth     Remote Engine ID
-----------------  ----------------------  -------  -------  --------------------------------
test               DefaultRead             MD5      DES      80001c4c032c600c83ad47
```

5.4.4.16. snmp-server user

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

Format snmp-server user <name> <group-name> [remote <engine-idstring>] {[auth-md5 | auth-md5-key <md5-key> | auth-sha | auth-sha-key <sha-key>] [priv-des-key <des-key>]}

Parameter	Definition
<name>	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 6 to 32 characters.
auth-md5	The keyword to enable you to set the plain-text password for MD5 authentication.
auth-sha	The keyword to enable you to set the plain-text password for SHA authentication.
<md5-key>	A pregenerated MD5 authentication key. The length is 32 characters.
<sha-key>	A pregenerated SHA authentication key. The length is 48 characters.
<priv-des-key>	A pregenerated DES encryption key. The length is 32 characters.

Default None

Mode Global Config

5.4.4.17. no snmp-server user

This command removes the specified SNMPv3 user.

Format no snmp-server user <name> [remote <engine-idstring>]

Mode Global Config

5.4.4.18. show snmp group

This command displays the configured groups.

Format show snmp group [<groupname>]

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
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.

Example: The following shows examples of the CLI display output for the commands.

```
(M4500-48XF8C) #show snmp group


       Name            Context        Security                  Views

                       Prefix     Model     Level       Read    Write    Notify

--------------------- ---------- ----- ------------- -------- -------- --------

DefaultRead            ""         V1    NoAuth-NoPriv Default  ""       Default

DefaultRead            ""         V2    NoAuth-NoPriv Default  ""       Default

DefaultRead            ""         V3    NoAuth-NoPriv Default  ""       Default

DefaultRead            ""         V3    Auth-NoPriv   Default  ""       Default

DefaultRead            ""         V3    Auth-Priv     Default  ""       Default

DefaultSuper           ""         V1    NoAuth-NoPriv DefaultS DefaultS DefaultS

                                                      uper     uper     uper

DefaultSuper           ""         V2    NoAuth-NoPriv DefaultS DefaultS DefaultS

                                                      uper     uper     uper

DefaultSuper           ""         V3    NoAuth-NoPriv DefaultS DefaultS DefaultS

                                                      uper     uper     uper

DefaultWrite           ""         V1    NoAuth-NoPriv Default  Default  Default

DefaultWrite           ""         V2    NoAuth-NoPriv Default  Default  Default

DefaultWrite           ""         V3    NoAuth-NoPriv Default  Default  Default

DefaultWrite           ""         V3    Auth-NoPriv   Default  Default  Default

DefaultWrite           ""         V3    Auth-Priv     Default  Default  Default
```

5.4.4.19. snmp-server group

This command creates an SNMP access group.

Format snmp-server group <group-name> [v1 | v2 | v3 {auth | priv}] {[read <readview>] | [write <writeview>] | [context <contextprefix>] | [notify <notifyview>]}

Parameter	Definition
<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.
<readview>	The view this group will use during GET requests. The range is 1 to 30 characters.
<writeview>	The view this group will use during SET requests. The range is 1 to 30 characters.
<notifyview>	The view this group will use when sending out traps. The range is 1 to 30 characters.

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

Mode Global Config

5.4.4.20. no snmp-server group

This command removes the specified group.

Format no snmp-server group <group-name> [v1 | v2 | v3 {auth | noauth | priv}] { [context <contextprefix>] | [notify <notifyview>]}

Mode Global Config

5.4.4.21. show snmp views

This command displays the currently configured views.

Format show snmp views [<viewname>]

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
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.

Example: The following shows examples of the CLI display output for the commands.

```
(M4500-32C) (Config)#show snmp views

Name                        OID Tree                        Type

------------------------    -------------------------------  ------------

Default                     iso                             Included

Default                     snmpVacmMIB                     Excluded

Default                     usmUser                         Excluded

Default                     snmpCommunityTable              Excluded

DefaultSuper                iso                             Included
```

5.4.4.22. 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.

Format snmp-server view <view-name> <oid-tree> [excluded | included]

Parameter	Definition
<view-name>	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 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).
excluded	The tree is excluded from the view.
included	The tree is included in the view.

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

Mode Global Config

5.4.4.23. no snmp-server view

This command removes the specified view.

Format no snmp-server view <view-name> [<oid-tree>]

Mode Global Config

5.4.5. SNMP Trap Commands

5.4.5.1. snmp-server host <host-addr> traps

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

Format snmp-server host <host-addr> traps version {1 <community> | 2 <community> | 3 <username> [auth | priv]} [filter <filtername>] [udp-port <1-65535>]

Parameter	Definition
<host-addr>	The IPv4 or IPv6 address of the host to send the trap to.
version 1	Sends SNMPv1 traps.
version 2	Sends SNMPv2 traps.
<community>	Community string sent as part of the notification. The range is 1 to 20 characters.
version 3	Sends SNMPv3 traps.
<username>	Username of SNMPv3.
auth	Enables authentication of a packet without encrypting.
priv	Enables authentication and encrypting of a packet.
<filtername>	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.
udp-port <1-65535>	The SNMP trap receiver port. The default is port 162.

Default None

Mode Global Config

5.4.5.2. no snmp-server host <host-addr>

This command deletes trap receivers.

Format no snmp-server host <host-addr>

Mode Global Config

5.4.5.3. show trapflags

This command displays trap conditions. 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 switch's SNMP agent sends the trap to all enabled trap receivers. The switch does not have to be reset to implement the changes. Cold and warm start traps are always generated and cannot be disabled.

Format show trapflags

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
Authentication Flag	May be enabled or disabled. The factory default is enabled. Indicates whether authentication failure traps will be sent.
Link Up/Down Flag	May be enabled or disabled. The factory default is enabled. Indicates whether link status traps will be sent.
Multiple Users Flag	May 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 via telnet or serial port).
Spanning Tree Flag	May be enabled or disabled. The factory default is enabled. Indicates whether spanning tree traps will be sent.
ACL Traps	May be enabled or disabled. The factory default is disabled. Indicates whether ACL traps will be sent.
BGP Traps	May be enabled or disabled. The factory default is disabled. Indicates whether BGP traps will be sent.
OSPFv2 Traps	May be enabled or disabled. The factory default is disabled. Indicates whether OSPF traps will be sent.
PIM Traps	May be enabled or disabled. The factory default is disabled. Indicates whether PIM traps will be sent.
OSPFv3 Traps	May be enabled or disabled. The factory default is disabled. Indicates whether OSPFv3 traps will be sent.

Power Supply Module state trap	May be enabled or disabled. The factory default is enabled. Indicates whether power supply status traps will be sent.
Temperature trap	May be enabled or disabled. The factory default is enabled. Indicates whether temperature status traps will be sent.
Fan trap	May be enabled or disabled. The factory default is enabled. Indicates whether fan status traps will be sent.
FIP snooping Traps	May be enabled or disabled. The factory default is enabled. Indicates whether snooping traps will be sent.
Transceiver Traps	May be enabled or disabled. The factory default is disabled. Indicates whether Transceiver traps will be sent.

Example: The following shows examples of the CLI display output for the commands.

```
(M4500-32C) (Config)#show trapflags

Authentication Flag.......................... Enable

Link Up/Down Flag............................ Enable

Multiple Users Flag.......................... Enable

Spanning Tree Flag........................... Enable

ACL Traps.................................... Disable

BGP Traps.................................... Disable

OSPFv2 traps................................. Disable

PIM Traps.................................... Disable

OSPFv3 Traps................................. Disable

Power Supply Module state trap............... Enable

Temperature trap............................. Enable

Fan trap..................................... Enable

FIP snooping Traps........................... Enable

Transceiver Flag............................. Disable
```

5.4.5.4. snmp trap link-status all

This command enables link status traps for all interfaces.

Note: This command is valid only when the Link Up/Down Flag is enabled. See 'snmp-server enable traps linkmode‘ command.

Format snmp trap link-status all

Default Disabled

Mode Global Config

5.4.5.5. no snmp trap link-status all

This command disables link status traps for all interfaces.

Format no snmp trap link-status all

Mode Global Config

5.4.5.6. snmp-server enable traps acl-trapflags

This command enables the acl trap.

Format snmp-server enable traps acl-trapflags

Default Disabled

Mode Global Config

5.4.5.7. no snmp-server enable traps acl-trapflags

This command disables the acl trap.

Format no snmp-server enable traps acl-trapflags

Mode Global Config

5.4.5.8. snmp-server enable traps authentication

This command enables the Authentication trap.

Format snmp-server enable traps authentication

Default Enabled

Mode Global Config

5.4.5.9. no snmp-server enable traps authentication

This command enables the Authentication trap.

Format no snmp-server enable traps authentication

Mode Global Config

5.4.5.10. snmp-server enable traps bgp state-changes limited

This command enables the BGP trap.

Format snmp-server enable traps bgp state-changes limited

Default Disabled

Mode Global Config

5.4.5.11. no snmp-server enable traps bgp state-changes limited

This command disables the BGP trap.

Format no snmp-server enable traps bgp state-changes limited

Mode Global Config

5.4.5.12. snmp-server enable traps fan

This command enables the fan status trap.

Format snmp-server enable traps fan

Default Enabled

Mode Global Config

5.4.5.13. no snmp-server enable traps fan

This command disables the fan status trap.

Format no snmp-server enable traps fan

Mode Global Config

5.4.5.14. snmp-server enable traps linkmode

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 (see ‘snmp trap link-status’ command).

Format snmp-server enable traps linkmode

Default Enabled

Mode Global Config

5.4.5.15. 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

5.4.5.16. 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.

Format snmp-server enable traps multiusers

Default Enabled

Mode Global Config

no snmp-server enable traps multiusers

This command disables Multiple User trap.

Format no snmp-server enable traps multiusers

Mode Global Config

5.4.5.17. snmp-server enable traps ospf

This command enables OSPF traps.

Format snmp-server enable traps ospf {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}}

Default Disabled

Mode Global Config

5.4.5.18. no snmp-server enable traps ospf

This command disables OSPF trap.

Format no snmp-server enable traps ospf {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 Global Config

5.4.5.19. snmp-server enable traps ospfv3

This command enables OSPFv3 traps.

Format snmp-server enable traps ospfv3 {all | errors {all | bad-packet | config-error | 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}}

Default Disabled

Mode Global Config

5.4.5.20. no snmp-server enable traps ospfv3

This command disables OSPFv3 trap.

Format no snmp-server enable traps ospfv3 {all | errors {all | bad-packet | config-error | 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 Global Config

5.4.5.21. snmp-server enable traps pim

This command enables PIM traps.

Format snmp-server enable traps pim

Default Disabled

Mode Global Config

5.4.5.22. no snmp-server enable traps pim

This command disables PIM trap.

Format no snmp-server enable traps pim

Mode Global Config

5.4.5.23. snmp-server enable traps powersupply

This command enables power supply status traps.

Format snmp-server enable traps powersupply

Default Enabled

Mode Global Config

5.4.5.24. no snmp-server enable traps powersupply

This command disables power supply status trap.

Format no snmp-server enable traps powersupply

Mode Global Config

5.4.5.25. snmp-server enable traps stpmode

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

Format snmp-server enable traps stpmode

Default Enabled

Mode Global Config

5.4.5.26. 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

5.4.5.27. snmp-server enable traps temperature

This command enables the temperature status trap.

Format snmp-server enable traps temperature

Default Enabled

Mode Global Config

5.4.5.28. no snmp-server enable traps temperature

This command disables the temperature status trap.

Format no snmp-server enable traps temperature

Mode Global Config

5.4.5.29. snmp-server enable traps transceiver

This command enables the transceiver trap.

Format snmp-server enable traps transceiver

Default Disabled

Mode Global Config

5.4.5.30. no snmp-server enable traps transceiver

This command disables the transceiver trap.

Format no snmp-server enable traps transceiver

Mode Global Config

5.4.5.31. snmp-server enable traps violation

This command enables the violation trap.

Format snmp-server enable traps violation

Default Disabled

Mode Global Config

Interface Config

5.4.5.32. no snmp-server enable traps violation

This command disables the violation trap.

Format no snmp-server enable traps violation

Mode Global Config

Interface Config

5.4.5.33. show snmp source-interface

This command displays the configured global source interface used for the SNMP client. The IP address of the selected interface is used as source IP for all communications with the server.

Format show snmp source-interface

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
SNMP trap Client Source Interface	The interface configured as the source interface for the SNMP trap/inform client.
SNMP trap Client IPv4 Address	The IP address configured on the SNMP client source interface.

Example: The following shows examples of the CLI display output for the commands.

```
(M4500-32C) (Config)#show snmp source-interface

SNMP trap Client Source Interface.............. serviceport
SNMP trap Client Source IPv4 Address........... 172.16.3.60                [Up]
SNMP trap Client Source IPv6 Address........... fe80::2e60:cff:fe83:ad47   [Up]
```

5.4.5.34. snmptrap source-interface

Use this command in Global configuration mode to configure the global source-interface (Source IP address) for all SNMP communications between the SNMP client and the server. This command takes effect for both SNMP trap and inform client.

Format snmptrap source-interface {<slot/port> | loopback <loopback-id> | serviceport | tunnel <tunnel-id> | vlan <vlan-id>}

Parameter	Definition
<slot/port>	Specifies the interface 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 63.
<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 interface to use as the source interface. The range of VLAN ID is 1 to 4093.

Default Disabled

Mode Global Config

5.4.5.35. no snmptrap source-interface

This command removes the global source-interface for all SNMP communication between the SNMP client and the server.

Format no snmptrap source-interface

Mode Global Config

5.4.5.36. snmp trap link-status

This command enables link up/down traps for the specified port.

Format snmp trap link-status

Default Enabled

Mode Interface Config

5.4.5.37. no snmp trap link-status

This command disables link status traps for the specified interfaces.

Format no snmp trap link-status all

Mode Interface Config

5.4.6. SNMP Inform Commands

5.4.6.1. snmp-server host <host-addr> informs

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

Format snmp-server host <host-addr> informs version 2 <community> [filter <filtername>] [udp-port <1-65535>] [retries <1-255>] [timeout <1-300>]

Parameter	Definition
<host-addr>	The IPv4 or IPv6 address of the host to send the inform to.
version 2	Sends SNMPv2 informs.

<community>	Community string sent as part of the notification. The range is 1 to 20 characters.
<filtername>	The filter name to associate with this host. Filters can be used to specify which informs are sent to this host. The range is 1 to 30 characters.
<udp-port>	The SNMP Inform receiver port. The default is port 162.
<retries>	The number of times to resend an Inform. The default is 3 attempts. The range is 1 to 255 retries.
<timeout>	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.

Default None

Mode Global Config

5.4.6.2. no snmp-server host <host-addr>

This command deletes inform receivers.

Format no snmp-server host <host-addr>

Mode Global Config

5.4.7. Secure Shell (SSH) Commands

5.4.7.1. show ip ssh

This command displays the SSH settings.

Format show ip ssh

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
Administrative Mode	This field indicates whether the administrative mode of SSH is enabled or disabled.
SSH Port	The listen port number of SSH service.

Protocol Levels	The protocol level supports.
SSH Sessions Currently Active	This field specifies the current number of SSH connections.
Max SSH Sessions Allowed	The maximum number of inbound SSH sessions allowed on the switch.
SSH Timeout	This field is the inactive timeout value for incoming SSH sessions to the switch.
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.
User Password Authentication	Indicates whether the SSH authentication mode of user password is enabled or disabled.
User Public Key Authentication	Indicates whether the SSH authentication mode of user public key is enabled or disabled.
Terminal Length	indicates the number of lines to be paginated and displayed on a screen for a new SSH session.

5.4.7.2. show ip ssh user-public-key current-user

This command displays the public key content of current login session.

Format show ip ssh user-public-key current-user

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
Username	Username of current login session.
Key Type	Type of user public key. Possible values are DSA or RSA.
Context of Public Key	Full context of current user's public key.

5.4.7.3. show ip ssh user-public-key who-has-key

This command displays a username list which indicates the owners of public keys, and it only allows user "admin" to execute this command.

Format show ip ssh user-public-key who-has-key

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
Public Key Owners	A username list which indicates the owners of public keys in this device.

5.4.7.4. ip ssh

This command is used to enable SSH.

Format ip ssh

Default Enabled

Mode Global Config

5.4.7.5. no ip ssh

This command is used to disable SSH.

Format no ip ssh

Mode Global Config

5.4.7.6. ip ssh 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.

Format ip ssh maxsessions <0-5>

Default 5

Mode Global Config

5.4.7.7. no ip ssh maxsessions

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

Format no ip ssh maxsessions

Mode Global Config

5.4.7.8. ip ssh port

This command specifies the listen port number of SSH service. The range is 1 to 65535.

Format ip ssh port <1-65535>

Default 1234

Mode Global Config

5.4.7.9. no ip ssh port

This command sets the listen port number of SSH service to the default value.

Format no ip ssh port

Mode Global Config

5.4.7.10. ip ssh timeout

This command specifies the maximum idle time for each SSH login session. The range is 1 to 160 minutes.

Format ip ssh port <1-160>

Default 5

Mode Global Config

5.4.7.11. no ip ssh timeout

This command sets the maximum idle time for each SSH login session to the default value.

Format no ip ssh timeout

Mode Global Config

5.4.7.12. ip ssh user-password-auth

This command is used to enable the SSH authentication mode of user password.

Format ip ssh user-password-auth

Default Enabled

Mode Global Config

5.4.7.13. no ip ssh user-password-auth

This command is used to disable the SSH authentication mode of user password.

Format no ip ssh user-password-auth

Mode Global Config

5.4.7.14. ip ssh user-public-key-auth

This command is used to enable the SSH authentication mode of user public key.

Format ip ssh user-public-key-auth

Default Disabled

Mode Global Config

5.4.7.15. no ip ssh user-public-key-auth

This command is used to disable the SSH authentication mode of user public key.

Format no ip ssh user-public-key-auth

Mode Global Config

5.4.8. Management Security Commands

5.4.8.1. crypto key generation {RSA|DSA}

This command is used to generate an RSA or DSA key pair for SSH. Please note that the SSHv1 key will not be generated.

Format crypto key generate {RSA | DSA}

Default None

Mode Global Config

5.4.8.2. no crypto key generate {RSA | DSA}

This command is used to delete the RSA or DSA key from the device.

Format no crypto key generate {RSA | DSA}

Mode Global Config

5.4.8.3. crypto certificate generation

This command is used to generate a certificate for HTTPS.

Format crypto certificate generate

Default None

Mode Global Config

5.4.8.4. no crypto certificate generate

This command is used to delete the certificate from the device.

Format no crypto certificate generate

Mode Global Config

5.4.9. DHCP Client Commands

5.4.9.1. dhcp client vendor-id-option

This command is used to enable the inclusion of the DCHP Option 60, Vendor Class Identifier, in the requests transmitted to the DHCP server by the DHCP client in this switch. Use the **no** form to restore to default value.

Format dhcp client vendor-id-option

Default Not include DHCP Option 60

Mode Global Config

5.4.9.2. no dhcp client vendor-id-option

This command is used to restore to default value.

Format no dhcp client vendor-id-option

Mode Global Config

5.4.9.3. dhcp client vendor-id-option-string

This command is used to set the DCHP Option 60 string in the requests transmitted to the DHCP server by the DHCP client in this switch. The length of the string is from 0 to 128 characters. Use the **no** form to restore to default value.

Format dhcp client vendor-id-option-string <string>

Default No string defined

Mode Global Config

5.4.9.4. no dhcp client vendor-id-option-string

This command is used to restore to default value.

Format no dhcp client vendor-id-option-string

Mode Global Config

5.4.9.5. show dhcp client vendor-id-option

This command is used to display the configured administration mode of the vendor-id-option and the vendor-id string to be included in DHCP requests.

Format show dhcp client vendor-id-option

Default None

Mode Privilege Exec

Display Message

Parameter	Definition
DHCP Client Vendor Identifier Option	The administration mode of the Vendor ID Option

DHCP Client Vendor Identifier Option String	The string to be included in the Vendor ID Option

5.4.9.6. show dhcp lease

This command is used to display the DHCP client lease parameters.

Format show dhcp lease [interface {<slot/port> | vlan <vlan-id>}]

Default None

Mode Privilege Exec

Display Message

Parameter	Definition
IP address	The IP address allocated by DHCP server and correspond interface.
Subnet mask	The IP subnet mask allocated by DHCP server for the interface.
DHCP lease server	The IPv4 address of the DHCP server that leased the address
State	The state of the DHCP client on this interface
DHCP transaction id	The transaction ID of the DHCP 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 DHCP client to renew the leased IP address
Rebind	The time (in seconds) when the DHCP Rebind process starts
Retry count	The number of times the DHCP client sends a DHCP REQUEST before the server responds

5.4.10. sFlow Commands

5.4.10.1. show sflow agent

The user can go to the CLI Privilege Exec to get the sFlow agent information, use the **show sflow agent** Privilege command.

Format show sflow agent

Default None

Mode Privilege Exec

Display Message

Parameter	Definition
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: Netgear. • Revision: The version of FW
IP Address	The IP address associated with this agent.

5.4.10.2. show sflow pollers

The user can go to the CLI Privilege Exec to get the sFlow polling instances created on the switch, use the **show sflow pollers** Privilege command.

Format show sflow pollers

Default None

Mode Privilege Exec

Display Message

Parameter	Definition
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.

5.4.10.3. show sflow receivers

The user can go to the CLI Privilege Exec to get the configuration information related to the sFlow receivers, use the **show sflow receivers** Privilege command.

Format show sflow receivers [< rcvr- index >]

Default None

Mode Privilege Exec

Display Message

Parameter	Definition

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.

5.4.10.4. show sflow samplers

The user can go to the CLI Privilege Exec to get the sFlow sampling instances created on the switch, use the **show sflow samplers** Privilege command.

Format show sflow samplers

Default None

Mode Privilege Exec

Display Message

Parameter	Definition
Sampler Data Source	The sFlowDataSrouce for this sFlow sampler. This agent supports 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.

5.4.10.5. show sflow source-interface

The user can go to the CLI Privilege Exec to get the configured source interface for sFlow, use the **show sflow source-interface** Privilege command.

Format show sflow source-interface

Default None

Mode Privilege Exec

Display Message

Parameter	Definition
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.

5.4.10.6. sflow receiver maximum datagram

Use this command to configure the sFlow collector maximum datagram size. This specifies 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 200-9312.

Format sflow receiver <index> maxdatagram <200-9312>

Default 1400

Mode Global Config

5.4.10.7. no sflow receiver maxdatagram <index>

Use the **no sflow receiver <index> maxdatagram** return to default value 1400.

Format no sflow receiver <index> maxdatagram

Mode Global Config

5.4.10.8. sflow receiver owner

Use this command to configure the sFlow collector owner string.

Format sflow receiver < index> owner <owner> {notimeout | timeout <0 - 2147483647>}

Parameter	Definition
<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.
notimeout	Entries configured with a notimeout entry will be in the running config until the user explicitly removes the entry.
<0 - 2147483647>	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.

Default None

Mode Global Config

5.4.10.9. no sflow receiver <index>

Use the **no sflow receiver <index>** to remove the session.

Format no sflow receiver <index> [owner]

Mode Global Config

5.4.10.10. sflow receiver ip

Use this command to assign an IPv4 address to the sFlow collector. When sFlow hardware sampling is enabled, the switch/hardware sends sampled packets encapsulated in sFlow custom packet to this IP address. If set to 0.0.0.0, no sFlow datagrams will be sent. The default is 0.0.0.0.

Format sflow receiver < index> ip <ip>

Default 0.0.0.0

Mode Global Config

5.4.10.11. no sflow receiver <index> ip

Use the **no sflow receiver <index> ip** to clear collector ip address.

Format no sflow receiver <index> ip

Mode Global Config

5.4.10.12. sflow receiver port

Use this command to configure the destination UDP port for the sFlow collector.

Format sflow receiver <index> port <1-65535>

Default 6343

Mode Global Config

5.4.10.13. no sflow receiver <index> port

Use the **no sflow receiver <index> port** return to default UDP port 6343.

Format no sflow receiver <index> port

Mode Global Config

5.4.10.14. sflow poller interval

Use this command to configure the sFlow instance polling interval. A poll interval of zero (0) disables counter sampling. 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. A value of N means once in N seconds a counter sample is generated.

Format sflow poller interval <0-86400>

Default 0

Mode Interface Config

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.

5.4.10.15. no sflow poller interval

Use the **no sflow poller interval** return to default value zero.

Format no sflow poller interval

Mode Interface Config

5.4.10.16. sflow sampler index

Use this command to configure a new sFlow sampler instance on an interface or a range of interfaces for this data source if the specified receiver is valid. A data source configured to collect flow samples is called a sampler. Flow samples for the sFlow sampler are sent to the sFlow receiver. Only active receivers can be set. If a receiver expires, then all samplers associated with the receiver will also expire. The range of <index> is 1-8.

Format sflow sampler <index>

Default None

Mode Interface Config

5.4.10.17. no sflow sampler

Use the **no sflow sampler** return to default setting.

Format no sflow sampler

Mode Interface Config

5.4.10.18. sflow poller index

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 a range of interfaces for this data source if the specified receiver is valid. The range of <index> is 1-8, which indicates the sFlow receiver associated with the poller.

Format sflow poller <index>

Default None

Mode Interface Config

5.4.10.19. no sflow poller

Use the **no sflow poller** return to default setting.

Format no sflow poller

Mode Interface Config

5.4.10.20. sflow source-interface

Use this command to specify the physical or logical routing 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 service port is configured as the source interface, sFlow packets will be transmitted via source port only. If the configured interface is down, the sFlow client falls back to normal behavior. User can go to the CLI Interface Configuration Mode to configure a new sFlow source interface, use the **sflow source-interface** global configuration command.

Format sflow source-interface {<slot/port> | loopback <loopback-id> | serviceport | tunnel <tunnel-id> | vlan <vlan-id>}

Parameter	Definition
<slot/port>	Specifies the interface 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 interface to use as the source interface. The range of the VLAN ID is 1 to 4093.
serviceport	Specifies the service port as the outgoing interface.

Default None

Mode Global Config

5.4.10.21. no sflow source-interface

Use the **no sflow source-interface** remove the source interface setting

Format no sflow source-interface

Mode Global Config

5.4.10.22. sflow sampler rate

Use this command to configure the statistical sampling rate for packet sampling from this source. 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 of

<rate> is 1024-65536 and 0.

Format sflow sampler rate <rate>

Default 0

Mode Interface Config

5.4.10.23. no sflow sampler rate

Use the **no sflow sampler rate** return to default setting.

Format no sflow sampler rate

Mode Interface Config

5.4.10.24. sflow sampler maxheadersize

Use this command to configure the maximum number of bytes that should be copied from the sampler packet. The range is 20-256. When set to zero (0), all the sampler parameters are set to their corresponding default value.

Format sflow sampler maxheadersize <size>

Default 128

Mode Interface Config

5.4.10.25. no sflow sampler maxheadersize

Use the **no sflow sampler maxheadersize** return to default setting.

Format no sflow sampler maxheadersize

Mode Interface Config

5.4.11. Service Port Commands

5.4.11.1. show serviceport

This command displays service port configuration information.

Format show serviceport

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
Interface Status	Indicates whether the interface is up or down.
IP Address	The IP address of the interface. The factory default value is 192.168.0.238.
Subnet Mask	The IP subnet mask for this interface. The factory default value is 255.255.255.0.
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 Prefix is	The IPv6 address and length. Default is Link Local format.
IPv6 Default Router	The default gateway address on the service port. The factory default value is an unspecified address.
Configured IPv4 Protocol	Indicate what IPv4 network protocol was used on the last, or current power-up cycle, if any.
Configured IPv6 Protocol	Indicate what IPv6 network protocol was used on the last, or current power-up cycle, if any.
IPv6 AutoConfig Mode	Whether IPv6 Stateless address autoconfiguration is enabled or disabled. Default value is disabled.
IPv6 Link-local Scope ID	The scope ID for this interface
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.

5.4.11.2. 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

Default None

Mode Privileged Exec

User Exec

Display Message

Parameter	Definition
DHCPv6 Advertisement Packets Received	The number of DHCPv6 Advertisement packets received on the network.
DHCPv6 Reply Packets Received	The number of DHCPv6 Reply packets received on the network interface.
Received DHCPv6 Advertisement Packets Discard	The number of DHCPv6 Advertisement packets discarded on the network.
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.

```
(M4500-32C) #show serviceport ipv6 dhcp statistics

DHCPv6 Client Statistics

-------------------------

DHCPv6 Advertisement Packets Received.......... 0

DHCPv6 Reply Packets Received.................. 0

Received DHCPv6 Advertisement Packets Discard.. 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
```

5.4.11.3. show serviceport ipv6 neighbors

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

Format show serviceport ipv6 neighbors

Default None

Mode Privileged Exec

User Exec

Display Message

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

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

```
(M4500-32C) #show serviceport ipv6 neighbors
```

```
Neighbor
Age

IPv6 Address                 Type     MAC Address         isRtr   State
(Secs)

---------------------------------- ----------------   -----   ---------
------

fe80::290:e8ff:feaa:35       Dynamic  00:90:e8:aa:00:35   True    Stale
3

fe80::a9e:1ff:feff:eed4      Dynamic  08:9e:01:ff:ee:d4   True    Stale
3
```

5.4.11.4. serviceport ip

This command sets the IP address, the netmask and the gateway of the service port. User can specify the none option to clear the Ipv4 address, mask, and the default gateway.

Format serviceport ip {<ipaddr> <netmask> [<gateway>] | none}

Parameter	Definition
<ipaddr>	The user manually configures the IP address for the switch.
<netmask>	The user manually configures the subnet mask for the switch.
<gateway>	The user manually configures the default gateway.
none	Resets the IP address, netmask, and default gateway.

Default None

Mode Global Config

5.4.11.5. 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 *dhcp* parameter, the switch periodically sends requests to a DHCP server until a response is received. If you use the *dhcp6* parameter, the switch periodically sends requests to a DHCPv6 server until a response is received. If you use the *none* parameter, you must configure the network information for the switch manually.

Format serviceport protocol {none [dhcp6] | dhcp [client-id | restart] | dhcp6 [restart]}

Parameter	Definition

none	Disable the DHCP client on the sevice port. Option **dhcp6** is used to disable the DHCPv6 client on the service port.
dhcp	Periodically sends requests to a DHCP server until a response is received. Option **client-id** is used to send DHCP client messages with the client identifier option (DHCP Option 61). Option **restart** is used to restart DHCP client.
dhcp6	Periodically sends requests to a DHCPv6 server until a response is received. Option **restart** is used to restart DHCPv6 client.

Default DHCP with client-id

Mode Global Config

5.4.11.6. serviceport ipv6 enable

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

Format serviceport ipv6 enable

Default Enabled

Mode Global Config

5.4.11.7. no serviceport ipv6 enable

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

Format no serviceport ipv6 enable

Mode Global Config

5.4.11.8. serviceport ipv6 address

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

i Multiple IPv6 prefixes can be configured on the service port.

Format serviceport ipv6 address {<address>/<prefix-length> [eui64] | autoconfig}

Parameter	Definition
<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.

Default None

Mode Global Config

5.4.11.9. no serviceport ipv6 address

This command removes all configured IPv6 prefixes on the service port interface. Use this command with the address option to remove the manually configured IPv6 global address. Use the command with the autoconfig option to disable the stateless global address autoconfiguration on the service port.

Format no serviceport ipv6 address [{<address>/<prefix-length> [eui64] | autoconfig}]

Mode Global Config

5.4.11.10. serviceport ipv6 gateway

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

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>

Default None

Mode Global Config

5.4.11.11. no serviceport ipv6 gateway

This command removes IPv6 gateways on the service port interface.

Format no serviceport ipv6 gateway

Mode Global Config

5.4.11.12. clear serviceport ipv6 dhcp statistics

This command clears IPv6 DHCP Statistics.

Format clear serviceport ipv6 dhcp statistics

Default None

Mode Privileged Exec

5.4.11.13. serviceport ipv6 neighbor

Use this command to configure IPv6 neighbor information for the service port.

Format serviceport ipv6 neighbor <ipv6-address><macaddr>

Default None

Mode Global Config

5.4.11.14. no serviceport ipv6 neighbor

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

Format no serviceport ipv6 neighbor <ipv6-address><macaddr>

Mode Global Config

5.4.12. Time Range Commands

5.4.12.1. 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 [<name>]

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
Admin mode	The administrative mode of time ranges for ACLs.
Current number of all Time Ranges	Number of time ranges configured on the switch.
Maximum number of all Time Ranges	The maximum number of time ranges can be configured.
Time Range Name	Name of the time range.
Time Range Status	Status of the time range (active/inactive).
Absolute Start Time	Start time and day for absolute time entry.
Absolute End Time	End time and day for absolute time entry.
Periodic Entries	Number of periodic entries in a time-range.
Periodic Start Time	Start time and day for periodic entry.
Periodic End Time	End time and day for periodic entry.

5.4.12.2. time-range

Use this command to enable or disable the time range Admin mode.

Format time-range

Default Enabled

Mode Global Config

5.4.12.3. no time-range

This command sets the time-range Admin mode to disable.

Format no time-range

Mode Global Config

5.4.12.4. time-range <name>

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

Format time-range <name>

Parameter	Definition
<name>	time range name.

Default None

Mode Global Config

5.4.12.5. no time-range <name>

This command deletes a time-range identified by name.

Format no time-range <name>

Mode Global Config

5.4.12.6. 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 <hh:mm> <1-31> <month> <1970-2035> [end <hh:mm> <1-31> <month> <1970-2035>] | end <hh:mm> <1-31> <month> <1970-2035>}

Default None

Mode Time-Range Config

5.4.12.7. no absolute

This command deletes the absolute time entry in the time range.

Format no absolute

Mode Time-Range Config

5.4.12.8. 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.

You can decide how often this perodic entry becomes active. If the value for <frequency> is set to 0, the option is disabled and a periodic entry becomes active only once.

Format periodic {{days-of-the-week time} to {[days-of-the-week] time} | <frequency>}

Default None

Mode Time-Range Config

5.4.12.9. 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} | <frequency>}

Mode Time-Range Config

5.4.13. Command Scheduler Commands

5.4.13.1. kron occurrence

Kron Occurrence is defined as a scheduled event. Policy lists are configured to run after a period of time since the scheduling was set, or at a specified calendar date and time.

Format kron occurrence <name> {at <hh:mm> {<1-31> <month> <2000-2037>| <DAY> {oneshot | recurring}| oneshot | recurring} | in <ddd:hh:mm> {oneshot | recurring}}

Parameter	Definition
<name>	Specifies an occurrence name.
at	Date of the kron occurrence.
<hh:mm>	Time of the day for the occurrence.
<1-31>	Day of the month.
<month>	Month of the year, for example, jan, feb, and so on.
<2000-2037>	Specifies the year.
<DAY>	Day of the week, for example, mon, tue, and so on.
oneshot	Schedule the kron occurrence exactly once.
recurring	Schedule the kron occurrence repeatedly.
in	Delta time to kron occurrence.
<ddd:hh:mm>	The day, hour, and minutes in the format ddd:hh:mm. The valid range is as follows: ddd: 0-999; hh: 0-23; mm: 0-59.

Default None

Mode Global Config

5.4.13.2. no kron occurrence <name>

This command deletes a scheduler event by the specific name.

Format no kron occurrence <name>

Mode Global Config

5.4.13.3. policy-list <name>

This command associates a policy list with an occurrence. When the occurrence is fired, the policy-list will be executed. Maximum 16 policy-lists could be added into an occurrence.

Format policy-list <name>

Default None

Mode Kron Occurrence Config

5.4.13.4. no policy-list <name>

This command dissociates the specified policy-list by name with the occurrence.

Format no policy-list <name>

Mode Kron Occurrence Config

5.4.13.5. kron policy-list

Policy lists consist of one or more lines of fully-qualified EXEC CLI commands. All commands in a policy list are executed when the policy list is run by Command Scheduler using the kron occurrence command.

The policy lists is run in the order in which it was configured. If an existing policy list name is used, new entries are added to the end of the policy list.

Format kron policy-list <name>

Parameter	Definition
<name>	Specifies a policy-list name.

Default None

Mode Global Config

5.4.13.6. no kron policy-list <name>

This command deletes a policy list by the specific name.

Format no kron policy-list <name>

Mode Global Config

5.4.13.7. cli <line><line><line> …

Specify the EXEC CLI commands to a policy list. Maximum 16 EXEC CLI commands could be added into a policy-list.

Format cli <LINE> <LINE> <LINE> ...

Parameter	Definition
<LINE>	Exec level cli to be executed.

Default None

Mode Kron Policy-list Config

5.4.13.8. no cli <line> <line> <line> …

This command deletes a list of CLI command lines.

Format no cli <LINE> <LINE> <LINE> ...

Mode Kron Policy-list Config

5.4.14. 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.

5.4.14.1. show sdm prefer

Use this command to display the current active SDM template and its scaling parameters, or to display the scaling parameters for an inactive template. When invoked with no optional keywords, this command lists the current active template and the template that will become active on the next reboot if it is different from the current active template. To list the scaling parameters of a specific template, use that template's keyword as an argument to the command.

Format show sdm prefer [dual-ipv4-and-ipv6 {alpm | data-center | dcvpn-data-center | default} | ipv4-routing {data-center {default | plus} | dcvpn-data-center | default}]

Default None

Mode Privileged Exec

Options

Parameter	Definition
dual-ipv4-and-ipv6 alpm	(Optional) Lists the scaling parameters for the alpm template.
dual-ipv4-and-ipv6 data-center	(Optional) Lists the scaling parameters for the Dual IPv4 and IPv6 template supporting more ECMP next hops.
dual-ipv4-and-ipv6 dcvpn-data-center	(Optional)Lists the scaling parameters for the Dual IPv4 and IPv6 template for the DCVPN feature.
dual-ipv4-and-ipv6 default	(Optional) Lists the scaling parameters for the template supporting IPv4 and IPv6.
ipv4-routing data-center default	(Optional) Lists the scaling parameters for the IPv4-only template supporting more ECMP next hops.
ipv4-routing data-center plus	(Optional) Lists the scaling parameters for the IPv4-only template maximizing the number of unicast routes and also supporting more ECMP next hops.
ipv4-routing dcvpn-data-center	(Optional) Lists the scaling parameters for the IPv4-only template for DCVPN feature.
ipv4-routing default	(Optional) Lists the scaling parameters for the IPv4-only template maximizing the number of unicast routes.

Display Message

Parameter	Definition
ARP Entries	Maximum number of ARP entries supported in a specific SDM template.
IPv4 Unicast Routes	Maximum number of IPv4 routes supported in a specific SDM template.
IPv6 NDP Entries	Maximum number of NDP entries supported in a specific SDM template.
IPv6 Unicast Routes	Maximum number of IPv6 routes supported in a specific SDM template.
ECMP Next Hops	Maximum number of ECMP next hops supported in a specific SDM template.
IPv4 Multicast Routes	Maximum number of IPv4 multicast routes supported in a specific SDM template.
IPv6 Multicast Routes	Maximum number of IPv6 multicast routes supported in a specific SDM template.

5.4.14.2. sdm prefer

Use this command to change the template that will be active after the next reboot.

Format sdm perfer {dual-ipv4-and-ipv6 {alpm | data-center | dcvpn-data-center | default} | ipv4-routing {data-center {default | plus}| dcvpn-data-center | default}}

Parameter	Definition
dual-ipv4-and-ipv6 alpm	Accommodate larger routes.
dual-ipv4-and-ipv6 data-center	Increase the number of ECMP next hops in each route to 32 and reduce the number of IPv4 and IPv6 unicast routes.
dual-ipv4-and-ipv6 dcvpn-data-center	Maximize the number of IPv4 and IPv6 unicast routes while supporting DCVPN feature.
dual-ipv4-and-ipv6 default	Maximize the number of IPv4 and IPv6 unicast routes while limiting the number of ECMP next hops in each route to 4.
ipv4-routing data-center default	Increase the number of ECMP next hops to 32 and reduce the number of IPv4 routes.
ipv4-routing data-center plus	Increase the number of ECMP next hops to 32 while keeping the maximum IPv4 routes.
ipv4-routing dcvpn-data-center	Maximize the number of IPv4 unicast routes while supporting DCVPN feature.
ipv4-routing default	Maximize the number of IPv4 unicast routes while limiting the number of ECMP next hops in each route to 4.

Default dual-ipv4-and-ipv6 alpm

Mode Global Config

5.4.14.3. no sdm prefer

This command reverts to the default template after the next reboot.

Format no sdm prefer

Mode Global Config

5.4.15. 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.

5.4.15.1. show rmon alarms

This command displays the entries in the RMON alarm table.

Format show rmon {alarms | alarm <index>}

Mode Privileged EXEC

Display Message

Fields	Definition
index	An index that uniquely identifies an entry in the table. Each entry defines a diagnostic sample at a particular interval for an object on the device. The range is 1 to 65535.
OID	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of integer.
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.
Sample Type	The value of the statistic during the last sampling period. This object is a read-only, 32-bit signed value.
rising threshold	The rising threshold for the sample statistics. The range is 2147483648 to 2147483647. The default is 1.
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.
falling threshold	The falling threshold for the sample statistics. The range is 2147483648 to 2147483647. The default is 1.
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.
startup alarm	The alarm that may be sent. Possible values are rising, falling or both rising-falling. The default is rising- falling.
owner	The owner string associated with the entry. The default is monitorAlarm.

Example:

```
(M4500-48XF8C) #show rmon alarms

Index  OID                        Owner

-----  -------------------------  ----------------------------------------

1      alarmInterval.1            mibbrowser
```

```
(M4500-48XF8C) #show rmon alarm 1

Alarm 1

----------

OID: alarmInterval.1

Last Sample Value: 5

Interval: 5

Sample Type: absolute

Startup Alarm: rising-falling

Rising Threshold: 100

Falling Threshold: 10

Rising Event: 1

Falling Event: 2

Owner: mibbrowser
```

5.4.15.2. 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

Display Message

Fields	Definition
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.
interface	The source interface for which historical data is collected.
interval	The interval in seconds over which the data is sampled. The range is 1 to 3600. The default is 1800.
requested samples	The requested number of discrete time intervals over which data is to be saved. The range is 1 to 65535. The default is 50.
granted samples	The number of discrete sampling intervals over which data shall be saved. This object is read-only. The default is 10.

owner	The owner string associated with the entry. The default is monitorHistoryControl.

Example:

```
(M4500-48XF8C) #show rmon collection history

Index   Interface    Interval   Requested   Granted     Owner
                                 Samples     Samples
-----   ---------    --------   ---------   -------     ----------------------
1       0/1          30         50          10          monitorHistoryControl
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

--More-- or (q)uit


(M4500-48XF8C) #show rmon collection history interfaces 0/1

Index   Interface    Interval   Requested   Granted     Owner
                                 Samples     Samples
-----   ---------    --------   ---------   -------     ----------------------
1       0/1          30         50          10          monitorHistoryControl
        0/1          1800       50          10          monitorHistoryControl
```

5.4.15.3. show rmon events

This command displays the entries in the RMON event table.

Format show rmon events

Mode Privileged EXEC

Display Message

Fields	Definition
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.
description	A comment describing the event entry. The default is alarmEvent.
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.
community	The SNMP community specific by this octet string which is used to send an SNMP trap. The default is public.
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:

```
(M4500-48XF8C) #show rmon events

Index   Description       Type      Community   Owner         Last time sent

-----   ---------------   --------  ----------  ---------     --------------------

1       test              log       public      monitorEvent  May 04 2020 01:04:35
```

5.4.15.4. show rmon history

This command displays the specified entry in the RMON history table.

Format show rmon history <index> {errors | other | throughput} [period <seconds>]

Mode Privileged EXEC

Display Message

Fields	Definition
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 (interval) 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	Total number of undersize packets. Packets are less than 64 octets long (excluding framing bits, including FCS octets).
Oversize	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 Other Parameter	
Time	Time at which the sample is collected, displayed as period seconds.
Dropped Collisions	Total number of dropped collisions.
Output for Throughput Parameter	
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.

Example:

```
(M4500-48XF8C) #show rmon history 1 errors

Sample set: 1   Owner: monitorHistoryControl

Interface: 0/1   Interval: 30

Requested Samples: 50   Granted Samples: 10

Maximum table size: 630

Time                  CRC Align  Undersize Oversize  Fragments  Jabbers

--------------------  ---------  --------- --------  ---------  -------

May 06 2020 07:03:43  0          0         0         0          0

May 06 2020 07:04:13  0          0         0         0          0

May 06 2020 07:04:44  0          0         0         0          0

May 06 2020 07:05:14  0          0         0         0          0

May 06 2020 07:05:44  0          0         0         0          0

May 06 2020 07:06:14  0          0         0         0          0

May 06 2020 07:06:44  0          0         0         0          0

May 06 2020 07:07:14  0          0         0         0          0

May 06 2020 07:07:44  0          0         0         0          0

May 06 2020 07:08:15  0          0         0         0          0


(M4500-48XF8C) #show rmon history 1 other

Sample set: 1   Owner: monitorHistoryControl

Interface: 0/1   Interval: 30

Requested Samples: 50   Granted Samples: 10

Maximum table size: 630

Time                  Dropped Collisions

--------------------  ------- ----------

May 06 2020 07:04:13 0       0

May 06 2020 07:04:44 0       0

May 06 2020 07:05:14 0       0
```

```
May 06 2020 07:05:44 0       0

May 06 2020 07:06:14 0       0

May 06 2020 07:06:44 0       0

May 06 2020 07:07:14 0       0

May 06 2020 07:07:44 0       0

May 06 2020 07:08:15 0       0

May 06 2020 07:08:45 0       0


(M4500-48XF8C) #show rmon history 1 throughput

Sample set: 1   Owner: monitorHistoryControl

Interface: 0/1   Interval: 30

Requested Samples: 50   Granted Samples: 10

Maximum table size: 630

Time                 Octets     Packets   Broadcast Multicast  Util

-------------------- ------     -------   --------- ---------  ----

May 06 2020 07:04:13 0          0         0         0          0

May 06 2020 07:04:44 0          0         0         0          0

May 06 2020 07:05:14 0          0         0         0          0

May 06 2020 07:05:44 0          0         0         0          0

May 06 2020 07:06:14 0          0         0         0          0

May 06 2020 07:06:44 0          0         0         0          0

May 06 2020 07:07:14 0          0         0         0          0

May 06 2020 07:07:44 0          0         0         0          0

May 06 2020 07:08:15 0          0         0         0          0

May 06 2020 07:08:45 0          0         0         0          0
```

5.4.15.5. show rmon log

This command displays the entries in the RMON log table.

Format show rmon log [<event-index>]

Mode Privileged EXEC

Display Message

Fields	Definition
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:

```
(M4500-48XF8C) #show rmon log

Event   Description                   Time

-----   ---------------------------   --------------------


(M4500-48XF8C) #show rmon log 1

Maximum table size: 10

Event   Description                   Time

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

5.4.15.6. show rmon statistics interfaces

This command displays the RMON statistics for the given interfaces.

Format show rmon statistics interfaces <slot/port>

Mode Privileged EXEC

Display Message

Fields	Definition
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).

Example:

```
(M4500-48XF8C) #show rmon statistics interfaces 0/1

Port: 0/1

Dropped: 0

Octets: 772245  Packets: 6477

Broadcast: 0  Multicast: 6477

CRC Align Errors: 0  Collisions: 0

Undersize Pkts: 0  Oversize Pkts: 0

Fragments: 0  Jabbers: 0

64 Octets: 414  65 - 127 Octets: 6063

128 - 255 Octets: 0  256 - 511 Octets: 0

512 - 1023 Octets: 0  1024 - 1518 Octets: 0

HC Overflow Pkts: 0  HC Pkts: 6477

HC Overflow Octets: 0  HC Octets: 772245

HC Overflow Pkts 64 Octets: 0  HC Pkts 64 Octets: 414
```

```
HC Overflow Pkts 65 - 127 Octets: 0  HC Pkts 65 - 127 Octets: 6063

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
```

5.4.15.7. show rmon hcalarms

This command displays the entries in the RMON high-capacity alarm table.

Format show rmon { hcalarms | hcalarm <index>}

Mode Privileged EXEC

Display Message

Fields	Definition
Index	An arbitrary integer index value used to uniquely identify the high capacity alarm entry. The range is 1 to 65535.
OID	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of integer.
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.
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.
Startup Alarm	
Rising Threshold 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.
Rising Threshold 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.
Rising Threshold 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.
Falling Threshold 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.

Falling Threshold 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.
Falling Threshold 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.
Rising Event	The index of the eventEntry that is used when a rising threshold is crossed. The range is 1 to 65535. The default is 1.
Falling Event	The index of the eventEntry that is used when a falling threshold is crossed. The range is 1 to 65535. The default is 2.
Startup Alarm	Alarm that sent when the entry is enabled. The default is rising-falling.
Owner	The owner string associated with the alarm entry. The default is monitorHCAlarm.

Example:

```
(M4500-48XF8C) #show rmon hcalarms

Index  OID                        Owner

-----  -------------------------  ------------------------------------------

1      alarmInterval.1            monitorHCAlarm


(M4500-48XF8C) #show rmon hcalarm 1

Alarm 1

----------

OID: alarmInterval.1

Last Sample Value: 5

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: monitorHCAlarm
```

5.4.15.8. rmon alarm

This command sets the RMON alarm entry in the RMON alarm MIB group.

Format rmon alarm <index> <variable> <interval> {absolute | delta} rising-threshold <rising threshold> [<rising event index>] falling-threshold <falling threshold> [<falling event index>] [startup {rising | falling | rising-falling}] [owner <owner string>]

Default None

Mode Global Config

Parameter	Description
index	An index that uniquely identifies an entry in the table. Each entry defines a diagnostic sample at a particular interval for an object on the device. The rage is 1 to 65535.
variable	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of integer.
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.
absolute	The value of the statistic during the last sampling period. This object is a read-only, 32-bit signed value.
rising threshold	The rising threshold for the sample statistics. The range is -2147483648 to 2147483647. The default is 1.
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.
falling threshold	The falling threshold for the sample statistics. The range is -2147483648 to 2147483647. The default is 1.
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.
{rising | falling | rising-falling}	The alarm that may be sent. Possible values are rising, falling or both rising-falling. The default is rising-falling.

owner string	The owner string associated with the entry. The default is monitorAlarm.

Example:

```
(M4500-48XF8C) (Config)#rmon alarm 1 ifInErrors.2 30 absolute rising-threshold 100
1 falling-threshold 10 2 startup rising owner myOwner
```

5.4.15.9. no rmon alarm

This command deletes the RMON alarm entry

Format

Mode Global Config

5.4.15.10. rmon hcalarm

This command sets the RMON hcalarm entry in the High Capacity RMON alarm MIB group.

Format rmon hcalarm <index> <variable> <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 <owner string>]

Default None

Mode Global Config

Parameter	Description
index	An arbitrary integer index value used to uniquely identify the high capacity alarm entry. The range is 1 to 65535.
variable	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of integer.
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.
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.
rising-threshold value high	The lower 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 1.

rising-threshold value low	The upper 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 0.
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.
falling-threshold value high	The lower 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 1.
rising-threshold value low	The upper 32 bits of the absolute value for threshold for the sampled statistic. The range is 0 to 4294967295. The default is 0.
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.
rising 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.
owner string	The owner string associated with the alarm entry. The default is monitorHCAlarm.

Example:

```
(M4500-48XF8C) (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
```

5.4.15.11. no rmon hcalarm

This command deletes the RMON hcalarm entry

Format no rmon hcalarm <index>

Mode Global Config

5.4.15.12. rmon event

This command sets the RMON event entry in the RMON event MIB group.

Format rmon event <event number> [description <string> | log | owner <owner string> | trap <community>]

Default None

Mode Global Config

Parameter	Description
event number	An number 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.
string	A comment describing the event entry. The default is alarmEvent.
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.
owner string	Owner string associate with the entry. The default is monitorEvent.
community	The SNMP community specific by this octet string which is used to send an SNMP trap. The default is public.

Example:

```
(M4500-48XF8C) (Config)# rmon event 1 log description test
```

5.4.15.13. no rmon event

This command deletes the rmon event entry.

Format no rmon event <event number>

Mode Global Config

5.4.15.14. 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> [buckets <number> | interval <interval> | owner <owner string>]

Default None

Mode Interface Config

Parameter	Description
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 the 65535.

number	The requested number of discrete time intervals over which data is to be saved The range is 1 to 65535. The default is 50.
interval	The interval in seconds over which the data is sampled. The range is 1 to 3600. The default is 1800.
owner string	The owner string associated with the entry. The default is monitorHistoryControl.

Example:

```
(M4500-48XF8C) (Interface 0/1)#rmon collection history 1 buckets 10 interval 30
owner myOwner
```

5.4.15.15. no rmon collection history

This command will delete the history control group entry with the specified index number.

Format no rmon collection history <index>

Mode Interface Config

5.4.16. Statistics Application Commands

The statistics application lets you query port utilization statistics, flow-based statistics, and packet reception statistics 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 an absolute time entry, a periodic time, or both. 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.

5.4.16.1. 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} tierange time <range name> reporing list of reporting methods
no stats group group {id | name}

Mode Global Config

Parameter	Definition
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 from 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

(Routing) (Config)# no stats group received

(Routing) (Config)# no stats group received-errors

(Routing) (Config)# no stats group received-transmitted
```

5.4.16.2. 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} {srccppor portid} {dsttcpport portid} {srcudpport portid} {dstudpprt portid}]

no stats flow-based <rule-id>

Mode Global Config

Parameter	Definition
Rule ID	The flow-base 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 from 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. The range is 1 to 65535.
Dsttcpport portid	Configure the destination TCP port for the rule. The range is 1 to 65535.
Srcudpport portid	Configure the source UDP port for the rule. The range is 1 to 65535.
Dstudpport portid	Configure the destination UDP port for the rule. The range is 1 to 65535.

Example:s

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

(Routing) (Config)# no stats flow-based 1

(Routing) (Config)# no stats flow-based 2
```

5.4.16.3. 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
```

5.4.16.4. stats group (Interface Config)

This command applies the group specified on an interface or interface-range.

Format stats group {group-id | name}
no stats group {group-id | name}

Mode Interface Config

Parameter	Definition
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.

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

(Routing) (Interface 0/1-0/10)# no stats group 1

(Routing) (Interface 0/1-0/10)# no stats group 2
```

5.4.16.5. 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>
no stats flow-based <rule-id>

Mode Interface Config

Parameter	Definition
Rule ID	The flow-base 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
```

5.4.16.6. 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	Definition
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) #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


(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
```

5.4.16.7. 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	Definition
Rule ID	The flow-base rule ID. The range is 1 to 16. The default is None.

Example:

The following shows examples of 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

(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
```

5.5. 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: STP is enabled on the switch and on all ports and LAGs by default.

Note: If STP is disabled, the system does not forward BPDU messages.

5.5.1. 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

Display Message

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 in progress	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
Bridge Max Age	Maximum message age.
Bridge Max Hops	The maximum number of hops for the spanning tree.
Max Tx Hold Count	The max value of bridge tx hold count for the spanning tree.
Bridge Forwarding Delay	A timeout value to be used by all Bridges in the Bridged LAN. The value of Forward Delay is set by the Root.
Hello Time	Configured value of the parameter for the CST.
Bridge Hold Time	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).
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.

5.5.2. 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> is the desired switch port. The following details are displayed on execution of the command.

Format show spanning-tree interface {<slot/port> | port-channel <portchannel-id>}

Mode Privileged EXEC

User EXEC

Display Message

Parameter	Definition
Hello Time	Admin hello time for this port.
Port Mode	Enabled or disabled.
BPDU Guard	Enabled or disabled BPDU Guard
BPDU Guard Effect	The effect of BPDU Guard when the BPDU Guard is enabled
Root Guard	Enabled or disabled Root Guard
Loop Guard	Enabled or disabled Loop Guard
TCN Guard	Enabled or disabled TCN Guard
Auto Edge	Enabled or disabled 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.

5.5.3. show spanning-tree vlan

This command displays the association between a VLAN and a multiple tree instance. The <vlan-id> corresponds to an existing VLAN ID. The <vlan-id> range is 1 to 4093.

Format show spanning-tree vlan <vlan-id>

Default None

Mode Privileged EXEC

User EXEC

Example: The following example shows the CLI display output for the command show spanning-tree vlan1.

```
M4500-32C) #show spanning-tree vlan 1
```

```
VLAN Identifier.............................. 1

Associated Instance.......................... CST
```

5.5.4. show spanning-tree mst detailed

This command displays the detailed settings for an MST instance. The instance <0-4094> is a number that corresponds to the desired existing multiple spanning tree instance ID. The following details are displayed.

Format show spanning-tree mst detailed <mstid>

Mode Privileged EXEC

User EXEC

Display Message

Parameter	Definition
MST Instance ID	The multiple spanning tree instance ID.
MST Bridge Priority	The bridge priority of current MST.
MST Bridge Identifier	The bridge ID of current MST.
Time Since Topology Change	In seconds.
Topology Change Count	Number of times the topology has changed for this multiple spanning tree instance.
Topology Change in progress	Value of the Topology Change parameter for the multiple spanning tree instance.
Designated Root	Identifier of the Regional Root for this multiple spanning tree instance.
Root Path Cost	Path Cost to the Designated Root for this multiple spanning tree instance.
Root Port Identifier	Port to access the Designated Root for this multiple spanning tree instance.
Associated FIDs	List of forwarding database identifiers associated with this instance.
Associated VLANs	List of VLAN IDs associated with this instance.

5.5.5. 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

Display Message

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.

5.5.6. 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> is the desired switch port.

Format show spanning-tree mst port detailed <mstid> {<slot/port> | port-channel <portchannel-id>}

Mode Privileged EXEC

User EXEC

Display Message

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.
Designated Port Cost	Path Cost offered to the LAN by the Designated Port.
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.

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.
Designated Port Cost	Path Cost offered to the LAN by the Designated 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 MSTP loop inconsistent state of the port in a specific instance.
Transitions Into Loop Inconsistent State	The number of times this interface has transitioned into the MSTP loop inconsistent state.
Transitions Out Of Loop Inconsistent State	The number of times this interface has transitioned out of the MSTP loop inconsistent state.

5.5.7. 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 <misted> range is 0 to 4096. The parameter <slot/port> indicates the desired switch port.

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> | active | port-channel <portchannel-id>}]

Mode Privileged EXEC

User EXEC

Display Message

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.

5.5.8. 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

Display Message

Parameter	Definition
Spanning Tree Admin mode	Enabled or disabled.
Spanning Tree Forward BPDU	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.
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.

5.5.9. 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

Display Message

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).

5.5.10. spanning-tree

This command sets the spanning-tree operational mode to enabled.

Note: If the MST is enabled with MLAG, MST must be enabled on both MLAG peer devices.

Format spanning-tree

Default Enabled

Mode Global Config

5.5.11. 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

5.5.12. spanning-tree bpdu-forwarding

This command sets the BPDU forwarding mode.

Format spanning-tree bpdu-forwarding

Default Enabled

Mode Global Config

5.5.13. no spanning-tree bpdu-forwarding

This command sets the BPDU forwarding mode to disabled.

Format no spanning-tree bpdu-forwarding

Mode Global Config

5.5.14. spanning-tree protocol-migration

This command enables BPDU migration check on a given interface. The all option enables BPDU migration check on all interfaces.

Format spanning-tree protocol-migration {<slot/port> | port-channel <portchannel-id> | all}

Default None

Mode Global Config

5.5.15. 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.

Note: **If the MST is enabled with MLAG, the Configuration Identifier Name must be the same on both MLAG peer devices.**

Format spanning-tree configuration name <name>

Default Base MAC address in hexadecimal notation

Mode Global Config

5.5.16. no spanning-tree configuration name

This command sets the Configuration Identifier Name to “DEFAULT”.

Format no spanning-tree configuration name

Mode Global Config

5.5.17. 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.

Format spanning-tree configuration revision <0-65535>

Default 0

Mode Global Config

5.5.18. 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

5.5.19. spanning-tree mode

This command configures global spanning tree mode per VLAN spanning tree. On a switch, only one mode can be enabled at a time.

Note: Both RSTP and MSTP can be enabled with MLAG. The configuration of RSTP and MSTP on peers of MLAG must be the same to guarantee that MLAG can work correctly. If you configure one peer of MLAG as RSTP, the other peer must be RSTP. The same as MSTP.

Format spanning-tree mode {mstp | rstp}

Default mstp

Mode Global Config

5.5.20. no spanning-tree mode

This command globally configures the switch to the default spanning-tree mode, MSTP.

Format no spanning-tree mode

Mode Global Config

5.5.21. 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”.

Format spanning-tree forward-time <4-30>

Default 15

Mode Global Config

5.5.22. 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

5.5.23. 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 times (Bridge Forward Delay - 1)” and greater than or equal to “2 times (Bridge Hello Time + 1)”.

Format spanning-tree max-age <6-40>

Default 20

Mode Global Config

5.5.24. 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

5.5.25. spanning-tree forward-time max-age

This command sets the Bridge Forward Delay and Max Age parameter to a new value for the common and internal spanning tree.

Format spanning-tree forward-time <4-30> max-age <6-40>

Default forward-time: 15

max-age: 20

Mode Global Config

5.5.26. 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 6 to 40.

Format spanning-tree max-hops <6-40>

Default 20

Mode Global Config

5.5.27. 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

5.5.28. spanning-tree hold-count

This command sets the Bridge Tx Hold Count parameter to a new value for the common and internal spanning tree. The Tx Hold Count value is in a range of 1 to 10.

Format spanning-tree hold-count <1-10>

Default 6

Mode Global Config

5.5.29. no spanning-tree hold-count

This command sets the Bridge Tx Hold Count parameter for the common and internal spanning tree to the default value.

Format no spanning-tree hold-count

Mode Global Config

5.5.30. 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.

Format spanning-tree mst instance <mstid>

Default None

Mode Global Config

5.5.31. 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

5.5.32. spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance. The parameter mstid <0-4094> 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.

Format spanning-tree mst priority <mstid> <0-61440>

Default 32768

Mode Global Config

5.5.33. 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 <0-4094> 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

5.5.34. 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 <0-4094> is a number that corresponds to the desired existing multiple spanning tree instance. The vlan-list 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> <vlan-list>

Mode Global Config

5.5.35. 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> <vlan-list>

Mode Global Config

5.5.36. 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 <0-4094> 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.

Note: **If the MST is enabled with MLAG, the path cost of the MLAG peer-link cannot be modified.**

Format spanning-tree mst <mstid> {{cost <1-200000000> | auto} | port-priority <0-240>}

Default cost: auto

port-priority: 128

Mode Interface Config

5.5.37. 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 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

5.5.38. spanning-tree port mode

This command sets the Administrative Switch Port State for this port to enabled.

Format spanning-tree port mode

Default Enabled

Mode Interface Config

5.5.39. 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

5.5.40. spanning-tree port model all

This command sets the Administrative Switch Port State for all ports to enabled.

Format spanning-tree port mode all

Default Enabled

Mode Global Config

5.5.41. 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

5.5.42. spaning-tree auot-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.

Format spanning-tree auto-edge

Default Enabled

Mode Interface Config

5.5.43. 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

5.5.44. 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.

Note: If the MST is enabled with MLAG, the path cost of the MLAG peer-link cannot be modified.

Format spanning-tree cost {<cost> | auto}

Default Auto

Mode Interface Config

5.5.45. no spanning-tree cost

This command resets the path cost to the default value.

Format no spanning-tree cost

Mode Interface Config

5.5.46. spanning-tree edgeport

This command specifies that an interface 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

5.5.47. 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

5.5.48. spanning-tree edgeport bpduguard

This command sets the Edgeport BPDU Guard enable/disable parameter on this switch.

Format spanning-tree edgeport bpduguard

Default Disabled

Mode Global Config

5.5.49. no spanning-tree edgeport bpduguard

This command sets the Edgeport BPDU Guard to the default value that is disabled.

Format no spanning-tree edgeport bpduguard

Mode Global Config

5.5.50. spanning-tree bpduguard

Use this command to enable BPDU Guard on an interface.

Format spanning-tree bpduguard

Default Disabled

Mode Interface Config

5.5.51. no spanning-tree bpduguard

Use this command to disable BPDU Guard on the interface.

Format no spanning-tree bpduguard

Mode Interface Config

5.5.52. spanning-tree guard

Use this command to select whether loop guard or root guard is enabled on an interface or range of interfaces.

Format spanning-tree guard {loop | root}

Parameter	Definition
loop	This command sets the Guard Mode to loop guard on this interface.
root	This command sets the Guard Mode to root guard on this interface.

Default Disabled

Mode Interface Config

5.5.53. no spanning-tree guard

Use this command to disable loop guard or root guard on the interface.

Format no spanning-tree guard

Mode Interface Config

5.5.54. 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.

Format spanning-tree tcnguard

Default Enabled

Mode Interface Config

5.5.55. no spanning-tree tcnguard

Use this command to reset the TCN guard status of the port to the default value.

Format no spanning-tree tcnguard

Mode Interface Config

5.6. System Log Commands

5.6.1. show logging

This command displays configurations of logging application.

Format show logging

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show logging

Logging Client Local Port           : 514
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             : user

Terminal Monitor                    : disabled
Terminal Logging Severity Filter    : warning

Log Messages Received               : 139
Log Messages Dropped                : 0
Log Messages Relayed                : 0

Log Command Messages Received       : 2

(M4500-32C) #
```

5.6.2. show logging buffered

This command displays the log messages which record system operating and tracing information. The log buffered messages store in memory, therefore, it isn’t retained across a switch reset.

Format show logging buffered

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show logging buffered

Buffered (In-Memory) Logging        : enabled
Buffered Logging Wrapping Behavior  : On
Buffered Log Count                  : 33

Apr 28 19:35:09: %1-6-NIM: [396203556] nim_rif.c(352) 117 %% Set expandable port 0/50 count
set to 1
Apr 28 19:35:09: %1-6-NIM: [396203556] nim_rif.c(352) 116 %% Set expandable port 0/49 count
set to 1
Apr 28 19:35:05: %1-5-TRAPMGR: [397164180] traputil.c(797) 115 %% Temperature state change
alarm: Unit Number: 1 Current: Normal, Previous: None
Apr 28 19:34:59: %1-5-TRAPMGR: [396792620] traputil.c(755) 114 %% Succeeded User Login:
Console started for user admin connected from EIA-232.
Apr 28 19:34:57: %1-5-TRAPMGR: [396792620] traputil.c(755) 113 %% Entity Database:
Configuration Changed
Apr 28 19:34:52: %1-2-General: [1212183788] Boot!(0) 112 %% Event(0xaaaaaaaaa)
Apr 28 19:34:52: %1-6-AUTO_INST: [1212183788] auto_install_control.c(1374) 111 %% AutoInstall
is stopped.
Apr 28 19:34:52: %1-5-SIM: [1212183788] sim_util.c(3841) 110 %% Switch firmware operational:
LY8, Runtime Code 5.4.01.10, Linux 3.8.13-rt9, U-Boot 2010.12 (Oct 03 2014 - 14:38:07) - ONIE
2014.05.03-7
Apr 28 19:34:52: %1-5-TRAPMGR: [396792620] traputil.c(755) 109 %% Link Down: VLAN- 1
Apr 28 19:34:52: %1-5-SIM: [1212183788] sim_svc_port.c(334) 108 %% Service port IPv4 address
has been set to 192.168.2.10.
Apr 28 19:34:52: %1-5-SIM: [1212183788] sim_svc_port.c(334) 107 %% Service port IPv4 address
has been set to 0.0.0.0.
Apr 28 19:34:52: %1-6-CLI_WEB: [1212183788] sysapi.c(2844) 106 %% Configuration file
<startup-config> read from flash!
Apr 28 19:34:51: %1-5-IP: [396819460] openr_policy.c(1438) 99 %% Added RPPI routing policy
client ospf:0.
Apr 28 19:34:51: %1-6-CLI_WEB: [1212183788] cli_txtcfg.c(542) 98 %% Configuration applied
from file <startup-config>
Apr 28 19:34:51: %1-6-CLI_WEB: [1212183788] sysapi.c(2844) 97 %% Configuration file <startup-
config> read from flash!
Apr 28 19:34:50: %1-6-General: [1209039980] procmgr.c(800) 94 %% Application Started
(opensshd, ID = 8, PID = 936
Apr 28 19:34:50: %1-5-General: [1209039980] procmgr.c(2436) 93 %% Administrative Command:app-
start opensshd
Apr 28 11:34:49: %1-6-DOT3AD: [396784740] dot3ad_cnfgr.c(1192) 20 %% Tech Support
Registration failed for DOT3AD related commands
Apr 28 11:34:45: %1-6-General: [1209039980] procmgr.c(800) 19 %% Application Started
(traceroute-0, ID = 12, PID = 916
Apr 28 11:34:45: %1-5-General: [1209039980] procmgr.c(2436) 18 %% Administrative Command:app-
start traceroute-0
Apr 28 11:34:45: %1-6-General: [1209039980] procmgr.c(800) 17 %% Application Started (ping-0,
ID = 11, PID = 909
Apr 28 11:34:45: %1-5-General: [1209039980] procmgr.c(2436) 16 %% Administrative Command:app-
start ping-0
Apr 28 11:34:44: %1-5-OSAPI: [1289614252] osapi_monitor.c(145) 15 %% Watchdog timer is
started.
Apr 28 11:34:44: %1-6-General: [1209039980] procmgr.c(800) 14 %% Application Started (ospf-
00, ID = 10, PID = 851
Apr 28 11:34:44: %1-5-General: [1209039980] procmgr.c(2436) 13 %% Administrative Command:app-
start ospf-00 0
Apr 28 11:34:44: %1-6-General: [1209039980] procmgr.c(800) 12 %% Application Started (vr-
agent-0, ID = 9, PID = 845
Apr 28 11:34:44: %1-5-General: [1209039980] procmgr.c(2436) 10 %% Administrative Command:app-
start vr-agent-0
Apr 28 11:34:44: %1-6-VR_AGENT: [1289691836] vr_agent_api.c(73) 7 %% initialized the clnt
addr:/tmp/fpcvragent.00,family:1
Apr 28 11:34:43: %1-1-SIM: [1289691836] sim_util.c(3877) 5 %% Switch was reset due to
operator intervention.
Apr 28 11:34:43: %1-5-BSP: [396148460] bootos.c(178) 4 %% BSP initialization complete,
starting switch firmware.
```

```
Apr 28 11:34:35: %1-5-General: [396148460] sdm_template_mgr.c(494) 3 %% Booting with default
SDM template Data Center - IPv4 and IPv6.
Apr 28 11:34:34: %1-6-General: [1209039980] procmgr.c(3677) 2 %% Application Terminated
(user.start, ID = 7, PID = 686
Apr 28 11:34:33: %1-1-General: [396148460] usmdb_sim.c(3921) 1 %% Reboot 1 (0x1)

(M4500-32C) #
```

5.6.3. logging buffered

This command is used to enable or disable logging to the in-memory log. If the log buffer is full, the log wrap around.

Format [no] logging buffered

Default Enabled

Mode Global Config

5.6.4. logging buffered threshold

This command is used to configure the threshold of the logging buffer. The range of the threshold is from 1 to 100 percent. The threshold mode and wraparound mode are mutually exclusive. When you configure the threshold, logs do not wrap around. When you set a threshold value, the switch sends an alert when the threshold is exceeded. When the maximum capacity of the log is reached, logging stops. If you configured an email alert for this event, the switch sends an email.

Format [no] logging buffered threshold <1-100>

Default 100

Mode Global Config

5.6.5. logging buffered severity level

This command sets logging severity level. The logging buffered only records the messages which of level is equal or above severity level.

The parameters “severitylevel” could be specified 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), informational (6), debug (7).

Format logging buffered [<severitylevel keyword> | <0 ~ 7>]

Default Info

Mode Global Config

In the following two examples, the severity level is set the warning level.

```
(M4500-32C) #logging buffered 4

(M4500-32C) #logging buffered warning
```

5.6.6. logging buffered wrap

This command enables wrapping of in-memory logging, it will overwrite old log records when full capacity reached. Otherwise when full capacity is reached, logging stops.

Format [no] logging buffered wrap

Default Enabled

Mode Global Config

5.6.7. clear logging buffered

This command clears all in-memory logs.

Format clear logging buffered

Default None

Mode Privilege EXEC

5.6.8. show logging traplogs

This command displays the trap log maintained by the switch. Trap log is not retained across a switch reset.

Format show logging traplogs

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show logging traplogs


Number of Traps Since Last Reset..... 5

Trap Log Capacity..... 256
```

```
Number of Traps Since Log Last Viewed..... 5


Log System Up Time           Trap
--- ------------------------ ----------------------------------------------
  0 Apr 28 19:35:51 2000     Cold Start: Unit: 0
  1 Apr 28 19:35:05 2000     Temperature state change alarm: Unit Number: 1
                             Current: Normal, Previous: None
  2 Apr 28 19:34:59 2000     Succeeded User Login: Console started for user
                             admin connected from EIA-232.
  3 Apr 28 19:34:57 2000     Entity Database: Configuration Changed
  4 Apr 28 19:34:52 2000     Link Down: VLAN- 1
(M4500-32C) #
```

5.6.9. show logging hosts

This command displays the configuration of logging hosts.

Format show logging hosts

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show logging hosts


Index   IP Address/Hostname      Type        Severity    Port     Status
-----  ------------------------ ----------  ----------  ------ -------------
1     10.1.1.100                ipv4        critical   514    Active
2     logging-server.test.dep   dns         critical   514    Active


(M4500-32C) #
```

5.6.10. logging host

This command is used to add addresses of remote log hosts.

The parameter “<hostaddress|hostname>” could be IPv4 address, or IPv6 address, or domain name. This parameter needs to match next parameter {dns | ipv4 | ipv6} to clarify its format.

The parameter “<port>” means the service port number of remote log host.

The parameters “severitylevel” could be specified 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), informational (6), debug (7).

Format logging host <hostaddress|hostname> {dns | ipv4 | ipv6} [<port>] [<severitylevel>]

Default <port> is 514
<severitylevel> is critical

Mode Global Config

Example: Adds two logging hosts: first one uses the format of IPv4 address, default port and, default severity level; second one uses the format of domain name, assigns server port to 514 and severity level to critical (2).

```
(M4500-32C) #configure

(M4500-32C) (Config)#logging host 10.1.1.100 ipv4

(M4500-32C) (Config)#logging host logging-server.test.dep dns 514 2
```

5.6.11. logging host remove

This command is used to remove a remote log host.

The parameter “<hostindex>” means logging host Index which could be found in the output of “show logging hosts".

Format logging host remove <hostindex>

Default None

Mode Global Config

Example: Remove an existing log host which of index is 1.

```
(M4500-32C) #configure

(M4500-32C) (Config)#logging host remove 1
```

5.6.12. logging host reconfigure

This command is used to reconfigure the setting of existing log host.

The parameter “<hostindex>” means logging host Index which could be found in the output of “show logging hosts".

The parameter “<hostaddress|hostname>” could be IPv4 address, or IPv6 address, or domain name.

The parameter “<port>” means the service port number of remote log host.

The parameters “severitylevel” could be specified 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), informational (6), debug (7).

Format logging host reconfigure <hostindex> {<hostaddress|hostname> | port <port> | severitylevel <severitylevel>}

Default None

Mode Global Config

Example: Changes the address of index 1 logging host to IPv4 address 2.2.2.2.

```
(M4500-32C) #configure

(M4500-32C) (Config)# logging host reconfigure 1 2.2.2.2
```

5.6.13. logging syslog

This command enables or disables syslog logging.

Format [no] logging syslog

Default Disabled

Mode Global Config

5.6.14. logging syslog port

This command sets the local port number of the log client for logging messages.

Format [no] logging syslog port <portid>

Default 514

Mode Global Config

5.6.15. logging syslog facility

This command sets the default facility used in syslog messages for components that do not have an internally assigned facility.

The parameter “<facility>” 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, all.

Format logging syslog facility <facility>

Default user

Mode Global Config

5.6.16. logging syslog source-interface

This command is used 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> | serviceport | tunnel <tunnel-id> | vlan <vlan-id>}

no logging syslog source-interface

Default not configure

Mode Global Config

5.6.17. logging console

This command enables or disables to print log message to console.

Format [no] logging console

Default Enabled

Mode Global Config

5.6.18. logging console severity level

This command sets the severity level of logging console. The logging console only prints the messages which of level is equal or above severity level.

The parameters “severitylevel” could be specified 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), informational (6), debug (7).

Format logging console [<severitylevel keyword> | <0 ~ 7>]

Default Info

Mode Global Config

Example: Below two examples are some configurations, it sets severity level of logging console to warning.

```
(M4500-32C) #logging console 4

(M4500-32C) #logging console warning
```

5.6.19. logging monitor

This command is used to enable or disable global configuration of terminal monitor. When logging monitor is enabled and terminal session (e.g. Telnet or SSH session) enables configuration of “terminal monitor”, the log messages will print to terminal session.

Format [no] logging monitor

Default Disabled

Mode Global Config

5.6.20. logging monitory severity level

This command sets the severity level of logging monitor. The logging monitor only prints the messages which of level is equal or above severity level.

The parameters “severitylevel” could be specified 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), informational (6), debug (7).

Format logging monitor [<severitylevel keyword> | <0 ~ 7>]

Default Info

Mode Global Config

Example: Below two examples are some configurations, it sets severity level of logging monitor to warning.

```
(M4500-32C) #logging monitor 4

(M4500-32C) #logging monitor warning
```

5.6.21. show logging cli-command-log

This command displays the logging configuration and the received cli command messages.

The log may not show in time order since the switch only keeps the last 5000 logs in file and the new log entries overwrite the old ones when the logs number is more than 5000.

Format show logging cli-command-log

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show logging cli-command-log


CLI Command Logging                 : enabled

CLI Command Log Maximum             : 5000

CLI Command Log Current Count       : 8

Jun 22 18:44:26: %Switch-1-LOG: [0xf7800754] 1 %% CLI:EIA-232:admin:clear cli-
command-log

Jun 22 18:50:15: %Switch-1-LOG: [0xdf956804] 2 %% CLI:EIA-232:admin:Disconnected
due to Idle Timeout

Jun 22 18:57:18: %Switch-1-LOG: [0xf7800754] 3 %% CLI:EIA-232:admin:User admin
logged in

Jun 22 19:05:36: %Switch-1-LOG: [0xf7800754] 4 %% CLI:EIA-232:admin:show logging
cli-command-log

Jun 22 19:06:28: %Switch-1-LOG: [0xf7800754] 5 %% CLI:EIA-232:admin:configure

Jun 22 19:06:34: %DUT-1-LOG: [0xf7800754] 6 %% CLI:EIA-232:admin:hostname DUT

Jun 22 19:06:40: %DUT-1-LOG: [0xf7800754] 7 %% CLI:EIA-232:admin:hostname DUT

Jun 22 19:06:59: %Test-1-LOG: [0xf7800754] 8 %% CLI:EIA-232:admin:hostname Test

(M4500-32C) #
```

5.6.22. logging cli-command

This command is used to enable or disable system logs the cli-command history to a file in global configuration mode.

The switch supports up to 5000 entries in the CLI command history log. If the logs are more than 5000 entries, the switch removes the oldest log and writes the new entry. All the entries have the time stamp for reference.

Format [no] logging cli-command

Default Enabled

Mode Global Config

5.6.23. clear cli-command-log

This command is used to reset the CLI command log file and the count of received commands.

The switch clears and resets the CLI command history log through the use of this command. Whether or not the CLI logging command function is enabled, you can clear the history log file.

Format clear cli-command-log

Default None

Mode Privileged Exec

5.7.Email Alert and Mail Server Commands

Email Alert is an extension of the logging system. This feature can immediately send urgent log messages to a specified mail address by email. It also can send non-urgent log messages created in a specified interval to a specified address. If there is no buffer to keep non-urgent log messages in the specified interval, the log messages will be sent and cleared.

5.7.1. show logging email config

This command displays the configurations of email alert.

Format show logging email config

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show logging email config

Email Alert Logging.......................... enabled

Email Alert From Address..................... switch@netgear.com

Email Alert Urgent Severity Level.............. alert

Email Alert Non Urgent Severity Level.......... warning

Email Alert Trap Severity Level................ info

Email Alert Notification Period................ 30 min


Email Alert To Address Table:

For Msg Type ............................... urgent

Address1 .....................................test01@email.com

For Msg Type ............................... non-urgent

Address1 ................................... test02@email.com


Email Alert Subject Table:

For Msg Type urgent, subject is.............. Urgent Log Messages

For Msg Type non-urgent, subject is.......... Non Urgent Log Messages

(M4500-32C) #
```

5.7.2. show logging email statistics

This command displays the statistics of email alert.

Format show logging email statistics

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) (Config)#show logging email statistics


Email Alert operation status.................. enabled


Email Alert Statistics:


No of email Failures so far................... 1

No of email sent so far....................... 3

Time since last email Sent..................... 00 days 00 hours 00 mins 29 secs


(M4500-32C) (Config)#
```

5.7.3. show mail-server config

This command displays information about email server configuration.

Format show mail-server {<ip-address | hostname> | all} config

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show mail-server all config

Mail Servers Configuration:
```

```
No of mail servers configured.................. 1


Email Alert Mail Server Address................ smtp.gmail.com

Email Alert Mail Server Port................... 465

Email Alert Security Protocol.................. tlsv1

Email Alert Username........................... mailServerUser01

M4500-32C) (Config)#
```

5.7.4. logging email

This command enables or disables email alerting function.

Format [no] logging email

Default Disabled

Mode Global Config

5.7.5. logging email urgent and non-urgent

This command sets the lowest serverity 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).

Format logging email {urgent | non-urgent} {<severity> | none}

no logging email {urgent | non-urgent}

Default Urgent severity level is alert(1)

Non-Urgent severity level is warning (4)

Mode Global Config

Example: Set severity level of urgent mail to critical(2), and set severity level of non-urgent mail to notice(5).

```
(M4500-32C) #configure

(M4500-32C) (Config)#logging email urgent 2

(M4500-32C) (Config)# logging email non-urgent 5
```

5.7.6. logging email logtime

This command is used to configure how frequently non-urgent email messages are sent. Non-urgent messages are collected and sent in a batch email at the specified interval.

The parameter “<interval>“ uses to Specify how frequently non-urgent email messages are sent. The valid interval is 30 to 1440 minutes.

Format logging email logtime <interval>

no logging email logtime

Default 30

Mode Global Config

5.7.7. logging email message-type and subject

This command is used to configure the subject line of the email for the specified type.

The parameter “<subject>“ sets the subject line of the email.

Format logging email message-type {both | urgent | non-urgent} subject <subject>

no logging email message-type {both | urgent | non-urgent} subject

Default type urgent is “Urgent Log Messages”

type non-urgent is “Non Urgent Log Messages”

Mode Global Config

5.7.8. logging email message-type and to-addr

This command is used to configure the destination 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 parameter “<to-addr>“ specifies a standard email address to be the destination address of urgent or non-urgent message.

Format [no] logging email message-type {both | urgent | non-urgent} to-addr <to-addr>

Default None

Mode Global Config

Example: Add an email address “toAddr01@email.com” to the destination address of urgent message, and add another email address “toAddr02@email.com” to the destination address of both urgent and non-urgent message.

```
(M4500-32C) #configure

(M4500-32C) (Config)# logging email message-type urgent to-addr toAddr01@email.com

(M4500-32C) (Config)# logging email message-type both to-addr toAddr02@email.com
```

5.7.9. logging email from-addr

This command is used to configure the email source address (the address of the sender, i.e., switch) to which messages are sent.

The parameter “<from-addr>“ specifies a standard email address to be the source address of both urgent and non-urgent message.

Format logging email from-addr <from-address>

no logging email from-addr

Default switch@netgear.com

Mode Global Config

Example: Set an email address “fromAddr@email.com” to the source address of both urgent and non-urgent message.

```
(M4500-32C) #configure

(M4500-32C) (Config)# logging email from-addr fromAddr@email.com
```

5.7.10. mail-server configuration

This command configures the parameters of SMTP server which is used to send email alert messages. This command changes CLI mode from Global Config Mode to Mail Server Config mode.

Format [no] mail-server <ipaddress|ipv6address|host-name>

Default None

Mode Global Config

Example: Set mail server address to hostname “smtp.gmail.com” and change to Mail Server Config mode.

```
(M4500-32C) #configure

(M4500-32C) (Config)#mail-server smtp.gmail.com

(M4500-32C) (Mail-Server)#
```

5.7.11. mail-server security

This command sets the email alerting security protocol by enabling the switch to use TLSv1/STARTTLS authentication with the SMTP Server. If the TLSv1/STARTTLS mode is enabled on the switch but the SMTP sever does not support TLSv1/STARTTLS mode, no email is sent to the SMTP server.

The parameter “none” means email server doesn’t use security protocol.

The parameter “starttls” means to use STARTTLS security protocol.

The parameter “tlsv1” means to use TLSv1 security protocol.

Format security {none | starttls | tlsv1}

Default none

Mode Mail Server Config

5.7.12. mail-server port

This command configures the TCP port to use for communication with the SMTP server. The recommended port for TLSv1 is 465, STARTTLS is 587, and for no security (i.e. none) is 25. However, any nonstandard port in the range 1 to 65535 is also allowed.

Format [no] port <465 | 25 | 1 to 65535>

Default 25

Mode Mail Server Config

5.7.13. mail-server username

This command configures the username (or login ID) which is used to authenticate with the SMTP server.

Format [no] username <username>

Default None

Mode Mail Server Config

5.7.14. mail-server password

This command configures the password that is used to authenticate with the SMTP server.

You can set the password using one of the following options:

- Type the **password** keyword to configure the password in plain text. The password is displayed with * for each character that you type. The password must be in alphanumeric characters with a maximum length of 64 characters.
- Type the **password 7** keyword to configure the password in encrypted form. The password must be in hexadecimal digits with a length of 128 characters.

Format [no] password [7 <password>]

Default None

Mode Mail Server Config

In the following examples, the first example sets the password of mail server to plain text “testPassword”, and the second one sets the password to an encrypted string that is fixed at 128 hexadecimal digits.

```
(M4500-32C) #configure

(M4500-32C) (Config)# mail-server smtp.gmail.com

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

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

(M4500-32C) (Mail-Server)#

(M4500-32C) (Mail-Server)# password 7
0fdd841c8a524979e5ba47893efcf48b12a08619953e1b6e42cde0931198ca717cb5ff8b49795a3497e
283990827c5ba1ce32855ced76a505726dfb1ee222c4b
```

5.7.15. clear logging email statistics

This command is used to clear the statistics of logging email.

Format clear logging email statistics

Default None

Mode Privilege EXEC

5.8. Script Management Commands

5.8.1. script apply

This command applies the commands in the script to the switch.

Format script apply <scriptname>

Default None

Mode Privilege EXEC

5.8.2. script delete

This command deletes a specified script or all scripts on the switch.

Format script delete {<scriptname> | all}

Default None

Mode Privilege EXEC

5.8.3. script list

This command lists all scripts on the switch as well as the remaining available space.

Format script list

Default None

Mode Privilege EXEC

Example:

```
(M4500-32C) #script list


Configuration Script Name        Size(Bytes)
-------------------------------- -----------
1.scr                                  1092
t.scr                                  1092
```

```
2 configuration script(s) found.

5117 Kbytes free.

(M4500-32C) #
```

5.8.4. script show

This command displays the content of a script file.

Format script show <scriptname>

Default None

Mode Privilege EXEC

Example:

```
(M4500-32C) #script show test.scr

1 : !Current Configuration:

2 : !

3 : !System Description "M4500-32C, Runtime Code 7.0.0.1"

4 : !System Software Version "7.0.0.1"

5 : !System Up Time          "0 days 0 hrs 1 mins 45 secs"

6 : !Additional Packages     BGP-4,QOS,Multicast,IPv6,Routing,Data Center

7 : !Current System Time: Aug  5 08:22:08 2019

8 : !

9 : configure

10 : hostname "Switch"

11 : serviceport protocol dhcp6

12 : vlan database

13 : exit

14 : time-range

15 : kron policy-list p1

16 : cli show version | redirect tftp://172.20.0.28/kr-t6.txt
```

```
17 : exit

18 : username "admin" passwd 7
d32036926a456949a1dd05f3768212c089add94bccd752314f0c05fedf66f52c407256118c62e461710
1230004dff4ee69c4e4d4eaed9590cfd5fe318b39dac3 level 15

19 : username "admin" role "network-admin"

20 : username "guest" role "network-operator"

21 : aaa authentication login "networkList" radius

22 : radius server host auth "172.20.0.107" name "Default-RADIUS-Server"

23 : line console

24 : exec-timeout 0

25 : exit

26 : line vty

27 : exit

28 : line ssh

29 : exit

30 : interface vlan 1

31 : exit

32 : snmp-server sysname "Switch"

33 : !

34 : interface control-plane

35 : exit

36 : application install orig_restful_api

37 : router ospf

38 : exit

39 : ipv6 router ospf

40 : exit

41 : exit

(M4500-32C) #
```

5.8.5. script validate

This command validates an assigned script by parsing each line. The validate option is intended to be used as a tool for script development.

Format script validate <scriptname>

Default None

Mode Privilege EXEC

Example:

```
(M4500-32C) #script validate test.scr


configure

hostname "Switch"

serviceport protocol dhcp6

vlan database

exit

time-range

kron policy-list p1

cli show version | redirect tftp://172.20.0.28/kr-t6.txt

exit

username "admin" passwd 7
d32036926a456949a1dd05f3768212c089add94bccd752314f0c05fedf66f52c407256118c62e461710
1230004dff4ee69c4e4d4eaed9590cfd5fe318b39dac3 level 15

username "admin" role "network-admin"

username "guest" role "network-operator"

aaa authentication login "networkList" radius

radius server host auth "172.20.0.107" name "Default-RADIUS-Server"

line console

exec-timeout 0

exit

line vty
```

```
exit

line ssh

exit

interface vlan 1

exit

snmp-server sysname "Switch"

interface control-plane

exit

application install orig_restful_api

router ospf

exit

ipv6 router ospf

exit

exit

Configuration script 'new-script.scr' validated.

(M4500-32C) #
```

5.9. User Account Management Commands

This section describes the commands you use to configure port-based network access control (IEEE 802.1X). Port-based network access control allows you to permit access to network services only and to permit access to devices that are authorized and authenticated.

5.9.1. show users

This command displays the configured user names and their settings.

Format show users

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
User Name	The name the user will use to login using the serial port, Telnet. A new user may be added to the switch by entering a name in a blank entry. The user name may be up to 64 characters, and is case sensitive. Two users are included as the factory default, admin, and guest.
User Access Mode	Shows whether the operator is able to change parameters on the switch (Privilege-15) or is only able to view them (Privilege-1). As a factory default, admin has Privilege-15 access and guest has Privilege-1 access. There can only be one Privilege-15 user and up to five Privilege-1 users.

Example: The following shows examples of the CLI display output for the commands.

```
(M4500-32C) (Config)#show users

                          User

User Name                 Access Mode

------------------------  --------------------

admin                     Privilege-15

guest                     Privilege-1
```

5.9.2. show users long

This command displays full names of users.

Format Show users long

Default None

Example:

```
(M4500-48XF8C) # show users long

User Name

------------

admin

guest

(M4500-48XF8C) #
```

5.9.3. show users accounts

The user can go to the CLI Privilege Exec to get all of user information, use the show users accounts Privilege command.

Format show users accounts [detail]

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
User Name	The local user account's user name.
Privilege	The user's privilege level. The range of privilege level is 1 and 15. Access mode for privilege level 15 is read/write, the others is read-only.
Password Aging	Indicates number of days, since the password was configured, until the password expires.
Password Expiration Date	The current password expiration date in date format.
Lockout	Indicates whether the user account is locked out (true or false).

Example: The following shows examples of the CLI display output for the commands.

```
(M4500-32C) (Config)#show users accounts

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


(M4500-32C) (Config)#show users accounts detail


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

UserName..................................... guest
Privilege.................................... 1
Password Aging............................... ---
Password Expiry.............................. ---
Lockout...................................... False
Override Complexity Check..................... Disable
Password Strength............................ ---
```

5.9.4. show passwords configuration

Use this command to display the configured password management settings.

Format show passwords configuration

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
Minimum Password Length	Minimum number of characters required when changing passwords.
Password Aging	Length in days that a password is valid.
Password History	Number of passwords to store for reuse prevention.
Lockout Attempts	Number of failed password login attempts before lockout.
Password Strength Check	The user to configure passwords that comply with the strong password configuration.
Minimum Password Uppercase Letters	Minimum number of uppercase characters required when changing passwords.
Minimum Password Lowercase Letters	Minimum number of lowercase characters required when changing passwords.
Minimum Password Numeric Characters	Minimum number of numeric characters required when changing passwords.
Minimum Password Special Characters	Minimum number of special characters required when changing passwords.
Maximum Password Repeated Characters	Maximum number of characters cannot repeated when changing passwords.
Maximum Password Consecutive Characters	Maximum number of characters cannot consecutive when changing passwords.
Minimum Password Character Classes	Valid range for user passwords.
Password Exclude Keywords	The password to be configured should not contain the keyword mentioned in this field.

Example: The following shows examples of the CLI display output for the commands.

```
(M4500-32C) (Config)#show passwords configuration
```

```
Passwords Configuration

--------------------------------

Minimum Password Length..................... 8

Password Aging (days)....................... 0

Password History............................ 0

Lockout Attempts............................ 0

Password Strength Check..................... Enable

Minimum Password Uppercase Letters.......... 0

Minimum Password Lowercase Letters.......... 0

Minimum Password Numeric Characters......... 1

Minimum Password Special Characters......... 1

Maximum Password Repeated Characters........ 0

Maximum Password Consecutive Characters..... 0

Minimum Password Character Classes.......... 3

Password Exclude Keywords................... <none>
```

5.9.5. show passwords result

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

Format show passwords result

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
Last User Whose Password Is Set	The local user account's user name.
Password Strength Check	The user's privilege level. The range of privilege level is 1 and 15. Access mode for privilege level 15 is read/write, the others is read-only.
Last Password Set Result	Indicates number of days, since the password was configured, until the password expires.

Example: The following shows examples of the CLI display output for the commands.

```
(M4500-32C) (Config)#show passwords result


Last User whose password is set ................. guest

Password strength check ......................... Disable

Last Password Set Result:

========================

Password Successfully Configured for User 'guest'.
```

5.9.6. username

This command adds a new user (account) if space permits. The default privilege level is 1. The account <username> can be up to 64 characters in length. The name may be comprised of alphanumeric characters as well as the dash (‘-’) and underscore (‘_’). The <username> is case-sensitive. Six user names can be defined.

This command changes the password of an existing operator. The user password should not be more than 64 characters in length. If a user is authorized for authentication or encryption is enabled, the password must be 64 alphanumeric characters in length. The username and password are case-sensitive. When a password is changed, a prompt asks for the operator’s former password. If none, press enter.

Note: The admin user account cannot be deleted. The special characters allowed in the password include # $ % & ‘ ( ) * + , - / ; < = > @ [\ ] ^ _ ` { | } ~

Format username <username> { level <level> | passwd [7 <password>]}

Parameter	Definition
<username>	A new user name (Range: up to 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. Enter access level 1 for Read Access or 15 for Read/Write Access. If not specified where it is optional, the privilege level is 1.
passwd	Type the **passwd** keyword to set the password in plain text. The text that you type is displayed in asterisk characters. The maximum length of a plain-text password is 64 characters.
7 <password>	Type the **7** keyword to set an encrypted password, which must be exactly 128 hexadecimal characters in length.

Default None

Mode Global Config

5.9.7. no username

This command removes a user name created before.

Format no username <username>

Mode Global Config

5.9.8. username <username> unlock

The user can go to the CLI Global Configuration Mode to unlock a locked user account, use the *username <name> unlock* global configuration command.

Format username <username> unlock

Parameter	Definition
<username>	A username.

Default None

Mode Global Config

5.9.9. passwords aging

If the passwords aging is set, the local user will be prompted to change it before logging in again when the local user's password expires.

Format passwords aging <1-365>

Parameter	Definition
<1-365>	Number of days until password expires.

Default 0, no aging

Mode Global Config

5.9.10. no passwords aging

Use the *no passwords aging* return to default value 0.

Format no passwords aging

Mode Global Config

5.9.11. passwords history

Use this command to set the number of previous passwords that shall be stored for each user account. If password history is set, the local user will not be able to reuse any password stored in password history when the local user changes his or her password.

Format passwords aging history <0-10>

Parameter	Definition
<0-10>	Number of passwords to be used in password history check.

Default 0, no aging

Mode Global Config

5.9.12. no passwords history

Use the *no passwords history* return to default value 0.

Format no passwords history

Mode Global Config

5.9.13. 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 read/write access can re-activate a locked user account. The user can go to the CLI Global Configuration Mode to set the password lock-out count.

Format passwords lock-out <1-5>

Parameter	Definition
<1-5>	The number of password failures before account lock.

Default 0

Mode Global Config

Note: If the admin user fails to connect to the switch using SSH port 1234 or telnet port 1223, the admin user is locked out. However, the admin user can still log in to the switch using a console connection or using SSH port 22 (Linux system login).

5.9.14. no passwords lock-out

Use the *no passwords lock-out* to return to default value 0.

Format no passwords lock-out

Mode Global Config

5.9.15. passwords min-length

The user can go to the CLI Global Configuration Mode to set the minimum password length.

Format passwords min-length <8-64>

Parameter	Definition
<8-64>	The length of password.

Default 8

Mode Global Config

5.9.16. no passwords min-length

Use the *no passwords min-length* return to default value 0.

Format no passwords min-length

Mode Global Config

5.9.17. passwords strength-check

The user can go to the CLI Global Configuration Mode to set the password strength policy enforcement, use the *passwords strength-check* Global configuration command.

Format passwords strength-check

Default Disable

Mode Global Config

5.9.18. no passwords strength-check

Use the *no passwords strength-check* return to default disable.

Format no passwords strength-check

Mode Global Config

5.9.19. passwords strength maximum

The user can go to the CLI Global Configuration Mode to set the password strength.

Format passwords strength maximum {consecutive-characters | repeated-characters} [<0-15>]

Default 0

Mode Global Config

5.9.20. no passwords strength maximum

Use the *no passwords strength maximum {consecutive-characters | repeated-characters}* return to default value 0.

Format no passwords strength maximum {consecutive-characters | repeated-characters}

Mode Global Config

5.9.21. passwords strength minimum

The user can go to the CLI Global Configuration Mode to set the password strength.

Format passwords strength minimum {character-classes <0-4> | lowercase-letters <0-16> | numeric-characters <0-16> | special-characters <0-16> | uppercase-letters <0-16>}

Default uppercase-letters 2

lowercase-letters 2

numeric-characters 2

special-characters 2

character-classes 4

Mode Global Config

5.9.22. no passwords strength minimum

Use the *no passwords strength minimum {character-classes | lowercase-letters | numeric-characters | special-characters | uppercase-letters}* return to default value 2.

Format no passwords strength minimum {character-classes | lowercase-letters | numeric-characters | special-characters | uppercase-letters}

Mode Global Config

5.9.23. passwords strength exclude-keyword

The user can go to the CLI Global Configuration Mode to set the password strength, use the **passwords strength exclude-keyword** <keyword> Global configuration command.

Format passwords strength exclude-keyword <keyword>

Default None

Mode Global Config

5.9.24. no passwords strength exclude-keyword

Use the **no passwords strength exclude-keyword** <keyword> return to default none.

Format no passwords strength exclude-keyword <keyword>

Mode Global Config

5.9.25. show users login-history

This command displays the history of user login.

Format show users login-history

Default None

Example:

```
(M4500-48XF8C) #show users login-history

Login Time             Username              Protocol      Location

---------------------  --------------------  ------------  ---------------

May 06 2020 03:33:21   admin                 Serial

May 06 2020 03:24:42   admin                 Serial

May 06 2020 02:46:16   admin                 Serial

May 06 2020 02:35:13   admin                 Serial

May 06 2020 02:14:59   admin                 Serial

May 06 2020 02:04:07   admin                 Serial

May 06 2020 01:56:32   admin                 Serial

May 06 2020 01:08:01   admin                 Serial

May 06 2020 00:46:43   admin                 Serial

May 06 2020 00:34:54   admin                 Serial

May 06 2020 00:10:26   admin                 Serial

May 05 2020 07:23:01   admin                 Serial

May 05 2020 07:04:51   admin                 Serial

May 05 2020 06:21:46   admin                 Serial

May 05 2020 06:21:32   admin                 Serial

(M4500-48XF8C) #
```

5.9.26. user password override-complexity-check

This command is used to enable override-complexity-check of password.

Format username <username> level<level> override-complexity-check password

Default Disabled

Mode Global Config

5.9.27. user role

This command is used to assign an RBAC role to a user.

Format username <username> role <name>

Default None

Mode Global Config

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). Port-based network access control allows you to permit access to network services only to and devices that are authorized and authenticated.

5.10.1. show authentication methods

This command displays the ordered authentication methods for all authentication login lists.

Format show authentication methods

Mode Privileged EXEC

Display Message

Parameter	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.

(M4500-32C) #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                  enableList

SSH            networkList                  enableList


DOT1X            :
```

5.10.2. 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 [summary [<slot/port>] | detail <slot/port> | statistics <slot/port>]

Mode Privileged EXEC

Display Message

If you do not use the optional parameters slot/port or vlanid, the command displays the global dot1x mode, the VLAN Assignment mode, and the Dynamic VLAN Creation mode.

Parameter	Definition
Administrative Mode	Indicates whether authentication control on the switch is enabled or disabled.
VLAN Assignment Mode	Indicates whether assignment of an authorized port to a RADIUS-assigned VLAN is allowed (enabled) or not (disabled).
Dynamic VLAN Creation Mode	Indicates whether the switch can dynamically create a RADIUS-assigned VLAN if it does not currently exist on the switch.
Monitor Mode	Indicates whether the Dot1x Monitor mode on the switch is enabled or disabled.
EAPOL Flood Mode	Indicates whether the Dot1x EAPOL Flood mode on the switch is enabled or disabled.

If you use the optional parameter summary [<slot/port>], the dot1x configurations for the specified port or all ports are displayed.

Parameter	Definition
Interface	The interface whose configuration is displayed.
Control Mode	The configured control mode for this port. Possible values are force-unauthorized | forceauthorized | auto | mac-based | authorized | unauthorized.
Operating Control Mode	The control mode under which this port is operating. Possible values are authorized | unauthorized.
Reauthentication Enabled	Indicates whether reauthentication is enabled on this port.
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 summary 0/1.

```
(M4500-32C) #show dot1x summary 0/1

                            Operating      Reauthentication

Interface    Control Mode   Control Mode   Enabled            Port Status

----------   ------------   ------------   ----------------   -----------

0/1          auto           N/A            False              N/A
```

If you use the optional parameter 'detail <slot/port>', the detailed dot1x configuration for the specified port is displayed.

Parameter	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.
Control Mode	The configured control mode for this port. Possible values are force-unauthorized | forceauthorized | auto | mac-based.
Authenticator PAE State	Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized. When MAC-based authentication is enabled on the port, this parameter is deprecated.
Backend Authentication State	Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize. When MAC-based

	authentication is enabled on the port, this parameter is deprecated.
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.
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.
Guest-VLAN ID	The guest VLAN identifier configured on the interface.
Guest VLAN Period	The time in seconds for which the authenticator waits before authorizing and placing the port in the Guest VLAN, if no EAPOL packets are detected on that port.
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.

Parameter	Definition
Maximum Requests	The maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/Identity before timing out the supplicant. The value will be in the range of 1 and 10.
Configured MAB mode	The dot1x MAC Authentication Bypass configuration status.
Operational MAB mode	The dot1x MAC Authentication Bypass operational status.
VLAN ID	The VLAN assigned to the port by the radius server. This is only valid when the port control mode is not Mac-based.
VLAN Assigned Reason	The reason the VLAN identified in the VLAN-assigned field has been assigned to the port. Possible values are RADIUS, Unauthenticated VLAN, Guest VLAN, default, and Not Assigned. When the VLAN Assigned Reason is Not Assigned, it means that the port has not been assigned to any VLAN by dot1x. This only valid when the port control mode is not MAC-based.
Reauthentication Period	The timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The value is expressed in seconds and will be in the range of 1 and 65535.
Reauthentication Enabled	Indicates if reauthentication is enabled on this port. Possible values are ‘True” or “False”.
Key Transmission Enabled	Indicates if the key is transmitted to the supplicant for the specified port.

	Possible values are True or False.
Control Direction	The control direction for the specified port or ports. Possible values are both or in.
Maximum Users	The maximum number of clients that can get authenticated on the port in the MAC-based dot1x authentication mode. This value is used only when the port control mode is not MACbased.
Unauthenticated VLAN ID	Indicates the unauthenticated VLAN configured for this port. This value is valid for the port only when the port control mode is not MAC-based.
Session Timeout	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. This value is valid for the port only when the port control mode is not MAC-based.
Session Termination Action	This value indicates the action to be taken once the session timeout expires. Possible values are Default, Radius-Request. If the value is Default, the session is terminated the port goes into unauthorized state. If the value is Radius-Request, then a reauthentication of the client authenticated on the port is performed. This value is valid for the port only when the port control mode is not MAC-based.

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

```
(M4500-32C) #show dot1x detail 0/1

Port..................................................... 0/1

Protocol Version......................................... 1

PAE Capabilities......................................... Authenticator

Control Mode............................................. auto

Authenticator PAE State.................................. Initialize

Backend authentication state............................. Initialize

Quiet Period (secs)...................................... 60

Transmit Period (secs)................................... 30

Guest VLAN ID............................................ 0

Guest VLAN Period (secs)................................. 90

Supplicant Timeout (secs)................................ 30

Server Timeout (secs).................................... 30

Maximum Requests......................................... 2

Configured MAB Mode...................................... Disabled
```

```
Operational MAB Mode.................................. Disabled

VLAN Id.............................................. 0

VLAN Assigned Reason................................. Not Assigned

Reauthentication Period (secs)....................... 3600

Reauthentication Enabled............................. False

Key Transmission Enabled............................. False

Control Direction.................................... both

Maximum Users........................................ 48

Unauthenticated VLAN ID.............................. 0

Session Timeout...................................... 0

Session Termination Action........................... Default
```

For each client authenticated on the port, the **show dot1x detail <slot/port>** command will display the following MAC-based dot1x parameters if the port-control mode for that specific port is MAC-based.

Parameter	Definition
Supplicant MAC-Address	The MAC-address of the supplicant.
Authenticator PAE State	Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized.
Backend Authentication State	Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize.
VLAN-Assigned	The VLAN assigned to the client by the radius server.
Logical Port	The logical port number associated with the client.

If you use the optional parameter statistics <slot/port>, the following dot1x statistics for the specified port appear.

Parameter	Definition
Port	The interface whose statistics are displayed.
PAE Capabilities	The port access entity (PAE) functionality of this port.
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.
EAPOL Length Error Frames Received	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.

5.10.3. show dot1x authentication-history

This command is used to display the Dot1x Authentication History Log for the specified port or all ports. Use the optional keywords to display only failure authentication events in summary or in detail

Format show dot1x authentication-history {<slot/port> | all} [{failed-auth-only [detail] | detail}]

Mode Privileged EXEC

Display Message

If you use the optional parameter detail, the following information for the specified port or all ports appears.

Parameter	Definition
Time Stamp	The exact time at which the event occurs.
Interface	Physical Port on which the event occurs.

MAC-Address	The supplicant/client MAC address.
VLAN assigned	The VLAN assigned to the client/port on authentication.
VLAN assigned Reason	The type of VLAN ID assigned, which can be Guest VLAN, Unauth, Default, RADIUS Assigned, or Monitor Mode VLAN ID.
Filter Name	Filter Name returned by RADIUS server when the client was authenticated. This is a configured DiffServ policy name on switch.
Auth Status	The authentication status.
Reason	The actual reason behind the successful or failed authentication.

If you do not use the optional parameter, the following information for the specified port or all ports appears.

Parameter	Definition
Time Stamp	The exact time at which the event occurs.
Interface	Physical Port on which the event occurs.
MAC-Address	The supplicant/client MAC address.
VLAN ID	The VLAN assigned to the client/port on authentication.
Auth Status	The authentication status.

5.10.4. show dot1x clients

This command is used to display the Dot1x client information. This command also displays information about the number of clients that are authenticated using Monitor mode and using Dot1x

Format show dot1x clients [<slot/port>]

Mode Privileged EXEC

Display Message

Parameter	Definition
Clients Authenticated using Monitor Mode	Indicates the number of the Dot1x clients authenticated using Monitor mode.
Clients Authenticated using Dot1x	Indicates the number of Dot1x clients authenticated using 802.1x authentication process.
Logical Interface	The logical port number associated with a client.

Interface	The physical port to which the supplicant is associated.
User Name	The user name used by the client to authenticate to the server.
Supp MAC Address	The supplicant device MAC address.
Session Time	The time since the supplicant is logged on.
Filter Id	Identifies the Filter ID returned by RADIUS server when the client was authenticated. This is a configured DiffServ policy name on switch.
VLAN ID	The VLAN assigned to the port.
VLAN Assigned	The reason the VLAN identified in the VLAN ID field has been assigned to the port. Possible values are RADIUS, Unauthenticated VLAN, Monitor Mode, or Default. When the VLAN Assigned reason is Default, it means that the VLAN was assigned to the port because the P-VID of the port was that VLAN ID.
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. This value is valid for the port only when the port-control mode is not MAC-based.
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.

5.10.5. show dot1x users

This command is used to display the Dot1x port security user information for logically configured users

Format show dot1x users <slot/port>

Mode Privileged EXEC

Display Message

Parameter	Definition
Users	Users configured locally to have access to the specified port.

5.10.6. aaa authentication dot1x default

Use this command to configure the authentication method for port-based access to the switch. The additional methods of authentication are used only if the previous method returns an error, not if there is an authentication failure. The possible methods are as follows:

- 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 {local | none | radius}

Mode Global Config

5.10.7. no aaa authentication dot1x default

This command resets the authentication method for port-based access to the switch.

Format no aaa authentication dot1x default

Mode Global Config

5.10.8. 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

5.10.9. clear dot1x authentication-history

This command clears the authentication history table captured during successful and unsuccessful authentication on all interface or the specified interface.

Format clear dot1x authentication-history [slot/port]

Mode Privileged EXEC

5.10.10. clear RADIUS statistics

This command is used to clear all RADIUS statistics.

Format clear radius statistics

Mode Privileged EXEC

5.10.11. dot1x eapolflood

Use this command to enable EAPOL flood support on the switch.

Format dot1x eapolflood

Default Disable

Mode Global Config

5.10.12. no dot1x eapolflood

This command disables EAPOL flooding on the switch.

Format no dot1x eapolflood

Mode Global Config

5.10.13. dot1x 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.

Format dot1x dynamic-vlan enable

Default Disable

Mode Global Config

5.10.14. no dot1x dynamic-vlan enable

Use this command to prevent the switch from creating VLANs dynamically when a RADIUS-assigned VLAN does not exist in the switch.

Format no dot1x dynamic-vlan enable

Mode Global Config

5.10.15. dot1x guest-vlan

This command configures VLAN as guest vlan on an interface. The command specifies an active VLAN as an IEEE 802.1X guest VLAN. The range is 1 to the maximum VLAN ID supported by the platform.

Format dot1x guest-vlan <vlan-id>

Default Disable

Mode Interface Config

5.10.16. no dot1x guest-vlan

This command disables Guest VLAN on the interface.

Format no dot1x guest-vlan

Mode Interface Config

5.10.17. dot1x initialize

This command begins the initialization sequence on the specified port. This command is only valid if the control mode for the specified port is auto or mac-based. If the control mode is not auto or mac-based, an error will be returned.

Format dot1x initialize <slot/port>

Mode Privileged EXEC

5.10.18. dot1x mac-auth-bypass

This command enables dot1x MAC authentication bypass on an interface.

Format dot1x mac-auth-bypass

Default Disable

Mode Interface Config

5.10.19. no dot1x mac-auth-bypass

This command disables dot1x MAC authentication bypass on an interface.

Format no dot1x mac-auth-bypass

Default Disable

Mode Interface Config

5.10.20. dot1x max-req

This command sets the maximum number of times the authenticator state machine on an interface will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant.

Format dot1x max-req <1-10>

Default 2

Mode Interface Config

5.10.21. no dot1x max-req

This command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant.

Format no dot1x max-req

Mode Interface Config

5.10.22. dot1x max-users

Use this command to set the maximum number of clients supported on an interface when MAC-based dot1x authentication is enabled on the port. The *count* value is in the range 1-48.

Format dot1x max-users <1-48>

Default 48

Mode Interface Config

5.10.23. no dot1x max-users

This command resets the maximum number of clients allowed per port to its default value.

Format no dot1x max-users

Mode Interface Config

5.10.24. dot1x port-control

This command sets the authentication mode to use on the specified interface. 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. If the mac-based option is specified, then MAC-based dot1x authentication is enabled on the port.

Format dot1x port-control {force-unauthorized | force-authorized | auto | mac-based}

Default Auto

Mode Interface Config

5.10.25. no dot1x port-control

This command sets the 802.1X port control mode on the specified port to the default value.

Format no dot1x port-control

Mode Interface Config

5.10.26. dot1x port-control all

This command sets the authentication mode to use on all ports. 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. If the mac-based option is specified, then MAC-based dot1x authentication is enabled on the port.

Format dot1x port-control all {force-unauthorized | force-authorized | auto | mac-based}

Default Auto

Mode Global Config

5.10.27. no dot1x port-control all

This command sets the authentication mode on all ports to the default value.

Format no dot1x port-control all

Mode Global Config

5.10.28. dot1x re-authenticate

This command begins the re-authentication sequence on the specified port. This command is only valid if the control mode for the specified port is auto or mac-based. If the control mode is not auto or mac-based, an error will be returned.

Format dot1x re-authenticate <slot/port>

Mode Privileged EXEC

5.10.29. dot1x re-authentication

This command enables re-authentication of the supplicant for the specified interface.

Format dot1x re-authentication

Default Disable

Mode Interface Config

5.10.30. no dot1x re-authentication

This command disables re-authentication of the supplicant for the specified port.

Format no dot1x re-authentication

Mode Interface Config

5.10.31. dot1x system-auth-control

Use this command to enable the dot1x authentication support on the switch. While disabled, the dot1x configuration is retained and can be changed, but is not activated.

Format dot1x system-auth-control

Default Disable

Mode Global Config

5.10.32. 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

5.10.33. dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on an interface. Depending on the token used and the value (in seconds) passed, various timeout configurable parameters are set. The following tokens are supported:

Format dot1x timeout {guest-vlan-period <seconds> | reauth-period <seconds> | quiet-period <seconds> | tx-period <seconds> | supp-timeout <seconds> | server-timeout <seconds>}

Tokens	Definition
guest-vlan-period	The time, in seconds, for which the authenticator waits to see if any EAPOL packets are received on a port before authorizing the port and placing the port in the guest vlan (if configured). The guest vlan timer is only relevant when guest vlan has been configured on that specific port. The reauth-period must be a value in the range 1 - 300.
reauth-period	The value, in seconds, of the timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The reauth-period must be a value in the range 1 - 65535.
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. The quiet-period must be a value in the range 0 - 65535.

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. The quiet-period must be a value in the range 1 - 65535.
supp-timeout	The value, in seconds, of the timer used by the authenticator state machine on this port to timeout the supplicant. The supp-timeout must be a value in the range 1 - 65535.
server-timeout	The value, in seconds, of the timer used by the authenticator state machine on this port to timeout the authentication server. The supp-timeout must be a value in the range 1 - 65535.

Default guest-vlan-period: 90 seconds
reauth-period: 3600 seconds
quiet-period: 60 seconds
tx-period: 30 seconds
supp-timeout: 30 seconds
server-timeout: 30 seconds

Mode Interface Config

5.10.34. 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 {guest-vlan-period | reauth-period | quiet-period | tx-period | supptimeout | server-timeout}

Mode Interface Config

5.10.35. dot1x unauthenticated-vlan

Use this command to configure the unauthenticated VLAN associated with the specified interface. The unauthenticated VLAN ID can be a valid VLAN ID from 0-Maximum supported VLAN ID (4093). The unauthenticated VLAN must be statically configured in the VLAN database to be operational. By default, the unauthenticated VLAN is 0, i.e. invalid and not operational.

Format dot1x unauthenticated-vlan <vlan-id>

Default 0

Mode Interface Config

5.10.36. no dot1x unauthenticated-vlan

This command resets the unauthenticated-vlan associated with the port to its default value.

Format no dot1x unauthenticated-vlan

Mode Interface Config

5.10.37. 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

5.10.38. 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

5.11. AAA Commands

This section describes the commands you use to add, manage, and delete system users. 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.

5.11.1. show accounting

This command displays ordered methods for accounting lists.

Format show accounting

Mode Privileged EXEC
User EXEC

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

```
(M4500-32C) #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 sent 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
```

5.11.2. show accounting methods

This command displays configured accounting method lists.

Format show accounting methods

Mode Privileged EXEC
User EXEC

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

```
(M4500-32C) #show accounting methods


AcctType    MethodName        MethodType    Method1    Method2

--------    --------------    ----------    -------    -------

Exec        dfltExecList      none          tacacs

Commands    dfltCmdList       none          tacacs

DOT1X       dfltDot1xList     start-stop    radius


Line            EXEC Method List    Command Method List

------------    ----------------    -------------------

Console         dfltExecList        dfltCmdList

Telnet          dfltExecList        dfltCmdList

SSH             dfltExecList        dfltCmdList
```

5.11.3. aaa authentication login

This command creates an authentication login list. The <listname> is up to 12 alphanumeric characters and is not case sensitive. Up to 5 authentication login lists can be configured on the switch.

If the authentication login list does not exist, a new authentication login list is first created and then the authentication methods are set in the authentication login list. The possible method values are enable, line, local, none, radius and tacacs.

To authenticate a user, the authentication methods in the user's login will be attempted in order until an authentication attempt succeeds or fails.

Note: The default login list included with the default configuration cannot be changed

Format aaa authentication login {<listname> | default | network} *method1 [method2…]*

Parameter	Definition
default	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
listname	Character string of up to 15 characters used to name the list of authentication methods activated when a user logs in.
method1…	At least one from the following:

[method2…]	enable. Uses the enable password 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.

Default . defaultList. Used by the console and only contains the method local.
. networkList. Used by telnet and SSH and only contains the method local.

Mode Global Config

Example: The following shows an example of the command.

```
(M4500-32C) (Config)#aaa authentication login default radius local enable none
```

5.11.4. no aaa authentication login

This command returns to the default.

Format no aaa authentication login {<listname> | default | network}

Mode Global Config

5.11.5. aaa accounting

Use this command in Global config mode to create an accounting method list for either user EXEC sessions or for user-executed commands. This list is identified by **default** or a user-specified **listname**. 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: Please note the following:

- A maximum of five Accounting Method lists can be created for each exec and command type.
- 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.
- Only the default Accounting Method list can be created for DOT1X. There is no provision to create mode.

- 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 | <listname>} {start-stop | stop-only | none} *method1* [*method2*]

Parameter	Definition
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.
listname	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 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.

Mode Global Config

5.11.6. no aaa accounting

This command deletes the accounting method list.

Format no aaa accounting {exec | commands | dot1x} {default | <listname>}

Mode Global Config

Example: The following shows an example of the command.

```
(M4500-32C) (Config)#aaa accounting commands userCmdAudit stop-only tacacs

(M4500-32C) (Config)#no aaa accounting commands userCmdAudit
```

5.11.7. 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>}

Parameter	Definition
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 list of methods for accounting services.
listname	Enter a string of not more than 15 characters.

Mode Line Config

Example: The following shows an example of the command.

```
(M4500-32C) (Config)#line console

(M4500-32C) (Config-line)#accounting exec default

(M4500-32C) (Config-line)#exit
```

5.11.8. no aaa accounting

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

Format no accounting {exec | commands}

Mode Line Config

5.11.9. clear aaa ias-users

This command clears the IAS user database.

Format clear aaa ias-users

Mode Privileged Exec

Example:

```
(M4500-32C) #clear aaa ias-users

Are you sure you want to clear all IAS user entries (y/n) y

All Internal Authentication Server user database entries are cleared.
```

5.11.10. clear accounting statistics

This command clears the accounting statistics.

Format clear accounting statistics

Mode Privileged Exec

Example:

```
(M4500-32C) #clear accounting statistics
```

5.12. RADIUS Commands

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

5.12.1. show radius

This command displays the various RADIUS configuration items for the switch.

Format show radius

Mode Privileged EXEC

Display Message

Parameter	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.
Number of Retransmits	The configured value of the maximum number of times a request packet is retransmitted.
Timeout Duration	The configured timeout value, in seconds, for request retransmissions.
Dead Time (mins)	The configured timeout value, in minutes, for request re-transmissions.
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 attributes to be used in RADIUS requests.

RADIUS Attribute MS-CHAPv2 Mode	A global parameter to indicate whether the MS-CHAPv2 attributes have been enabled to use at RADIUS authentication.

Example: The following shows an example of the command.

```
(M4500-32C) #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 Retransmits.......................... 4

Timeout Duration............................... 5

Dead Time (mins)............................... 0

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 MS-CHAPv2 Mode................ Disable
```

5.12.2. show radius accounting

This command is used to display the configured RADIUS accounting mode, accounting server, and the statistics for the configured accounting server.

Format show radius accounting [<ip-address | ipv6-address | hostname> | name [<servername>] | statistics {<ip-address | ipv6-address | hostname> | name <servername>}]

Mode Privileged EXEC

Display Message

If you do not specify any parameters, then only the accounting mode and the RADIUS accounting server details are displayed.

Parameter	Definition
RADIUS Accounting Mode	A global parameter to indicate whether the accounting mode for all the servers is enabled or not.
Host Address	The IP address 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.

If the optional token '<ip-address | ipv6-address | hostname>' or 'name <servername>' is included.

Parameter	Definition
RADIUS Accounting Server IP Address	IP Address of the configured RADIUS accounting server.
RADIUS Accounting Server Name	The name of the configured RADIUS accounting server.
RADIUS Accounting Mode	A global parameter to indicate whether the accounting mode for all the servers is enabled or not.
Link local interface	Indicate the outgoing interface for link local 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.

If the optional token 'statistics <ip-address | ipv6-address | hostname>' is included, the statistics for the configured RADIUS accounting server are displayed. The IP address parameter must match that of a previously configured RADIUS accounting server. The following information regarding the statistics of the RADIUS accounting server is displayed.

Parameter	Definition
RADIUS Accounting Server Host Address	IP Address of the configured RADIUS accounting server.
Round Trip Time	The time interval in centiseconds, between the most recent Accounting-Response and the Accounting-Request that matched it from the RADIUS accounting server.
Requests	The number of RADIUS Accounting-Request packets sent to this accounting server. This number does not include retransmissions.

Retransmissions	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 and 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 an example of the command.

(M4500-32C) #show radius accounting

```
RADIUS Accounting Mode..................... Disable

Host Address............................... 10.0.0.1

Port....................................... 1813

Secret Configured.......................... No


(M4500-32C) #show radius accounting 10.0.0.1


RADIUS Accounting Server IP Address..... 10.0.0.1

RADIUS Accounting Server Name.............. Default-RADIUS-Server

RADIUS Accounting Mode..................... Disable

Port....................................... 1813

Secret Configured.......................... No
```

```
(M4500-32C) #show radius accounting name

Server Name                     Host Address             Port    Secret
                                                                 Configured
------------------------------- ------------------------ ------- ----------
Default-RADIUS-Server           10.0.0.1                 1813    No

(M4500-32C) #show radius accounting statistics 10.0.0.1

RADIUS Accounting Server Host Address.......... 10.0.0.1
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
```

5.12.3. show radius servers

This command is used to display items of the configured RADIUS servers.

Format show radius servers [<ip-address | ipv6-address | hostname> | name [<servername>]]

Mode Privileged EXEC

Display Message

If you do not specify any parameters or only the token ‘name’, then only the RADIUS authentication server details are displayed.

Parameter	Definition
current	The ‘*’ symbol preceding the server host address specifies that the server is currently active.
ipaddr |Host Address	The IP address or host name of the authenticating server.
Server Name	The Name of the authenticating server.
Port	The port used for communication with the accounting server.
Type	Specifies whether this server is a primary or secondary type.
Usage	Specifies the server usage type is Login, Dot1x or All.
Secret Configured	Yes or No Boolean value indicating whether this server is configured with a secret.

If the optional token '<ip-address | ipv6-address | hostname>' or ‘name <servername>’ is included.

Parameter	Definition
RADIUS Server IP Address	The IP address or host name of the authenticating server.
RADIUS Server Name	The Name of the authenticating server.
Current Server IP Address	The IP address of the authenticating server.
Number of Retransmits	The configured value of the maximum number of times a request packet is retransmitted.
Timeout Duration	The configured timeout value, in seconds, for request re-transmissions.
Dead Time (mins)	The configured timeout value, in mins, for the time duration after a RADIUS sever is found non-responsive or dead.
RADIUS Accounting Mode	Indicates whether the accounting mode for the server is enabled or not.
RADIUS Attribute 4 Mode	Indicate whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.
RADIUS Attribute 4 Value	Specifies the IP address to be used in the NAS-IP-Address attribute to be used in RADIUS requests.
RADIUS Attribute 95 Mode	Indicate whether the NAS-IPv6-Address attribute has been enabled to use in RADIUS requests.

RADIUS Attribute 95 Value	Specifies the IPv6 address to be used in the NAS-IPv6-Address attribute to be used in RADIUS requests.
RADIUS Attribute MS-CHAPv2 Mode	Indicate whether the MS-CHAPv2 attributes have been enabled to use at RADIUS authentication.
Link local interface	Indicate the outgoing interface for link local address
Port	The port used for communication with the accounting server.
Type	Specifies whether this server is a primary or secondary type.
Usage Type	Specifies the server usage type is Login, Dot1x or All.
Secret Configured	Yes or No Boolean value indicating whether this server is configured with a secret.
Message Authenticator	The message authenticator attribute configured for the radius server.
Number of CoA Requests Received	Specifies the number of CoA Requests Received
Number of CoA ACK Responses Sent	Specifies the number of CoA ACK Responses Sent
Number of CoA NAK Responses Sent	Specifies the number of CoA NACK Responses Sent
Number of CoA Requests Ignored	Specifies the number of CoA Requests Ignored
Number of CoA Missing/Unsupported Attribute R	Specifies the number of CoA Missing/Unsupported Attribute Requests
Number of CoA Session Context Not Found Reque	Specifies the number of CoA Session Context Not Found Requests
Number of CoA Invalid Attribute Value Request	Specifies the number of CoA Invalid Attribute Value Requests
Number of Administratively Prohibited Request	Specifies the number of Administratively Prohibited Requests

Example: The following outputs show examples of the command.

```
M4500-48XF8C) #show radius servers

Current Host Address          Server Name                       Port  Type      Usage
---- ------------------------ --------------------------------- ----- --------- --------
     10.27.65.114             Default-RADIUS-Server             1812  Secondary Both
  *  10.27.65.103             Default-RADIUS-Server             1812  Primary   Both

 * currently selected server


(M4500-32C) #show radius servers name

Server Name             Host Address   Port     Secret
                                                Configured
----------------------  -------------  -------  ----------
Default-RADIUS-Server   192.168.100.1  1812     No


M4500-32C) #show radius servers 192.168.100.1

RADIUS Server IP Address..................... 192.168.100.1
RADIUS Server Name........................... Default-RADIUS-Server
Number of Retransmits........................ 4
Timeout Duration............................. 5
Dead Time (mins)............................. 0
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.................... ::
Port......................................... 1812
Type......................................... Secondary
Usage Type................................... both
Secret Configured............................ No
Message Authenticator........................ Enable
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
```

5.12.4. show radius statistics

This command is used to display the statistics for RADIUS or configured server. To show the configured RADIUS server statistic, the IP Address specified must match that of a previously configured RADIUS server. On execution, the following fields are displayed.

Format show radius statistics {<ipaddress | ipv6-address|hostname> | name <servername>}

Mode Privileged EXEC

Display Message

Parameter	Definition
RADIUS Server Name	The Name of the authenticating server.
Server Host Address	The IP address or host name of the authenticating server.
Round Trip Time	The time interval, in hundredths of a second, between the most recent Access-Reply, Access - Challenge and the Access-Request that matched it from the RADIUS authentication server.
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, which were received from this server.
Access Rejects	The number of RADIUS Access-Reject packets, including both valid and invalid packets, which were received from this server.
Access Challenges	The number of RADIUS Access-Challenge packets, including both valid and invalid packets, which 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 RADIUS packets of unknown types, which 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 an example of the command.

```
(M4500-32C) #show radius statistics 192.168.100.1


RADIUS Server Name..............................  Default-RADIUS-Server

Server Host Address.............................  192.168.100.1

Round Trip Time.................................  0.00

Access Requests.................................  0

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
```

5.12.5. show radius source-interface

This command is used 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

Display Message

Parameter	Definition
RADIUS Client Source Interface	The interface to use as the source interface for RADIUS client.
RADIUS Client Source IPv4 Address	The IP address of the interface configured as the RADIUS client source interface.

5.12.6. authentication network radius

This command enables the switch to accept VLAN assignment by the radius server.

Format authorization network radius

Default Disable

Mode Global Config

5.12.7. no authorization network radius

This command disables the switch to accept VLAN assignment by the radius server.

Format no authorization network radius

Mode Global Config

5.12.8. clear radius dynamic-author statistics

This command clear radius dynamic authorization counters.

Format clear radius dynamic-author statistics

Mode Privileged EXEC

Example:

(M4500-32C) #clear radius dynamic-author statistics

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

Statistics cleared.

5.12.9. radius accounting mode

This command is used to enable RADIUS accounting function.

Format radius accounting mode

Default Disable

Mode Global Config

5.12.10. no radius accounting mode

This command is used to set the RADIUS accounting function to the default value.

Format no radius accounting mode

Mode Global Config

5.12.11. radius server attribute 4

This command specifies the RADIUS client to use the NAS-IP Address attribute in the RADIUS requests. 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.

Format radius server attribute 4 [<ipaddr>]

Parameter	Definition
4	NAS-IP-Address attribute to be used in RADIUS requests.
ipaddr	The IP address of the server.

Default None

Mode Global Config

5.12.12. no radius server attribute 4

This command disables the NAS-IP-Address attribute global parameter for RADIUS client. When this parameter is disabled, the RADIUS client does not send the NAS-IP-Address attribute in RADIUS requests.

Format no radius server attribute 4

Mode Global Config

5.12.13. radius server attribute 95

This command specifies the RADIUS client to use the NAS-IPv6 Address attribute in the RADIUS requests. 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.

Format radius server attribute 95 [<ipv6-address>]

Parameter	Definition
95	NAS-IPv6-Address attribute to be used in RADIUS requests.
ipv6-address	The IPv6 address of the server.

Default None

Mode Global Config

5.12.14. no radius server attribute 95

This command disables the NAS-IPv6-Address attribute global parameter for RADIUS client. When this parameter is disabled, the RADIUS client does not send the NAS-IP-Address attribute in RADIUS requests.

Format no radius server attribute 95

Mode Global Config

5.12.15. radius server attribute mschapv2

This command is used to enable switch to support the version two of Microsoft Challenge-Handshake Authentication Protocol (MS-CHAPv2). When this parameter is enabled, the RADIUS client will use MS-CHAPv2 attributes at user login authentication.

Format RADIUS server attribute mschapv2

Parameter	Definition
machapv2	MS-CHAPv2 attributes to be used at RADIUS authenticaton.

Default None

Mode Global Config

5.12.16. no radius server attribute mschapv2

This command disables the MS-CHAPv2 attributes for RADIUS authentication.

Format no radius server attribute mschapv2

Mode Global Config

5.12.17. radius server deadtime

This command configures radius server dead time.

Format radius server deadtime <minutes>

Default 0

Mode Global Config

5.12.18. no radius server deadtime

This command is used to set dead time to the default value.

Format no radius server deadtime

Mode Global Config

5.12.19. radius server host

This command configures the IP address or DNS name to use for communicating with the RADIUS server of a selected server type. While configuring the IP address or DNS name for the authenticating or accounting servers, you can also configure the port number and server name. If the authenticating and accounting servers are configured without a name, the command uses the 'Default-RADIUS-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.

If the '**auth**' token is used, the command configures the IP address to use to connect to a RADIUS authentication server. Up to 3 servers can be configured per RADIUS client. If the maximum number of configured servers is reached, the command will fail until one of the servers is removed by executing the no form of the command. If the optional *port* parameter is used, the command will configure the UDP port number to use to connect to the configured RADIUS server. In order to configure the UDP port number, the IP address must match that of a previously configured RADIUS authentication server. The *port* number range is 1 - 65535, with 1812 being the default value.

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

If the '**acct**' token is used, the command configures the IP address to use for the RADIUS accounting server. Only a single accounting server can be configured. If an accounting server is currently configured, it must be removed from the configuration using the no form of the command before this command succeeds. If the optional *port* parameter is used, the command will configure the UDP port to use to connect to the RADIUS accounting server. The IP address specified must match that of a previously configured accounting server. If a port is already configured for the accounting server then the new port will replace the previously configured value. The port must be a value in the range 1 - 65535, with 1813 being the default value.

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

Format radius server host auth <ip-addr| ipv6-address | hostname> [name <servername>] [port <port>] [usage-type <8021x|login|both>]

radius server host acct <ip-addr| ipv6-address | hostname> [name <servername>] [port <port>]

Parameter	Definition
ip-addr | ipv6-address | hohstname	This field is an IPv4 or IPv6 address or a hostname
servername	Server name
port	Port number in the range 1-65535
usage-type	Configure the Radius server usage type. The type could be – 802.1x, login, or both

Default None

Mode Global Config

5.12.20. 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|hostname* parameter must match the IP address or hostname of the previously configured RADIUS authentication / accounting server.

Format no radius server host {acct | auth} <ip-addr| ipv6-address | hostname>

Mode Global Config

Example: The following shows an example of the command.

```
(M4500-32C) (Config) #radius server host acct 192.168.37.60

(M4500-32C) (Config) #radius server host acct 192.168.37.60 port 1813

(M4500-32C) (Config) #radius server host auth 192.168.37.60 name Network1_RS port 1813

(M4500-32C) (Config) #radius server host acct 192.168.37.60 name Network2_RS

(M4500-32C) (Config) #no radius server host acct 192.168.37.60
```

5.12.21. 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.

Format radius server host auth link-local <link-local-address> interface {<slot/port> | serviceport} [name <servername>] [port <port>] [usage-type <8021x|login|both>]

radius server host acct link-local <link-local-address> interface {<slot/port> | serviceport} [name <servername>] [port <port>]

Parameter	Definition
link-local	Specify the link local address
interface	Specify the outgoing interface for link local address
servername	Server name
port	Port number in the range 1-65535
usage-type	Configure the Radius server usage type. The type could be – 802.1x, login, or both

Default None

Mode Global Config

5.12.22. no radius server host link-local

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

Format no radius server host {acct | auth} link-local <link-local-address>

Mode Global Config

5.12.23. radius server key

This command is used to configure the shared secret between the RADIUS client and the RADIUS accounting / authentication server. Depending on whether the **'auth'** or **'acct'** token is used, the shared secret will be configured for the RADIUS authentication or RADIUS accounting server. The IP address provided must match a previously configured server. When this command is executed, the secret will be prompted. The secret must be an alphanumeric value not exceeding 20 characters.

Format radius server key {acct | auth} <ipaddress| ipv6-address | hostname> [encrypted <password>]

Default None

Mode Global Config

Example: The following shows an example of the command.

```
(M4500-32C) (Config) # radius server key auth 192.168.37.60

Enter secret (64 characters max):******

Re-enter secret:******
```

5.12.24. radius server primary

This command is used to configure the primary RADIUS authentication server for this RADIUS client. The primary server is the one that is used by default for handling RADIUS requests. The remaining configured servers are only used if the primary server cannot be reached. A maximum of three servers can be configured on each client. Only one of these servers can be configured as the primary. If a primary server is already configured prior to this command being executed, the server specified by the IP address specified used in this command will become the new primary server. The IP address must match that of a previously configured RADIUS authentication server.

Format radius server primary <ipaddress | ipv6-address | hostname>

Default None

Mode Global Config

5.12.25. radius server retransmit

This command sets the maximum number of times a request packet is re-transmitted when no response is received from the RADIUS server. The retries value is an integer in the range of 1 to 15.

Format radius server retransmit <retries>

Default 4

Mode Global Config

5.12.26. no radius server retransmit

This command is used to set the maximum number of retries to the default value.

Format no radius server retransmit

Mode Global Config

5.12.27. 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.

Format radius server timeout <seconds>

Default 5

Mode Global Config

5.12.28. no radius server timeout

This command is used to set the timeout value to the default value.

Format no radius server timeout

Mode Global Config

5.12.29. 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> | serviceport | tunnel <tunnel-id> | vlan <vlan-id> }

Parameter	Definition
slot/port	Specifies the interface 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 63.
tunnel-id	Specifies the tunnel interface. The range of the tunnel ID is 0 to 7.
vlan-id	Specifies the VLAN interface to use as the source interface. The range of VLAN ID is 1 to 4093.

Default None

Mode Global Config

5.12.30. 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

5.13. 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.

5.13.1. show tacacs

This command displays configured information and statistics of a TACACS+ server.

Format show tacacs [<ip-address | hostname>]

Mode Privileged EXEC

Display Message

Parameter	Definition
Host address	The IP address or hostname of the configured TACACS+ server.
Port	Shows the configured TACACS+ server port number.
Timeout	Shows the timeout in seconds for establishing a TCP connection.
Priority	Shows the preference order in which TACACS+ servers are contacted. If a server connection fails, the next highest priority server is contacted.
Link Local Interface	Shows the outgoing interface used by the link-local address

Example: The following shows an example of the command.

```
(M4500-32C) (Config)#show tacacs


Global Timeout: 10


Host address            Port     Timeout   Priority
----------------------  ------   -------   --------
10.0.0.1                49       Global    0
```

5.13.2. 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

Display Message

Parameter	Definition
TACACS Client Source Interface	The interface to use as the source interface for TACACS client.
TACACS Client Source IPv4 Address	The IP address of the interface configured as the TACACS client source interface.
TACACS Client Source IPv6 Address	The IPv6 address of the interface configured as the TACACS client source interface.

5.13.3. 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. The *ipaddr|hostname* parameter is the IPv4 or IPv6 address or hostname of the TACACS+ server. To specify multiple hosts, multiple **tacacs-server host** commands can be used.

Format tacacs-server host <ipaddress | ipv6-address | hostname>

Mode Global Config

no tacacs-server host

This command deletes the specified hostname or IP address.

Format no tacacs-server host <ip-address | ipv6-address | hostname>

Mode Global Config

5.13.4. tacacs-server host link-local

Use the **tacacs-server host link-local** command in Global Configuration mode 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 or the service port.

Format tacacs-server host link-local <link-local-address> interface {serviceport | <slot/port>}

Mode Global Config

5.13.5. no tacacs-server host link-local

This command revmoes the configured TACACS+ server link-local address.

Format no tacacs-server host link-local <link-local-address>

Mode Global Config

5.13.6. tacacs-server key

This command is used to configure the TACACS+ authentication and encryption key. You can configure the format of the key in two ways:

- Type the **key** keyword to configure the key in plain text. The key is displayed with * for each character that you type. The key must be in alphanumeric characters with a maximum length of 128 characters.
- Type the **key encrypted** keyword to configure the key in encrypted form. The <key-string> argument must be in hexadecimal digits with a length of 256 characters.

Format tacacs-server key [encrypted <key-string>]

Mode Global Config

5.13.7. no tacacs-server key

This command removes the TACACS+ server secret key.

Format no tacacs-server key

Mode Global Config

5.13.8. tacacs-server keystring

This command is used to set the global authentication encryption key used for all TACACS+ communications between the TACACS+ server and the client.

Note: The length of the secret key is up to 128 characters.

Format tacacs-server keysting

Mode Global Config

Example: The following shows an example of the command.

```
(M4500-32C) # tacacs-server keystring


Enter key:**********


Re-enter key:**********
```

5.13.9. tacacs-server timeout

This command is used to configure the timeout value for communication with the TACACS+ servers. The *timeout* parameter has a range of 1 to 30 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.

Format tacacs-server timeout [<timeout>]

Default 10

Mode Global Config

5.13.10. no tacacs-server timeout

This command restores the default timeout value for all TACACS+ servers.

Format no tacacs-server timeout

Mode Global Config

5.13.11. key

This command is used to configure the TACACS+ authentication and encryption key. You can configure the format of the key in two ways:

- Type the **key** keyword to configure the key in plain text. The key is displayed with * for each character that you type. The key must be in alphanumeric characters with a maximum length of 128 characters.
- Type the **key encrypted** keyword to configure the key in encrypted form. The <key-string> argument must be in hexadecimal digits with a length of 256 characters.

Format key [encrypted <key-string>]

Mode TACACS server Config

5.13.12. no key

This command removes the TACACS+ server secret key.

Format no key

Mode TACACS server Config

5.13.13. keystring

This command is used to set the TACACS+ server-specific authentication encryption key used for all TACACS+ communications between the TACACS+ server and the client.

Note: The length of the secret key is up to 128 characters.

Format keysting

Mode TACACS server Config

5.13.14. port

This command is used to set the TACACS+ server-specific port number. The server *port-number* range is 0 to 65535.

Format port [<port-number>]

Default 49

Mode TACACS server Config

5.13.15. no port

This command set the TACACS+ server-specific port to default.

Format no port

Mode TACACS server Config

5.13.16. priority

This command is used to set the TACACS+ server-specific authentication host priority. The server priority range is 0 to 65535.

Format priority [<priority>]

Default 0

Mode TACACS server Config

5.13.17. no priority

This command set the TACACS+ server-specific authentication host priority to default.

Format no priority

Mode TACACS server Config

5.13.18. timeout

This command is used to configure the timeout value for communication with the TACACS+ servers. The *timeout* parameter has a range of 1 to 30 seconds.

Format timeout [<timeout>]

Default 10

Mode TACACS server Config

5.13.19. no timeout

This command set the timeout value for communication with the TACACS+ servers to default.

Format no timeout

Mode TACACS server Config

5.13.20. tacacs-server source-interface

Use this command in Global config 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> | serviceport | tunnel <tunnel-id> | vlan <vlan-id>}

Parameter	Definition
slot/port	Specifies the interface 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 63.
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 interface to use as the source interface. The range of VLAN ID is 1 to 4093.

Default None

Mode Global Config

5.13.21. 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

5.13.22. clear tacacs

This command clears the TACACS configuration.

Format clear tacacs

Mode Privileged Exec

Example:

```
(M4500-32C) # clear tacacs

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

No TACACS servers configured.
```

5.14. Security Commands

This section describes the commands you use to configure 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 discards.

Note: To enable the SNMP trap specific to port security, see “snmp-server enable traps violation”.

5.14.1. 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, port-channel, or on all interfaces.

Format show port-security [{<slot/port> | all | port-channel <portchannel-id>}]

Mode Privileged EXEC

User EXEC

Display Message

If you do not use the optional parameters *slot/port*, all, or port-channel <id>, then the command displays following information.

Parameter	Definition
Administrative Mode	Port Locking mode for the entire system. The field displays if you do not support 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.
Violation Shutdown	Whether violation shutdown mode are enabled.
Sticky Mode	Whether sticky mode are enabled.

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

```
(M4500-32C) #show port-security

Port Security Administration Mode: Disabled


(M4500-32C) #show port-security 0/1


        Admin       Dynamic   Static    Violation     Violation     Sticky
Intf    Mode        Limit     Limit     Trap Mode     Shutdown      Mode
------  ----------- --------  --------  ------------- ------------  --------
0/1     Disabled    600       20        Disabled      Disabled      Disabled
```

5.14.2. show port-security dynamic

This command displays the dynamically locked MAC address for the port.

Format show port-security dynamic {<slot/port> | port-channel <portchannel-id>}

Mode Privileged EXEC
User EXEC

Display Message

Parameter	Definition
MAC AddressDynamically learned MAC Address	MAC Address of dynamically locked MAC
VLAN ID	VLAN ID on which the MAC address was learnt.
Number of Dynamic MAC addresses learned	The number of dynamic MAC addresses learned

5.14.3. show port-security static

This command displays the statically locked MAC address for port.

Format show port-security static {<slot/port> | port-channel <portchannel-id>}

Mode Privileged EXEC
User EXEC

Display Message

Parameter	Definition
Number of static MAC addresses configured	The number of static MAC addresses configured
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.

```
 (M4500-32C) #show port-security static 0/1


Number of static MAC addresses configured: 1


 Statically configured MAC Address   VLAN ID   Sticky

 ---------------------------------   -------   ------

 00:00:01:01:00:00                   2         No
```

5.14.4. show port-security violation

This command displays the source MAC address of the last packet discarded on a locked port.

Format show port-security violation {<slot/port> | port-channel <portchannel-id>}

Mode Privileged EXEC
User EXEC

Display Message

Parameter	Definition
Last Violation MAC AddressMAC 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.

5.14.5. port-security

This command enables port locking at the system level (Global Config) or port level (Interface Config) on an interface, a range of interfaces.

Format port-security

Default Disabled

Mode Global Config
Interface Config

5.14.6. no port-security

This command disables port locking for one or a range of ports (Interface Config) or all (Global Config) ports.

Format no port-security

Mode Global Config
Interface Config

5.14.7. port-security max-dynamic

This command sets the maximum number of dynamically locked MAC addresses allowed on a specific port.

Format port-security max-dynamic <0-600>

Default 600

Mode Interface Config

5.14.8. 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

5.14.9. port-security max-static

This command sets the maximum of statically locked MAC addresses allowed on a specific port.

Format port-security max- static <0-20>

Default 20

Mode Interface Config

5.14.10. no port-security max-static

This command resets the maximum number of statically locked MAC addresses allowed on a specific port to its default value.

Format no port-security max- static

Mode Interface Config

5.14.11. port-security mac-address

This command adds a MAC address to the list of statically locked MAC addresses

Format port-security mac-address <mac-address> <vlan-id>

Default None

Mode Interface Config

5.14.12. 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> <vlan-id>

Mode Interface Config

5.14.13. port-security mac-address move

This command converts dynamically locked MAC addresses to statically locked MAC addresses for an interface or a range of interfaces

Format port-security mac-address move

Default None

Mode Interface Config

5.14.14. 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 Global command applies the "sticky" mode to all valid interfaces (physical and port-channel). 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-address> <vid>**" entries. This distinguishes them from the static entries.

Format port-security mac-address sticky [<mac-address> <vlan-id>]

Default None

Mode Global Config
Interface Config

5.14.15. no port-security mac-address sticky

This command removes the sticky mode. The sticky MAC address can be deleted by using the command "**no port-security mac-address <mac-address> <vlan-id>**".

Format no port-security mac-address sticky

Mode Global Config
Interface Config

Example: The following shows an example of the command.

(M4500-32C) (Config)#port-security mac-address sticky

(M4500-32C) (Interface 0/1)#port-security mac-address sticky

(M4500-32C) (Interface 0/1)#port-security mac-address sticky 00:00:00:00:00:01 2

5.14.16. port-security violation shutdown

This command configures the port violation shutdown mode. Once the violation happens, the interface will be shutdown

Format port-security violation shutdown

Default Disabled

Mode Interface Config

5.14.17. no port-security violation

This command restores violation mode to the default value.

Format no port-security violation

Mode Interface Config

5.15. LLDP (Link Layer Discovery Protocol) Commands

5.15.1. show lldp

This command is used to display a summary of the current LLDP configuration.

Format show lldp

Default None

Mode Privileged Exec

Display Message

Term	Definition
Transmit Interval	Shows how frequently the system transmits local data LLDPDUs, in seconds.
Transmit Hold Multiplier	Shows the multiplier on the transmit interval that sets the TTL in local data LLDPDUs.
Reinit Delay	Shows the delay before re-initialization, in seconds.
Notification Interval	Shows how frequently the system sends remote data change notifications, in seconds.
Transmit Delay	Shows how frequently the system transmits local data LLDPDUs after a change is made in a TLV (type, length, or value) element in LLDP, in seconds.
Management-address Source Interface	Shows the source of the management interface

5.15.2. show lldp interface

This command is used to display a summary of the current LLDP configuration for a specific interface or for all interfaces.

Format show lldp interface [<slot/port>]

Default None

Mode Privileged Exec

Display Message

Term	Definition
Interface	Shows 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.

5.15.3. show lldp statistics

This command is used to display the current LLDP traffic and remote table statistics for a specific interface or for all interfaces.

Format show lldp statistics [<slot/port>]

Default None

Mode Privileged Exec

Display Message

Term	Definition
Last Update	Shows 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.
Interface	Shows the interface in slot/port format.
Tx Total	Total number of LLDP packets transmitted on the port.
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.
Ageout	Total number of times a complete remote data entry was deleted for the port because the Time to Live interval expired.
TLV Discards	Shows the number of TLVs discarded.
TLV Unknowns	Total number of LLDP TLVs received on the port where the type value is in the reserved range, and not recognized.
TLV 802.1	Total number of LLDP TLVs received on the port where the type value is 127 and OUI type is 00-80-C2.
TLV 802.3	Total number of LLDP TLVs received on the port where the type value is 127 and OUI type is 00-12-0F.

5.15.4. show lldp remote-device

This command is used 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>]

Default None

Mode Privileged Exec

Display Message

Term	Definition
Local Interface	Identifies the interface that received the LLDPDU from the remote device.
Rem ID	Shows the ID of the remote device.
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	Shows the port number that transmitted the LLDPDU.
System Name	Shows the system name of the remote device

5.15.5. show lldp remote-device detail

This command is used to display detailed information about remote devices that transmit current LLDP data to an interface on the system.

Format show lldp remote-deveice detail <slot/port>

Default None

Mode Privileged Exec

Display Message

Term	Definition
Local Interface	Identifies 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	Shows the type of identification used in the Chassis ID field.
Chassis ID	Identifies the chassis of the remote device.
Port ID Subtype	Identifies the type of port on the remote device.
Port ID	Shows the port number that transmitted the LLDPDU.
System Name	Shows 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	Shows the amount of time (in seconds) the remote device's information received in the LLDPDU should be treated as valid information.
MAC/PHY Configuration/Status	**Auto-Negotitation:** Identifies the auto-negotiation support and current status of the remote device.

	PMD Auto-Negotitation Advertised Capabilities: The duplex and bit-rate capability of the port of the remote device. **Operational MAU Type:** Displays the MAU type. The MAU performs physical layer functions, including digital data conversion from the Ethernet interfaces' collision detection and bit injection into the network.
Power Via MDI	**MDI Power Support:** The MDI power capabilities and status. **PSE Power Pair:** Indicates the way of feeding the voltage to the data cable. **Power Class:** PoE power class.
Link Aggregation	**Aggregation Status:** Indicates the link aggregation capabilities and the current aggregation status. **Aggregation Port Id:** Aggregated port identifier.
Maximum Frame Size	Shows the maximum frame size capability of the implemented MAC and PHY of the remote device.
Port VLAN Identity	Shows the PVID of the connected port of the remote device.
Protocol VLAN	**Status:** Indicates the port and protocol VLAN capability and status. **ID:** The PPVID number for the port of the remote device.
VLAN Name	Shows the name of the VLAN which the connected port is in.
Protocol Identity	Shows the particular protocols that are accessible through the port of the remote device.

5.15.6. show lldp local-device

This command is used 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>]

Default None

Mode Privileged Exec

Display Message

Term	Definition
Interface	Identifies the interface in a slot/port format.

Port ID	Shows the port ID associated with this interface.
Port Description	Shows the port description associated with the interface.

5.15.7. show lldp local-device detail

This command is used to display detailed information about the LLDP data a specific interface transmits.

Format show lldp local-deveice detail <slot/port>

Default None

Mode Privileged Exec

Display Message

Term	Definition
Interface	Identifies the interface that sends the LLDPDU.
Chassis ID Subtype	Shows the type of identification used in the Chassis ID field.
Chassis ID	Identifies the chassis of the local device
Port ID Subtype	Identifies the type of port on the local device.
Port ID	Shows the port number that transmitted the LLDPDU.
System Name	Shows 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. 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	The type of address and the specific address the local LLDP agent uses to send and receive information.
MAC/PHY Configuration/Status	**Auto-Negotitation:** Identifies the auto-negotiation support and current status of the local device.

	PMD Auto-Negotitation Advertised Capabilities: The duplex and bit-rate capability of the port of the local device. **Operational MAU Type:** Displays the MAU type. The MAU performs physical layer functions, including digital data conversion from the Ethernet interfaces' collision detection and bit injection into the network.
Power Via MDI	**MDI Power Support:** The MDI power capabilities and status. **PSE Power Pair:** Indicates the way of feeding the voltage to the data cable. **Power Class:** PoE power class.
Link Aggregation	**Aggregation Status:** Indicates the link aggregation capabilities and the current aggregation status. **Aggregation Port Id:** Aggregated port identifier.
Maximum Frame Size	Shows the maximum frame size capability of the implemented MAC and PHY of the local device.
Port VLAN Identity	Shows the PVID of the port.
VLAN Name	Shows the name of the VLAN which the port is in.
Protocol Identity	Shows the particular protocols that are accessible through the port.

5.15.8. show lldp dcbx interface

This command is used to display the local Data Center Bridging Capability Exchange (DCBX) control status of an interface on the system.

Format show lldp dcbx interface [<slot/port> [detail]]

Default None

Mode Privileged Exec

Display Message

Term	Definition
Is configuration source selected	Is any interface configured configuration source or not.
Configuration source port	The interface that is configured as the configuration source.
Interface	Specifies all the ports on which DCBX can be configured.

Status	Specifies the DCBX status of the interfaces.
Role	Specifies the DCBX role on the interfaces.
Version	Specifies the DCBX version on the interfaces.
DCBX Tx	Total number of transmitted DCBX TLV(s) on the interfaces.
DCBX Rx	Total number of received DCBX TLV(s) on the interfaces.
DCBX Error	Total number of error DCBX TLV(s) on the interfaces.
unknown TLV	Total number of unknown DCBX TLV(s) on the interfaces.
DCBX operational status	Specifies the DCBX status of the interface.
Configured DCBX version	Specifies the DCBX version on this interface.
Peer DCBX version	Specifies the DCBX version of the peer device.
Peer MAC	Specifies the MAC address of the peer device.
Peer Description	Specifies the description of the peer device.
Auto-configuration Port Role	Specifies the DCBX role on this interface.
Peer Is configuration Source	Is peer device configured configuration source or not.
Error counters	Total number of error DCBX TLV(s) on this interface.
PFC incompatible configuration	Total number of PFC incompatible configuration on this interface.
Disappearing neighbor	Total number of Disappearing neighbor on this interface.
Multiple neighbors detected	Total number of Multiple neighbors detected on this interface.
Local configuration	Specifies the configuration of the local device.
PFC configuration	Specifies the PFC configuration of the local device.
Application priority (Tx enabled/disabled)	Specifies the mapping of the specific application to the priority of the local device.
Peer configuration	Specifies the configuration of the peer device.

PFC configuration	Specifies the PFC configuration of the peer device.
Application priority (Tx enabled/disabled)	Specifies the mapping of the specific application to the priority of the peer device.

Note: Local DCBX configuration shown is configured according to:

(1) Configuration set by user via PFC commands (priority-flow-control) for manual ports. (Note: We currently do not provide command to manually configure local application priority)

(2) Configuration propagated internally by the configuration source for auto-down ports and auto-up ports not selected as configuration source.

(3) Configuration received from peer for manually selected or auto-detected configuration source.

5.15.9. show lldp tlv-select interface

This command is used to display the DCBX TLV configuration of an interface on the system.

Format show lldp tlv-select interface [<slot/port>]

Default None

Mode Privileged Exec

Display Message

Term	Definition
Interface	Specifies all the ports on which DCBX TLV can be configured.
PFC	Specifies the DCBX priority flow control TLV on the interfaces.
App priority	Specifies the DCBX application-priority TLV on the interfaces.

5.15.10. show lldp remote-comparison

This command is used to display LLDP comparison between remote & local interface on the system.

Format show lldp remote-comparison [<slot/port>]

Default None

Mode Privileged Exec

Display Message

Term	Definition
LLDP Comparison	Specifies all the difference of TLVs between remote interface & local interface.

5.15.11. lldp notification

This command is used to enable remote data change notifications.

Format lldp notification

Default Disabled

Mode Interface Config

5.15.12. no lldp notification

This command is used to disable notifications**.**

Format no lldp notification

Mode Interface Config

5.15.13. lldp notification-interval

This command is used to configure how frequently the system sends remote data change notifications. The <interval-seconds> parameter is the number of seconds to wait between sending notifications. The valid interval range is 5-3600 seconds.

Format lldp notification-interval <interval-seconds>

Default 5

Mode Global Config

5.15.14. no lldp notification-interval

This command is used to return the notification interval to the default value.

Format no lldp notification-interval

Mode Global Config

5.15.15. lldp receive

This command is used to enable the LLDP receive capability.

Format lldp receive

Default Enable

Mode Interface Config

5.15.16. no lldp receive

This command is used to return the reception of LLDPDUs to the default value.

Format no lldp receive

Mode Interface Config

5.15.17. lldp transmit

This command is used to enable the LLDP advertise capability.

Format lldp transmit

Default Enable

Mode Interface Config

5.15.18. no lldp transmit

This command is used to return the local data transmission capability to the default.

Format no lldp transmit

Mode Interface Config

5.15.19. lldp transmit-mgmt

This command is used to include transmission of the local system management address information in the LLDPDUs.

Format lldp transmit-mgmt

Default None

Mode Interface Config

5.15.20. no lldp transmit-mgmt

This command is used to cancel inclusion of the management information in LLDPDUs.

Format no lldp transmit-mgmt

Mode Interface Config

5.15.21. lldp transmit-tlv

This command is used to specify which optional type length values (TLVs) in the 802.1AB basic management set are transmitted in the LLDPDUs. Use sys-name to transmit the system name TLV. To configure the system name, please refer to “snmp-server” command. Use sys-descto transmit the system description TLV. Use sys-cap to transmit the system capabilities TLV. Use port-desc to transmit the port description TLV. To configure the port description, please refer to “description” command. Use org-spec to transmit the organization specific TLV.

Format lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc] [org-spec]

Default None

Mode Interface Config

5.15.22. no lldp transmit-tlv

This command is used 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] [org-spec]

Mode Interface Config

5.15.23. lldp timers

This command is used 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 5-32768 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 re-initialization, and the range is 1-10 seconds.

Format lldp timers [interval <interval-seconds>] [hold <hold-value>] [reinit <reinit-seconds>]

Default Interval-seconds 30

Hold-value 4

Reinit-seconds 2

Mode Global Config

5.15.24. no lldp timers

This command is used 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

5.15.25. lldp tx-delay

This command is used to set the timing parameters for data transmission delay on ports enabled for LLDP. The <delay-seconds> determines the number of seconds to wait between transmitting local data LLDPDUs. The range is 1-8192 seconds.

Format lldp tx-delay <delay-seconds>

Default 2

Mode Global Config

5.15.26. no lldp tx-delay

This command is used to return the transmit delay to the default value.

Format no lldp tx-delay

Mode Global Config

5.15.27. lldp dcbx version

This command is used 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.

Format lldp dcbx version <auto | cee | cin | ieee>

Term	Definition
auto	Configure the switch to auto detect the peer DCBX version.
cee	Configure the switch to operate according to standard cee 1.06.
cin	Configure the switch to operate according to DCBX standard CIN 1.0.
ieee	Configure the switch to operate according to standard IEEE 802.1Qaz.

Default Auto

Mode Global Config

Note: Application priority is only supported in IEEE mode with application selector 2 (TCP) and 3 (UDP). ACL rules corresponding to the application-to-priority mapping(s) will only be added with application selector 2 and 3; mapping(s) with application selector other than 2 and 3 will be propagated internally and transmitted to peer(s) in application priority TLVs without actual effect in local device.

Current supported TLVs for each version are listed in the table below.

version	PFC	ETS Configuration	ETS Recommend	Application Priority
CEE	O	O	O	X
CIN	O	O	O	X
IEEE	O	O	O	O

5.15.28. no lldp dcbx version

Use the **no lldp dcbx version** to reset the value to default.

Format no lldp dcbx version

Mode Global Config

5.15.29. lldp dcbx port-role

This command is used to configure 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.

Format lldp dcbx port-role <auto-down | auto-up | configuration-source | manual>

Term	Definition
auto-down	Configure interface as auto-down stream. 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. An auto-downstream port that receives an internally propagated configuration overwrites its local configuration with the new parameter values. 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.
auto-up	Configure interface as auto-up stream. 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. A port that receives an internally propagated configuration overwrites its local configuration with the new parameter values. The first auto-upstream that is capable of receiving a peer configuration is elected as the configuration source. These ports have the willing bit enabled. These ports should be connected to FCFs.
configuration-source	Configure interface as 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. Note that coexistence of configuration sources is not allowed.
manual	Configure interface as manual port. 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.

Default Manual

Mode Interface Config

5.15.30. no lldp dcbx port-role

Use the **no lldp dcbx port-role** to reset this function to default.

Format no lldp dcbx port-role

Mode Interface Config

5.15.31. lldp tlv-select dcbxp

This command is used to send specific DCBX TLVs if LLDP is enabled to transmit on the given interface.

Format lldp tlv-select dcbxp [pfc | application-priority]

Term	Definition
pfc	Transmit DCBX priority flow control TLV.
application-priority	Transmit DCBX application-priority TLV.

Default PFC and application priority

Mode Global Config
Interface Config

Note: Application priority is only supported in IEEE mode with application selector 2 (TCP) and 3 (UDP). An IP access list named “AppPriACL” will be created with all auto-ports as inbound interfaces when the configuration source receives such information. ACL rule(s) corresponding to the application-to-priority mapping(s) will only be added with application selector 2 and 3; mapping(s) with other application selectors will be propagated internally and transmitted to peer in application priority TLVs without actual effect in local device. A maximum of 4 application-to-priority mappings are allowed.

5.15.32. no lldp tlv-select

Use the **no lldp tlv-select** 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 [pfc | application-priority]

Mode Global Config
Interface Config

5.15.33. lldp mgmt-address

This command is used to specify which management address is transmitted in the LLDPDUs.

Format lldp mgmt-address {vlan | serviceport | sys-mac}

Term	Definition
vlan	Configure the IP address on VLAN 1 as the management address
serviceport	Configure the IP address on service port as the management address
sys-mac	Configure the system MAC as the management address

Default serviceport

Mode Global Config

5.15.34. no lldp mgmt-address

Use the **no lldp mgmt-address** to reset this function to default value.

Format no lldp mgmt-address

Mode Global Config

5.15.35. lldp portid-subtype

This command is used to configure the port ID subtype field which is used to indicate how the port is being referenced in the Port ID field in LLDPDU.

Format lldp portid-subtype {interface-alias | interface-name | mac-address}

Term	Definition
interface-alias	Interface alias name (configured by "*description*" CLI command)
interface-name	Interface system name
mac-address	MAC address of the physical port

Default Interface-name

Mode Interface Config

5.15.36. no lldp portid-subtype

Use the **no lldp portid-subtype** to reset this function to default value.

Format no lldp portid-subtype

Mode Interface Config

5.15.37. data-center-bridging

This command enables the data-center bridging mode. In order to use the Data Center Bridging Capability Exchange (DCBX) command, you must first enable this mode.

Format data-center-bridging

Default Disabled

Mode Interface Config

5.16. System Utilities

This section describes the commands you use to help troubleshoot connectivity issues and to restore various configurations to their factory defaults.

5.16.1. Clear

5.16.1.1. clear arp

This command is used to remove all dynamic ARP entries from the ARP cache.

Format clear arp

Default None

Mode Privileged Exec

5.16.1.2. clear traplog

This command clears the trap log.

Format clear traplog

Default None

Mode Privileged Exec

5.16.1.3. clear eventlog

This command is used to clear the event log, which contains error messages from the system.

Format clear eventlog

Default None

Mode Privileged Exec

5.16.1.4. clear logging buffered

This command is used to clear the message log maintained by the switch. The message log contains system trace information.

Format clear logging buffered

Default None

Mode Privileged Exec

5.16.1.5. clear config

This command resets the configuration to the factory defaults without powering off the switch. You are prompted to confirm if the IP settings of service port would be kept and if the reset should proceed.

Format clear config

Default None

Mode Privileged Exec

5.16.1.6. 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

Default None

Mode Privileged Exec

5.16.1.7. clear counters

This command clears the statistics for a specified slot/port, for all the ports, for BHD counter, for loop-detection information, or for an interface on an assigned VLAN based or port channel ID.

Format clear counters [<slot/port> | bhd | port-channel <portchannel-id> | loop-detection | vlan <vlan-id> | all [vrf <vrf-name>]]

Default None

Mode Privileged Exec

5.16.1.8. clear vlan

This command resets VLAN configuration parameters to the factory defaults.

Format clear vlan

Default None

Mode Privileged Exec

5.16.1.9. clear igmp snooping

This command clears IGMP snooping entries from the MFDB table.

Format clear igmp snooping

Default None

Mode Privileged Exec

5.16.1.10. clear ip filter

This command is used to clear all IP filter entries.

Format clear ip filter

Default None

Mode Privileged Exec

5.16.1.11. clear dot1x authentication-history

This command is used to clear 802.1x authentication history table.

Format clear dot1x authentication-history [<slot/port>]

Default None

Mode Privileged Exec

5.16.1.12. clear radius statistics

This command is used to clear all RADIUS statistics.

Format clear radius statistics

Default None

Mode Privileged Exec

5.16.1.13. clear host

This command is used to delete entries from the host name-to-address cache, and it clears the entries from the DNS cache maintained by the software.

The parameter “hostname” means to deletes the cached entry which matches assigned hostname.

Format clear host <all | hostname >

Default None

Mode Privileged Exec

5.16.1.14. clear port-security dynamic

This command is used to clear an entry of dynamic MAC address in the port security table.

Format clear port-security dynamic [interface {<slot/port> | port-channel <1-64>} | mac-address <mac-address>] [vlan <1-4093>]

Default None

Mode Privileged Exec

5.16.1.15. clear ip arp-cache

This command is used to remove dynamic ARP entries which belong to assigned parameter type from ARP cache.

The parameter “gateway” means to clear the dynamic and gateway entries from the ARP cache.

Format clear ip arp-cache [gateway | interface {<slot/port> | vlan <vlan-id>} | vrf <vrf-name> [gateway]]

Default None

Mode Privileged Exec

5.16.1.16. clear lldp statistics

This command is used to reset LLDP (Link Layer Discovery Protocol) statistics.

Format clear lldp statistics

Default None

Mode Privileged Exec

5.16.1.17. clear lldp remote-data

This command is used to delete all information from the LLDP (Link Layer Discovery Protocol) remote data table, including MED-related information.

Format clear lldp remote-data

Default None

Mode Privileged Exec

5.16.1.18. clear ipv6 neighbors

This command is used to clear all entries in IPv6 neighbor table or an entry on a specific interface. Use the <slot/port> parameter to specify the interface.

Format clear ipv6 neighbors [<slot/port> | address <ipv6-address> | vlan <1-4093>]

Default None

Mode Privileged Exec

5.16.1.19. clear ipv6 statistics

This command is used to clear IPv6 statistics for all interfaces or for a specific interface, including loopback and tunnel 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 are reset to zero.

Format clear ipv6 statistics [<slot/port> | loopback <0-63> | tunnel <0-7> | vlan <1-4093>]

Default None

Mode Privileged Exec

5.16.1.20. clear ipv6 dhcp statistics

This command is used to clear DHCPv6 statistics for all interfaces.

Format clear ipv6 dhcp statistics

Default None

Mode Privileged Exec

5.16.1.21. clear ipv6 dhcp statistics per interface

This command is used to clear DHCPv6 statistics for a specific interface.

Format clear ipv6 dhcp interface {<slot/port> | vlan <1-4093>} statistics

Default None

Mode Privileged Exec

5.16.1.22. enable password

This command changes the password that is used to confirm that the user mode can be upgraded to Privileged EXEC mode. You can configure the format of the password in two ways:

- Type the **passwd** keyword to configure the key in plain text. The text that you type is displayed in asterisk characters. The <password> argument must be in alphanumeric characters with a maximum length of 64 characters.
- Type the **passwd 7** keywords to configure the key in encrypted form. The <password> argument must be in hexadecimal digits with a length of 128 characters.

Format [no] enable passwd [7 <password>]

Default None

Mode Global Config

In the following examples, the first example sets the password to “testPassword” in plain text. The second example sets the password to an encrypted string that is fixed at 128 hexadecimal digits.

```
(M4500-32C) (Config)# enable passwd

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

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

Password Changed!

(M4500-32C) (Config)#
```

```
(M4500-32C) (Config)# enable passwd 7
0fdd841c8a524979e5ba47893efcf48b12a08619953e1b6e42cde0931198ca717cb5ff8b4979
5a3497e283990827c5ba1ce32855ced76a505726dfb1ee222c4b
```

5.16.1.23. clear cpu-traffic counters

This command clears the CPU traffic counters on all interfaces.

Format clear cpu-traffic counters

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #clear cpu-traffic counters
```

5.16.1.24. clear cpu-traffic traces

This command clears the CPU traffic traces on all interfaces.

Format clear cpu-traffic traces

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #clear cpu-traffic traces
```

5.16.1.25. clear default interface

This command sets interface configurations to default.

Format clear default interface {<slot/port> | loopback <0-63> | port-channel <1-64> | vlan <1-4093>}

Parameter	Description
<slot/port>	Enter an interface in slot/port format.
loopback	Configuration of Loopback Interface.

port-channel	Enter specific port-channel ID.
vlan	Configuration of VLAN Interface.

Default None

Mode Privileged Exec

5.16.1.26. clear network ipv6 dhcp statistics

This command clears IPv6 DHCP statistics.

Format clear network ipv6 dhcp statistics

Default None

Mode Privileged Exec

5.16.2. copy

This 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. Local URLs can be specified using FTP, TFTP. SFTP and SCP are available as additional transfer methods if the software package supports secure management. If FTP is used, a password is required.

5.16.2.1. copy *source* <url>

This command uploads files from the switch. The parameter *url* can be specified using FTP, TFTP, SCP, or SFTP. If FTP is used, a password is required.

Format copy *source* <url>

Parameter	Definition
url	Uploads file using {tftp://<ipaddress|ipv6address[%scopeid]|hostname>/<filepath>/<filename>| ftp://<user>@<ipaddr|ipv6address[%scopeid]|hostname>/<path>/<filename>| scp://<user>@<ipaddr|ipv6address[%scopeid]|hostname>/<path>/<filename> | sftp://<user>@<ipaddr|ipv6address[%scopeid]|hostname>/<path>/<filename>}.

Mode Privileged EXEC

Source Parameter	Definition
application <sourcefilename>	Uploads *sourcefilename* application file
backup-config	Uploads Backup Config file.
clibanner	Uploads Pre-login Banner file.
core-dump	Uploads the core dump file.
cpu-pkt-capture	Uploads CPU packets capture file
crash-log	Uploads Crashlog file
errorlog	Uploads Errorlog file.

fastpath.cfg	Uploads Binary Config file.
log	Uploads Log file.
operational-log	Uploads Operational Log file.
running-config	Copies system config file.
script <sourcefilename>	Uploads *sourcefilename* Configuration Script file.
startup-config	Uploads Startup Config file.
startup-log	Uploads Startup Log file.
tech-support	Uploads Tech Support file.
traplog	Uploads Trap log file.

5.16.2.2. copy <url> destination

This command downloads files to the switch. The parameter *url* can be specified using FTP, TFTP, SCP, or SFTP. If FTP, SCP, or SFTP are used, a password is required

Format copy <url> *destination*

Parameter	Definition
url	Downloads file using {tftp://<ipaddress|ipv6address[%scopeid]|hostname>/<filepath>/<filename>| ftp://<user>@<ipaddr|ipv6address[%scopeid]|hostname>/<path>/<filename>| scp://<user>@<ipaddr|ipv6address[%scopeid]|hostname>/<path>/<filename> | sftp://<user>@<ipaddr|ipv6address[%scopeid]|hostname>/<path>/<filename>}

Mode Privileged EXEC

Destination Parameter	Definition
application <destfilename>	Downloads the application file as *destfilename* file name.
backup-config	Downloads the Backup Config file.
clibanner	Downloads the Pre-login Banner file.
openflow-ssl-ca-cert	Downloads the OpenFlow CA certificate file.
openflow-ssl-cert	Downloads the OpenFlow switch certificate file.
openflow-ssl-priv-key	Downloads the OpenFlow private key file.
publickey-config	Downloads the Public Key for Config Script validation.
publickey-image	Downloads the Public Key for image.
script <destfilename>	Downloads the Configuration Script file as *destfilename* file name.
sshkey-dsa	Downloads the SSH DSA Key file.
sshkey-rsa2	Downloads the SSH RSA2 Key file.
sshkey-user-public-key {dsa | rsa}	Downloads the SSH user Public Key file for the current user. It supports the DSA or RSA Key file of the OpenSSH key format.
sslpem-root	Downloads the SSL root certificate file for the SSL feature of the RESTFul API. If both the root certificate and the server key exist, two keys are merged as an ssl.pem file.
sslpem-server	Download the SSL server key file for the SSL feature of the RESTFul API. If both the root certificate and the server key exist, the two keys are merged as an ssl.pem file.
startup-config	Downloads the Config file as the startup configuration file.

Example: The following shows an example of downloading and applying as users file.

```
(M4500-32C) #
copy tftp://172.20.0.1/id_dsa.pub sshkey-user-public-key dsa
Mode..................................... TFTP
Set Server IP............................ 172.20.0.1
Path..................................... ./
```

```
Filename..................................... id_dsa.pub
Data Type.................................... SSH User Public DSA key

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...

User Public Key transfer completely and update key successfully.
```

5.16.2.3. copy running-config

This command saves the running configuration to NVRAM.

Format copy running-config {startup-config | url}

Mode Privileged EXEC

5.16.2.4. copy {startup-config backup-config | backup-config startup-config}

This command manages the dual configurations (startup and backup) on the file system. You can copy startup configuration file to backup or copy backup configuration file to startup.

Format copy {startup-config {backup-config | <url>} | backup-config {startup-config | <url>}}

Mode Privileged EXEC

5.16.3. 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 | core-dump-file {<filename> | all}}

Mode Privileged EXEC

5.16.4. erase application

This command erases the application file from the permanent storage.

Format erase application <filename>

Mode Privileged EXEC

5.16.5. erase startup-config

This command erases the startup-config from the permanent storage.

Format erase startup-config

Mode Privileged EXEC

5.16.6. erase user public key

This command erases an assigned SSH user public key from the permanent storage, and it only allows user “admin” or public key owner to execute this command.

Format erase user-public-key <username>

Mode Privileged EXEC

5.16.7. dir

Use this command to list the files in the directory /mnt/fastpath in flash from the CLI.

Format dir

Mode Privileged EXEC

Example: The following shows an example of dir.

```
(M4500-32C) #dir

      2  drwx                     4096 Mar 13 2000 10:24:58 .
     12  drwx                     0 Mar 11 2000 06:26:20 ..
     11  drwx                     16384 Feb 13 2000 11:38:49 lost+found
     12  -rw-                     62284359 Feb 13 2000 11:39:26 image1
     13  -rw-                     62268250 Mar 13 2000 10:24:58 image2
     14  -rw-                     668 Feb 19 2000 05:07:47 ssh_host_dsa_key
     15  -rw-                     891 Feb 19 2000 05:07:39 ssh_host_rsa_key
     16  -rw-                     222 Feb 19 2000 05:07:39 ssh_host_rsa_key.pub
     17  -rw-                     525 Feb 19 2000 05:07:39 ssh_host_key
     18  -rw-                     330 Feb 19 2000 05:07:39 ssh_host_key.pub
     19  -rw-                     598 Feb 19 2000 05:07:47 ssh_host_dsa_key.pub
     20  -rw-                     5 Feb 13 2000 11:41:15 sshkey
  26241  drwx                     4096 Feb 13 2000 11:41:21 ruby
 371681  drwx                     4096 Feb 13 2000 11:41:23 bootstrap
 379761  drwx                     4096 Feb 13 2000 11:41:53 usr
 121201  drwx                     4096 Feb 13 2000 11:42:06 python
```

```
 428241  drwx                     4096 Feb 13 2000 11:42:06 dstat
     21  -rw-                     0 Mar 11 2000 06:26:39 fluent.conf
     22  -rwx                     10 Feb 13 2000 11:42:08 user.start
 436321  drwx                     4096 Feb 13 2000 11:42:08 crashlogs
     23  -rw-                     16328 Mar 11 2000 06:26:40 log2.bin
     36  -rw-                     5 Mar 11 2000 06:26:23 ologNdx0.txt
     25  -rw-                     0 Mar 05 2000 12:48:11 slog2.txt
     33  -rw-                     5 Mar 09 2000 06:05:18 ologNdx1.txt
     27  -rw-                     172 Feb 13 2000 11:42:25 hpc_port_broad.cfg
 395921  drwx                     4096 Mar 11 2000 08:45:59 user-apps
     28  -rw-                     413 Mar 11 2000 06:26:38 coredump_regular_config
     29  -rw-                     72 Mar 11 2000 06:26:38 coredump_regular_config.md5sum
     30  -rw-                     96 Mar 11 2000 06:26:40 snmpOprData.cfg
     31  -rw-                     156 Feb 13 2000 11:42:44 dh512.pem
     32  -rw-                     245 Feb 13 2000 11:42:44 dh1024.pem
     26  -rw-                     0 Mar 05 2000 12:48:11 olog2.txt
     34  -rw-                     0 Mar 09 2000 06:05:18 slog1.txt
     24  -rw-                     5 Mar 05 2000 12:48:11 ologNdx2.txt
     35  -rw-                     0 Mar 09 2000 06:05:18 olog1.txt
     37  -rw-                     0 Mar 11 2000 06:26:23 slog0.txt
     38  -rw-                     0 Mar 11 2000 06:26:23 olog0.txt
     39  -rw-                     64 Mar 11 2000 06:26:23 logNvmSave.bin
     40  -rw-                     2401 Mar 11 2000 06:24:45 fastpath.cfg
     41  -rw-                     678 Mar 11 2000 06:24:47 startup-config

Total Size: 3646722048
Bytes Free: 3354427392
```

5.16.8. show bootvar

This command is used to display which image was booted when the system powered up.

Format show bootvar

Mode Privileged EXEC

Example: The following shows an example of this command.

```
(M4500-32C) #show bootvar

Image Descriptions

 active :
 backup :


 Images currently available on Flash

 ------  ------------  ------------  ---------------------  -----------------
 unit       active        backup        current-active        next-active
 ------  ------------  ------------  ---------------------  -----------------

    1      7.0.0.11     <none>             7.0.0.11             7.0.0.11
```

5.16.9. Ping Commands

Use these commands to determine whether another computer is on the network. A ping provides a synchronous response when initiated from the CLI interface.

5.16.9.1. ping

Use this command to determine whether another computer is on the network. To use this 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.

Format ping [vrf <vrf-name>] {<ip-address> | <ip6addr> | <hostname>} [count <1-15>] [interval <1-60>] [size <0-13000>] [source {< ip-address> | <slot/port> | loopback <loopback-id> | serviceport |vlan <vlan-id>}]

Default The default count is 3.

The default interval is 3 seconds.

The default size is 0 bytes.

Mode 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	Definition
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.
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 13000 bytes.
source	Use the source parameter to specify the source IP/IPv6 address or interface to use when sending the Echo requests packets.

5.16.9.2. 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. You can utilize the ping or traceroute facilities over the service/network ports when using an IPv6 global address *ipv6-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 traceroute 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.

Format ping ipv6 <ipv6-address | hostname> [count <1-15>] [interval <1-60>] [size <0-13000>] [source {< ip-address> | <slot/port> | loopback <loopback-id> | serviceport | tunnel <tunnel-id> | vlan <vlan-id>}]

Default The default count is 3.

The default interval is 3 seconds.

The default size is 0 bytes.

Mode Privileged EXEC

User EXEC

5.16.9.3. ping ipv6 interface

This command use 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.

Format ping ipv6 interface {<slot/port> | loopback <loopback-id> | serviceport | tunnel <tunnel-id> | vlan <vlan-id>} <link-local-address> [count <1-15>] [interval <1-60>] [size <0-13000>] [source {< ip-address> | <slot/port> | loopback <loopback-id> | serviceport | tunnel <tunnel-id> | vlan <vlan-id>}]

Default The default count is 3.

The default interval is 3 seconds.

The default size is 0 bytes.

Mode Privileged EXEC

User EXEC

5.16.10. Traceroute

5.16.10.1. 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.

Format traceroute [vrf <vrf-name>] <ip-address | hostname> [initTtl <initTtl>] [maxTtl <maxTtl>] [maxFail <maxFail>] [interval <interval>] [count <count>] [port <port>] [size <size>] [source {< ip-address> | <slot/port> | loopback <loopback-id> | serviceport | tunnel <tunnel-id> | vlan <vlan-id>}]

Parameter	Definition
vrf-name	The name of the virtual router in 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.
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.
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.
count	Use the **count** parameter to specify the number of probes per hop. The range for count is 1 to 10.
interval	Use the **interval** parameter to specify the time between probes, in seconds. 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.
size	Use the **size** parameter to specify the size of probe packets, in bytes. Range is 0 to 39936 bytes.
source	Use the **source** parameter to specify the source IP/IPv6 address or interface to use for the traceroute.

Default The default initTtl is 1.

The default maxTtl is 30.

The default maxFail is 5.

The default interval is 3 seconds.

The default count is 3.

The default port is 33434.

The default size is 0 bytes.

Mode Privileged EXEC

5.16.10.2. traceroute ipv6

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. The <ipv6-address|hostname> parameter must be a valid IPv6 address|hostname.

Format traceroute ipv6 <ipv6-address | hostname> [initTtl <initTtl>] [maxTtl <maxTtl>] [maxFail <maxFail>] [interval <interval>] [count <count>] [port <port>] [size <size>] [source {< ipv6-address> | <slot/port> | loopback <loopback-id> | serviceport | tunnel <tunnel-id> | vlan <vlan-id>}]

Default The default initTtl is 1.

The default maxTtl is 30.

The default maxFail is 5.

The default interval is 3 seconds.

The default count is 3.

The default port is 33434.

The default size is 0 bytes.

Mode Privileged EXEC

5.16.11. 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] | os]

Parameter	Definition
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.
os	**Caution!** Resets the switch and starts ONIE. Prepare to reinstall the OS.

Default None

Mode Privileged Exec

5.16.12. configure

This command is used to activate global configuration mode.

Format Configure

Default None

Mode Privileged Exec

5.16.13. disconnect

This command is used to close a remote console session.

Format disconnect {<0-30> | all}

Parameter	Definition
<0-30>	Remote session ID.
all	All remote sessions.

Default None

Mode Privileged Exec

5.16.14. hostname

This command is used to set the system hostname. It also changes the prompt string. The length of name is up to 64 alphanumeric, case-sensitive characters.

Format hostname <hostname>

Default M4500-32C or M4500-48XF8C

Mode Global Config

5.16.15. quit

This command is used to exit a CLI session.

Format quit

Default None

Mode Privileged Exec

5.16.16. AutoInstall commands

5.16.16.1. show autoinstall

This command displays the current status of the AutoInstall process.

Format show autoinstall

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
AutoInstall Operation	Displays the autoinstall operation is started or stoped.
AutoInstall Persistent Mode	Displays the autoinstall persistently for next reboot cycle.
AutoSave Mode	Displays the auto-save of downloaded configuration.
AutoReboot Mode	Displays the auto-reboot, which is used to allow the switch to automatically reboot after successfully downloading an image.
AutoUpgrade Mode	Displays the upgrade mode, which is used to allow to download the newer image.
AutoInstall Retry Count	Retry Count The number of times the switch has attempted to contact the TFTP server during the current AutoInstall session.
AutoInstall State	Displays the status of autoinstall.

5.16.16.2. boot-system 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.

Format boot-system autoinstall { start | stop }

Default None

Mode Privileged Exec

5.16.16.3. boot-system host autoinstall

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.

Format boot-system host autoinstall

Default None

Mode Privileged Exec

5.16.16.4. no boot-system host autoinstall

Use this command to disable AutoInstall for the next reboot cycle.

Format no boot-system host autoinstall

Mode Privileged Exec

5.16.16.5. boot-system 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. If the switch reboots and the downloaded configuration has not been saved, the AutoInstall process begins, if the feature is enabled.

Format boot-system host autosave

Default None

Mode Privileged Exec

5.16.16.6. no boot-system host autosave

Use this command to disable automatically saving the downloaded configuration on the switch.

Format no boot-system host autosave

Mode Privileged Exec

5.16.16.7. boot-system 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.

This command only work on the autoupgrade is enabled.

Format boot-system host autoreboot

Default None

Mode Privileged Exec

5.16.16.8. no boot-system 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-system host autoreboot

Mode Privileged Exec

5.16.16.9. boot-system host upgrade

Use this command to allow the switch only to upgrade the newer image version.

Format boot-system host upgrade

Default None

Mode Privileged Exec

5.16.16.10. no boot-system host upgrade

Use this command to disable this function.

Format no boot-system host upgrade

Mode Privileged Exec

5.16.16.11. boot-system host retrycount

Use this command to set the number of attempts to download a configuration file from the TFTP server.

Format boot-system host retrycount <1-3>

Default 3

Mode Privileged Exec

5.16.17. Capture CPU packet commands

5.16.17.1. show capture

Use this command to display packets captured and save to RAM, It is possible to capture and save into RAM, packets that are received or transmitted throuph 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]

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
<packets>	Specifies this parameter to display the captured packets on the CLI.
Operational Status	Displays capture status.
Current Capturing Type	Displays the current capturing type. Possible types are Line, File, and Remote.
Capturing Traffic Mode	Displays the capturing traffic mode. Possible modes are Rx, Tx, or Tx/Rx.

Line Wrap Mode	Displays the line wrap mode for Line capturing type. Default is disabled.
RPCAP Listening Port	Displays the pcap listening port number. Default listening port number is 2002.
RPCAP dump file size (KB)	Disaply the capture packet file size. Default file size is 512KB.

5.16.17.2. capture start

Use this command to manually start capturing CPU packets for packet trace. The packet capture operates in three modes:

- capture file
- remote capture
- capture line

This command is not persistent across a reboot cycle.

Format capture start [{all | received | transmit}]

Parameter	Definition
all	Specifies all to capture packets for both transmitted and received packets.
received	Specifies received to capture only received packets.
transmit	Specifies transmit to capture only transmitted packets.

Default None

Mode Privileged Exec

5.16.17.3. capture stop

Use this command to manually stop capturing CPU packets for packets for trace.

Format capture stop

Default None

Mode Privileged Exec

5.16.17.4. capture {file | remote | line}

Use this command to configure packet capture options. This command is persistent across a reboot cycle.

Format capture {file | remote | line}

Parameter	Definition
file	In the capture file mode, the captured packets are stored in a file. The maximum file size defaults to 512KB. The switch can transfer the file to a TFTP server via TFTP, FTP via CLI. The file is formatted in pcap format, is name cpu-pkt-capture.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 captureing. 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 CLI command ***capture stop***.
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 disable 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 sotre any captured data locally on its file system.
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 btes that can be captured and displayed in Line mode.

Default Remote

Mode Global Config

5.16.17.5. capture remote port

Use this command to configure file capture options. This command is persistent across a reboot cycle.

Format capture remote [port <port-id>]

Parameter	Definition
<port-id>	Configure the listening TCP port. The range of port ID is 1024 to 49151.

Default 2002

Mode Global Config

5.16.17.6. capture file size

Use this command to configure file capture options. This command is persistent across a reboot cycle.

Format capture file [size <file-size>]

Parameter	Definition
<file-size>	Configure the file size in KB. The range of file size is 2 to 512KB.

Default 512

Mode Global Config

5.16.17.7. capture line wrap

This command enables wrapping of captured packets in line mode when the captured packets reaches full capacity. This command is persistent across a reboot cycle.

Format capture line [wrap]

Default Disable

Mode Global Config

5.16.17.8. 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

5.16.18. set clibanner

This command is used to set the pre-login CLI banner before displaying the login prompt.

Format set clibanner <line>

Default None

Mode Global Config

Parameter	Description

line	Banner text where “” (double quote) is a delimiting character. The banner message can be up to 2000 characters.

5.16.19. no set clibanner

This command unconfigures the pre-login CLI banner.

Format no set clibanner

Mode Global Config

5.16.20. 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.

Format show clibanner

Default No contents to display before displaying the login prompt.

Mode Privileged Exec

5.16.21. Link-Flap commands

5.16.21.1. show link-flap

Use this command to check the admin status and configured parameters of link-flap.

Format show link-flap

Mode Privileged Exec

Display Message

Parameter	Definition
Admin status	Displays the admin state of link-flap.
Maximum flap count	Displays maximal allowed number of link-flap in the detection duration
Detection duration	Displays the time (in seconds) of duration for detecting link-flap

5.16.21.2. link-flap

Use this command to enable Link-Flap functionality and configure the maximum allowed link-flap times and the detection duration.

Use no form of this command to reset to default.

Format [no] link-flap [<3-10> [<5-30>]]

Parameter	Definition
<3-10>	Configure the maximum allowed link-flap times before the interface is put into err-disabled state. (Default is 3)
<5-30>	Configure the error detection duration in seconds. (Default is 10)

Default Disabled

Mode Global Config

5.16.22. Loop Detection commands

5.16.22.1. show loop-detection

Use this command to display the admin status and configured parameters of loop detection.

Format show loop-detection

Mode Privileged Exec

Display Message

Parameter	Definition
Admin status	Displays the admin state of loop detection
Transmit interval	Displays the interval between transmission of PDUs (in second)
Max PDU Receive	Displays the maximal number of PDU to be received by switch before an action is taken on the interface

5.16.22.2. show loop-detection statistics

Use this command to display the statistics of loop detection for all ports or specific interfaces.

Format show loop-detection statistics {<intf-range> | all}

Mode Privileged Exec

Parameter	Definition
intf-range	The interfaces for which to show statistics.
all	Show statistics for all interfaces

Display Message

Parameter	Definition
Port	The slot and port associated with the interface.
Admin Status	Shows whether the specified port is enabled or disabled.
Loop Detected	The loop presence on the specified port.
Loop Count	The loop count for the the specified port.
Time Since Last Loop	The time since the last loop occured for the specified port.
Rx Action	The action mode for the the specified port.
Port Status	The admin state of the specified interface.

5.16.22.3. loop-detection (Global Config)

Use this command to enable loop-detection functionality and configure the transmission interval and the maximal packets to be received before an action is taken.

Use no form of this command to reset to default.

Format [no] loop-detection [<1-10> [1-10]]

Parameter	Definition
<1-10>	Configure the interval between transmission of PDUs in second (Default is 5)
<1-10>	Configure the maximal number of PDU to be received by switch before an action is taken on the interface (Default is 1)

Default Disabled

Mode Global Config

5.16.22.4. loop-detection (Interface Config)

Use this command to enable loop-detection on the interface.

Use no form of this command to reset to default.

Format [no] loop-detection

Default Disabled

Mode Interface Config

5.16.22.5. loop-detection action

Use this command to configure the action to be taken on an interface when a loop is detected.

Use no form of this command to reset to default.

Format [no] loop-detection action {both | disable | log}

Parameter	Definition
both	Logs and disables the port
disable	Shuts down the port. This is the default
log	Only logs the message. The log mode only logs the message to buffer logs without bringing the port down

Default both

Mode Interface Config

5.16.23. 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.

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 on x86 platforms only. The following features support ISSU:

L2 FDB, RSTP, MSTP, 802.1Q, 802.3AD, ARP, Routing Interfaces, NDP Cache, BGP with GR, and VRF

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 whithout the knowledge of previous active instance of the same and can cause traffic disruption during initialization.

5.16.23.1. show issu status

Use this command to display the current ISSU status summary.

Format show issu status

Mode Privileged Exec

Example:

```
(Switch) #show issu status

Last reset reason.............................. Normal

Current state.................................. In Service Software Upgrade not
started

Time elapsed since ISSU initiation.............. 0 minutes 0 seconds

(Switch) #
```

5.16.23.2. show issu status details

Use this command to display the ISSU event logs in chronological order.

Format show issu status detail

Mode Privileged Exec

Example:

```
(Switch) #show issu status detail

Timestamp            State                                          Time elapsed
-------------------- ---------------------------------------------- ------------
May 22 06:44:13 2019 ISSU initiated, storing application data       0m 0s
May 22 06:44:20 2019 Application data stored                        0m 7s

 (Switch) #
```

5.16.24. file verify

This command enables digital signature verification while a configuration script file is downloaded to the switch.

Format file verify {script | none}

no file verify

Default None

Mode Global Config

Fields	Definition
script	Verify the digital signature of configuration script files.
none	Disable digital signature verification for configuration script files.

5.17. DHCP Snooping Commands

DHCP snooping is a security feature that monitors DHCP messages between a DHCP client and DHCP servers to filter harmful DHCP messages and to build a bindings database of {MAC address, IP address, VLAN ID, port} tuples that are considered authorized. You can enable DHCP snooping globally and on specific VLANs, and configure ports within the VLAN to be trusted or untrusted. DHCP servers must be reached through trusted ports.

The DHCP snooping binding table contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information that corresponds to the local untrusted interfaces of a switch; it does not contain information regarding hosts interconnected with a trusted interface. An untrusted interface is an interface that is configured to receive messages from outside the network or firewall. A trusted interface is an interface that is configured to receive only messages from within the network.

DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. It also gives you a way to differentiate between untrusted interfaces connected to the end-user and trusted interfaces connected to the DHCP server or another switch.

DHCP snooping enforces the following security rules:

DHCP packets from a DHCP server (DHCPOFFER, DHCPACK, DHCPNAK, DHCPRELEASEQUERY) are dropped if received on an untrusted port.

DHCPRELEASE and DHCPDECLINE messages are dropped if for a MAC address in the snooping database, but the binding's interface is other than the interface where the message was received.

On untrusted interfaces, the switch drops DHCP packets whose source MAC address does not match the client hardware address. This feature is a configurable option.

The hardware identifies all incoming DHCP packets on ports where DHCP snooping is enabled. DHCP snooping is enabled on a port if (a) DHCP snooping is enabled globally, and (b) the port is a member of a VLAN where DHCP snooping is enabled. On untrusted ports, the hardware traps all incoming DHCP packets to the CPU. On trusted ports, the hardware forwards client messages and copies server messages to the CPU so that DHCP snooping can learn the binding.

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.

5.17.1. show ip dhcp snooping

This command displays the DHCP snooping global configurations and summaries of port configurations.

Format show ip dhcp snooping

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show ip dhcp snooping

DHCP snooping is Enabled
DHCP snooping source MAC verification is enabled
DHCP snooping is enabled on the following VLANs:
1

 Interface    Trusted     Log Invalid Pkts
-----------  ----------   ----------------
0/1          Yes          No
0/2          No           No
0/3          No           No
0/4          No           No
0/5          No           No
0/6          No           No
0/7          No           No
0/8          No           No
0/9          No           No
0/10         No           No
0/11         No           No
0/12         No           No
0/13         No           No
0/14         No           No
0/15         No           No

(M4500-32C) #
```

5.17.2. show ip dhcp snooping per interface

This command displays the DHCP snooping detail configurations for all interfaces or for a specific interface.

Format show ip dhcp snooping interfaces [<slot/port> | port-channel <portchannel-id>]

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show ip dhcp snooping interfaces

Interface     Trust State     Rate Limit      Burst Interval
                                 (pps)          (seconds)
----------   -------------   -------------   ---------------
0/1          Yes             None            N/A
0/2          No              None            N/A
0/3          No              None            N/A
0/4          No              None            N/A
0/5          No              None            N/A
0/6          No              None            N/A
0/7          No              None            N/A
0/8          No              None            N/A
0/9          No              None            N/A
0/10         No              None            N/A
```

```
0/11          No              None            N/A
0/12          No              None            N/A
0/13          No              None            N/A
0/14          No              None            N/A
0/15          No              None            N/A
0/16          No              None            N/A
0/17          No              None            N/A
0/18          No              None            N/A
0/19          No              None            N/A

(M4500-32C) #
```

5.17.3. show ip dhcp snooping binding

This command displays the DHCP Snooping binding entries.

The parameter “static” means to restrict the output based on static entries which are added by user manually.

The parameter “dynamic” means to restrict the output based on dynamic entries which are added by DHCP Snooping automatically.

Format show ip dhcp snooping binding [{static | dynamic}] [interface {<slot/port> | port-channel <portchannel-id>}] [vlan <vlan-id>]

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show ip dhcp snooping binding

Total number of bindings:  363
Total number of Tentative bindings:  61


   MAC Address       IP Address     VLAN   Interface    Type    Lease (Secs)
-----------------  ---------------  ----  -----------  -------  -----------
44:0A:A7:8A:00:00        10.10.1.6     1         0/10  DYNAMIC        86383
44:0A:A7:8A:00:01        10.10.1.8     1         0/10  DYNAMIC        86383
44:0A:A7:8A:00:02       10.10.1.10     1         0/10  DYNAMIC        86383
44:0A:A7:8A:00:03       10.10.1.11     1         0/10  DYNAMIC        86383
44:0A:A7:8A:00:04       10.10.1.12     1         0/10  DYNAMIC        86383
44:0A:A7:8A:00:05       10.10.1.13     1         0/10  DYNAMIC        86383
44:0A:A7:8A:01:00        10.10.1.2     1         0/10  DYNAMIC        86383
44:0A:A7:8A:01:01        10.10.1.3     1         0/10  DYNAMIC        86383
44:0A:A7:8A:01:02        10.10.1.4     1         0/10  DYNAMIC        86383
44:0A:A7:8A:01:03        10.10.1.5     1         0/10  DYNAMIC        86383
44:0A:A7:8A:01:04        10.10.1.7     1         0/10  DYNAMIC        86383
44:0A:A7:8A:01:05        10.10.1.9     1         0/10  DYNAMIC        86383
44:0A:A7:8A:02:00       10.10.1.20     1         0/10  DYNAMIC        86383
44:0A:A7:8A:02:01       10.10.1.21     1         0/10  DYNAMIC        86383
44:0A:A7:8A:02:02       10.10.1.22     1         0/10  DYNAMIC        86383
44:0A:A7:8A:02:03       10.10.1.23     1         0/10  DYNAMIC        86383
```

```
(M4500-32C) #
```

5.17.4. show ip dhcp snooping database

This command displays the DHCP Snooping configuration related to the database persistency.

Format show ip dhcp snooping database

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show ip dhcp snooping database

agent url:  local

write-delay:  300

(M4500-32C) #
```

5.17.5. show ip dhcp snooping information all

This command displays the summaries of DHCP Option-82 configurations.

Format show ip dhcp snooping information all

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show ip dhcp snooping information all

DHCP Information Option82 is  Enabled.

Interface   OPT82 Mode   TrustMode
---------  ------------  --------------
0/1        Enabled       trusted
0/2        Disabled      untrusted
0/3        Disabled      untrusted
0/4        Disabled      untrusted
0/5        Disabled      untrusted
0/6        Disabled      untrusted
0/7        Disabled      untrusted
0/8        Disabled      untrusted
0/9        Disabled      untrusted
0/10       Disabled      untrusted
0/11       Disabled      untrusted
```

```
0/12       Disabled      untrusted
0/13       Disabled      untrusted
0/14       Disabled      untrusted
0/15       Disabled      untrusted
0/16       Disabled      untrusted
0/17       Disabled      untrusted
0/18       Disabled      untrusted

(M4500-32C) #
```

5.17.6. show ip dhcp snooping information statistics

This command displays DHCP Option-82 statistics per interface.

Format show ip dhcp snooping information stats interface {<slot/port> | all}

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show ip dhcp snooping information stats interface all

Interface    UntrustedServer  UntrustedClient  TrustedServer     TrustedClient
             MsgsWithOpt82    MsgsWithOpt82    MsgsWithoutOpt82  MsgsWithoutOpt82
-----------  ---------------  ---------------  ----------------  ----------------
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                0                0                 0
0/8          0                0                0                 0
0/9          0                0                0                 0
0/10         0                0                0                 0
0/11         0                0                0                 0
0/12         0                0                0                 0
0/13         0                0                0                 0
0/14         0                0                0                 0
0/15         0                0                0                 0
0/16         0                0                0                 0
0/17         0                0                0                 0
0/18         0                0                0                 0
0/19         0                0                0                 0

(M4500-32C) #
```

5.17.7. show ip dhcp snooping information agent-option

This command displays the Option-82 configurations of DHCP Relay agent on specific VLAN.

Format show ip dhcp snooping information agent-option vlan <vlan-list>

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) # show ip dhcp snooping information agent-option vlan 1

DHCP Information Option82 is  Enabled.

VLAN Id    DHCP OPT82   CircuitId    RemoteId
---------  ---------    ----------   --------------------------------
1          Enabled      Enabled      testRemoteIdString

(M4500-32C) #
```

5.17.8. show ip dhcp snooping information per vlan

This command displays the DHCP Option-82 configurations per specific VLAN.

Format show ip dhcp snooping information vlan <vlan-list>

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show ip dhcp snooping information vlan 1

DHCP Information Option82 is  Enabled.

DHCP L2 Relay is enabled on the following VLANs:
1

(M4500-32C) #
```

5.17.9. show ip dhcp snooping information circuit-id

This command displays the circuit-id configuration of DHCP Option-82 per specific VLAN.

Format show ip dhcp snooping information circuit-id vlan <vlan-list>

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) # show ip dhcp snooping information circuit-id vlan 1

DHCP Information Option82 is Enabled.

DHCP Circuit-Id option is enabled on the following VLANs:
1

(M4500-32C) #
```

5.17.10. show ip dhcp snooping information remote-id

This command displays the remote-id configuration of DHCP Option-82 per specific VLAN.

Format show ip dhcp snooping information remote-id vlan <vlan-list>

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) # show ip dhcp snooping information remote-id vlan 1

DHCP Information Option82 is Enabled.

VLAN ID    Remote Id
---------  --------------------------------
1          testRemoteIdString

(M4500-32C) #
```

5.17.11. show ip dhcp snooping information interface

This command displays the remote-id configuration of DHCP Option-82 per interface.

Format show ip dhcp snooping information interface {<slot/port> | all}

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show ip dhcp snooping information interface 0/1
```

```
DHCP Information Option82 is  Enabled.

Interface  OPT82 Mode    TrustMode
---------  ------------  --------------
0/1        Enabled       trusted

(M4500-32C) #
```

5.17.12. ip dhcp snooping

This command enables or disables the DHCP Snooping globally.

Format [no] ip dhcp snooping

Default Disable

Mode Global Config

5.17.13. ip dhcp snooping vlan

This command enables or disables the DHCP Snooping to the specific VLAN.

Format [no] ip dhcp snooping vlan <vlan-list>

Default Disable

Mode Global Config

5.17.14. ip dhcp snooping verify mac-address

This command enables or disables the verification of the source MAC address with the client hardware address in the received DHCP message.

Format [no] ip dhcp snooping verify mac-address

Default Enable

Mode Global Config

5.17.15. ip dhcp snooping database

This command configures the persistent location of the DHCP Snooping database. This can be local or a remote file on a given IP machine.

The parameter “local” means to set database access inside device.

The parameter “tftp://hostIP/filename” means to set database access on remote TFTP Server.

Format ip dhcp snooping database {local | <url>}

Default Local

Mode Global Config

5.17.16. ip dhcp snooping database write-delay

This command configures the interval in seconds at which the DHCP Snooping database will be persisted, and this database stores the results of DHCP snooping bindings. Use keyword “no” to restore the default value of this command.

The parameter “<interval>” value ranges is from 15 to 86400 seconds.

Format ip dhcp snooping database write-delay <interval>

no ip dhcp snooping database write-delay

Default 300

Mode Global Config

5.17.17. ip dhcp snooping binding

This command configures the static DHCP Snooping binding which binds a MAC address to assigned IP address on a specific VLAN ID and interface. Use keyword “no” to remove an existing entry of DHCP Snooping binding.

Format ip dhcp snooping binding <mac-address> vlan <vlan id> <ip address> interface {<slot/port> | port-channel < portchannel-id>}

no ip dhcp snooping binding <mac-address>

Default None

Mode Global Config

Example: To add a static entry of DHCP snooping binding which binds MAC address 00:11:22:33:44:55 to IP address 10.0.0.1 on vlan 1 and port interface 0/1.

```
(M4500-32C) #configure
(M4500-32C) (Config)#ip dhcp snooping binding 00:11:22:33:44:55 vlan 1 10.0.0.1 interface 0/1
(M4500-32C) (Config)#
```

5.17.18. ip dhcp snooping information option

This command enables or disables the DHCP Snooping application to support information Option 82 in global configuration or a specific interface.

Format [no] ip dhcp snooping information option

Default Disable

Mode Global Config
Interface Config

5.17.19. ip dhcp snooping information option circuit-id

This command enables or disables the DHCP Snooping Option 82 with sub-option circuit-id in a range of VLANs.

The format of circuit-id is LLLLVVVVXXYYZZ, and LLLL is the length from V to Z, VVVV is VLAN ID, XX is the Unit ID, YY is the function/module ID and ZZ is the Port number.

Format [no] ip dhcp snooping information option circuit-id vlan <vlan-list>

Default Disable

Mode Global Config

5.17.20. ip dhcp snooping information option remote-id

This command enables or disables the DHCP Snooping Option 82 with sub-option remote-id in a range of VLANs. When it's enabled, all DHCP client's requests received to this device will be added remote-id sud-option with remote-id string.

The format of remote-id is LLLLXXXXX, and LLLL is the total length of all X, XXXXX is remote-id string which is set by user.

The parameter "<remoteId string>" defines remote-id string which of maximum length is 32 characters

Format ip dhcp snooping information option remote-id <remoteId string> vlan <vlan-list>
no ip dhcp snooping information option remote-id vlan <vlan-list>

Default Disable

Mode Global Config

5.17.21. ip dhcp snooping information option vlan

This command enables or disables the DHCP Snooping option 82 in a range of VLANs.

Format [no] ip dhcp snooping information option vlan <vlan-list>

Default Disable

Mode Global Config

5.17.22. ip dhcp snooping information option trust

This command configures an interface to be trusted for Option-82 reception.

Format [no] ip dhcp snooping information option trust

Default Disable

Mode Interface Config

5.17.23. ip dhcp snooping limit

This command controls the rate at which the DHCP Snooping messages come. If packet rate exceeds limitation over burst interval, the assigned port will shut down automatically. User could use interface command “shutdown” and then “no shutdown” to recover it. Use keyword “no” to restore the default value of this command.

The parameter “rate” means to the limitation of packet rate. Its range is from 0 to 300 packets per second.

The parameter “burst interval” means the time interval of packet burst could be over rate limitation. Its range is from 1 to 15 seconds.

Format ip dhcp snooping limit {rate <pps> [burst interval <seconds>] | none}

no ip dhcp snooping limit

Default “rate” is None

“burst interval” is 1 second.

Mode Interface Config

Example: While the packet rate of DHCP message received from port 0/1 exceeds 100 pps and consecutive time interval is over 10 seconds, the port 0/1 will be shutdown automatically.

```
(M4500-32C) #configure
(M4500-32C) (Config)#interface 0/1
```

```
(M4500-32C) (Interface 0/1)# ip dhcp snooping limit rate 100 burst interval 10
(M4500-32C) (Interface 0/1)#
```

5.17.24. ip dhcp snooping log-invalid

This command controls logging the illegal DHCP messages to logging buffer.

Format [no] ip dhcp snooping log-invalid

Default Disabled

Mode Interface Config

5.17.25. ip dhcp snooping trust

This command enables or disables a port as DHCP Snooping trust port.

Format [no] ip dhcp snooping trust

Default Disabled

Mode Interface Config

5.17.26. ip dhcp snooping trust

This command enables or disables a port as DHCP Snooping trust port.

Format [no] ip dhcp snooping trust

Default Disabled

Mode Interface Config

5.17.27. clear ip dhcp snooping binding

This command is used to clear all DHCP Snooping bindings on all interfaces or on a specific interface.

Format clear ip dhcp snooping binding [interface <slot/port>]

Default None

Mode Privileged EXEC

5.17.28. clear ip dhcp snooping statistics

This command is used to clear all DHCP Snooping statistics.

Format clear ip dhcp snooping statistics

Default None

Mode Privileged EXEC

5.17.29. clear ip dhcp snooping information statistics

This command is used to clear statistics of DHCP Snooping Option 82.

Format clear ip dhcp snooping information statistics interface {<slot/port> | all}

Default None

Mode Privileged EXEC

5.18. IP Source Guard (ISG) Commands

IP Source Guard (IPSG) is a security feature that filters IP packets based on source ID. The source ID may be either the source IP address or a {source IP address, source MAC address} pair. The DHCP snooping binding database and static IPSG entries identify authorized source IDs. You can configure:

- Whether enforcement includes the source MAC address.
- Static authorized source IDs.

Similar to DHCP snooping, this feature is enabled on a DHCP snooping untrusted Layer 2 port. Initially, all IP traffic on the port is blocked except for DHCP packets that are captured by the DHCP snooping process. When a client receives a valid IP address from the DHCP server, or when a static IP source binding is configured by the user, a per-port and VLAN Access Control List is installed on the port. This process restricts the client IP traffic to those source IP addresses configured in the binding; any IP traffic with a source IP address other than that in the IP source binding is filtered out. This filtering limits a host's ability to attack the network by claiming a neighbor host's IP address.

IPSG can be enabled on physical or LAG ports. IPSG is disabled by default. If you enable IPSG on a port where DHCP snooping is disabled or where DHCP snooping is enabled but the port is trusted, all IP traffic received on that port is dropped depending on the admin-configured IPSG entries. IPSG cannot be enabled on a port-based routing interface.

5.18.1. Show commands

5.18.1.1. show ip verify

This command displays the IPSG interface configurations on all ports.

Format show ip verify [interface <slot/port> | port-channel <portchannel-id>]

Term	Definition
<slot/port>	Specifies the interface number.
<portchannel-id>	Specifies the port-channel interfaces. The range of the port-channel ID is 1 to 64.

Default None

Mode Privileged Exec

Display Message

Term	Definition
Interface	Interface address in slot/port or port-channel 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.

5.18.1.2. show ip verify source

This command displays the IPSG interface and binding configurations on all ports.

Format show ip verify source [interface <slot/port> | port-channel <portchannel-id>]

Term	Definition
<slot/port>	Specifies the interface number.
<portchannel-id>	Specifies the port-channel interfaces. The range of the port-channel ID is 1 to 64.

Default None

Mode Privileged Exec

Display Message

Term	Definition
Interface	Interface address in slot/port or port-channel 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.

5.18.1.3. show ip source binding

This command displays the IPSG bindings.

Format show ip source binding [{static | dhcp-snooping}] [interface <slot/port>] [vlan <vlan-id>]

Term	Definition
static	Statically configured from CLI.
dhcp-snooping	Dynamically learned from DHCP Snooping.
<slot/port>	Specifies the interface number.
<vlan-id>	VLAN ID. The range of VLAN ID is 1 to 4093.

Default None

Mode Privileged Exec

Display Message

Term	Definition
Interface	IP address of the interface in the slot/port or port-channel format.
Type	Entry type; statically configured from CLI or dynamically learned from DHCP Snooping.
IP Address	The IP address of the entry that is added.
MAC Address	The MAC address for the entry that is added.
VLAN	VLAN for the entry.

5.18.2. Configuration commands

5.18.2.1. ip verify source

This command configures 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.

To disable the IPSG configuration in the hardware, use the no form of this command.

Format ip verify source [port-security]

no ip verify source

Term	Definition
<port-security>	Filter data traffic based on the IP and MAC addresses.

Default Disabled

Mode Interface Config

5.18.2.2. ip verify binding

This command configures static IP source guard (IPSG) entries.

To remove the IPSG static entry from the IPSG database, use the no form of this command.

Format ip verify binding <mac-address> vlan <vlan-id> <ip address> interface {<slot/port> | port-channel <portchannel-id> }

no ip verify binding <mac-address> vlan <vlan-id> <ip address> interface {<slot/port> | port-channel <portchannel-id> }

Term	Definition
<mac-address>	Specifies an MAC address.
<vlan-id>	VLAN ID. The range of VLAN ID is 1 to 4093.
<ip address>	Specifies an IP address.
<slot/port>	Specifies the interface number.
<portchannel-id>	Specifies the port-channel interfaces. The range of the port-channel ID is 1 to 64.

Default None

Mode Global Config

5.19. Dynamic ARP Instpection (DAI) Command

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.

To prevent ARP poisoning attacks, a switch must ensure that only valid ARP requests and responses are relayed. DAI prevents these attacks by intercepting all ARP requests and responses. Each of these intercepted packets is verified for valid MAC address to IP address bindings before the local ARP cache is updated or the packet is forwarded to the appropriate destination. Invalid ARP packets are dropped.

DAI determines the validity of an ARP packet based on valid MAC address to IP address bindings stored in a trusted database. This database is built at runtime by DHCP snooping, provided this feature is enabled on VLANs and on the switch. 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. In addition, in order to handle hosts that use statically configured IP addresses, DAI can also validate ARP packets against user-configured ARP ACLs.

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.

5.19.1. Show commands

5.19.1.1. show ip arp instpection statistics

This command displays 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>]

Term	Definition
<vlan-list>	Specifies VLAN ID in a list. The range of VLAN ID is 1 to 4093.

Default None

Mode Privileged Exec

Display Message

Term	Definition
VLAN	The VLAN ID for each displayed row.
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.
Bad Src MAC	The number of packets dropped due to Source MAC validation failure.

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.
Packet Queue Exceed	The number of packets dropped due to the DAI processing queue being full.

5.19.1.2. show ip arp inspection

This command displays 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 [vlan <vlan-list>]

Term	Definition
<vlan-list>	Specifies VLAN ID in a list. The range of VLAN ID is 1 to 4093.

Default None

Mode Privileged Exec

Display Message

Term	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.

5.19.1.3. show ip arp inspection interfaces

This command displays 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 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> | loopback <loopback-id> | port-channel <portchannel-id> | tunnel <tunnel-id> | vlan <vlan-list>]

Term	Definition
<slot/port>	Interface Number.
<loopback-id>	Specifies the loopback interfaces. The range of the loopback ID is 0 to 63.
<portchannel-id>	The range of the port-channel ID is 1 to 64.
<tunnel-id>	Specifies the tunnel interfaces. The range of the tunnel ID is 0 to 7.
<vlan-id>	VLAN ID. The range of VLAN ID is 1 to 4093.

Default None

Mode Privileged Exec

Display Message

Term	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

5.19.1.4. show arp access-list

This command displays 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]

Term	Definition
<acl-name>	Specifies the ARP ACL name.

Default None

Mode Privileged Exec

5.19.2. Configuration commands

5.19.2.1. ip arp inspection validate

This command enables additional validation checks like source-mac validation, destination-mac validation, and ip address validation on the received ARP packets.

To disable the additional validation checks on the received ARP packets, use the no form of this command.

Format ip arp inspection validate {[src-mac] [dst-mac] [ip]}

no ip arp inspection validate {[src-mac] [dst-mac] [ip]}

Default Disable

Mode Global Config

5.19.2.2. ip arp inspection vlan

This command enables Dynamic ARP Inspection on a list of comma-separated VLAN ranges.

To disable Dynamic ARP Inspection on a list of comma-separated VLAN ranges, use the no form of this command.

Format ip arp inspection vlan <vlan-list>

no ip arp inspection vlan <vlan-list>

Term	Definition
<vlan-list>	Specifies VLAN ID in a list. The range of VLAN ID is 1 to 4093.

Default Disable

Mode Global Config

5.19.2.3. ip arp inspection vlan logging

This command enables logging of invalid ARP packets on a list of comma-separated VLAN ranges.

To disable logging of invalid ARP packets on a list of comma-separated VLAN ranges, use the no form of this command.

Format ip arp inspection vlan <vlan-list> logging

no ip arp inspection vlan <vlan-list> logging

Term	Definition
<vlan-list>	Specifies VLAN ID in a list. The range of VLAN ID is 1 to 4093.

Default Enable

Mode Global Config

5.19.2.4. ip arp inspection filter

This command configures 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.

To unconfigure the ARP ACL used to filter invalid ARP packets on a list of comma-separated VLAN ranges, use the no form of this command.

Format ip arp inspection filter <acl-name> vlan <vlan-list> [static]

no ip arp inspection filter <acl-name> vlan <vlan-list> [static]

Term	Definition
<acl-name>	Specifies the ARP access-list name up to 31 characters in length.
<vlan-list>	Specifies VLAN ID in a list. The range of VLAN ID is 1 to 4093.
<static>	Specifies ARP ACL is configured static.

Default No ARP ACL is configured on a VLAN

Mode Global Config

5.19.2.5. ip arp inspection trust

This command configures an interface as trusted for Dynamic ARP Inspection.

To configure an interface as untrusted for Dynamic ARP Inspection, use the no form of this command.

Format ip arp inspection trust

no ip arp inspection trust

Default Disable

Mode Interface Config

5.19.2.6. ip arp inspection limit

This command configures the rate limit and burst interval values for an interface. Configuring none for the limit means the interface is not rate limited for Dynamic ARP Inspections.

To set the rate limit and burst interval values for an interface to the default values, use the no form of this command.

Format ip arp inspection limit {rate <pps> [burst interval <seconds>] | none}

no ip arp inspection limit

Term	Definition
<pps>	Specifies rate limit in pps. The range of rate is 0 to 300.
<seconds>	Specifies burst interval in seconds. The range of rate is 1 to 15.

Default 15 pps for rate and 1 second for burst-interval

Mode Interface Config

5.19.2.7. arp access-list

This command creates an ARP ACL.

To delete a configured ARP ACL, use the no form of this command.

Format arp access-list <acl-name>

no arp access-list <acl-name>

Term	Definition
<acl-name>	Specifies the ARP access-list name up to 31 characters in length.

Default None

Mode Global Config

5.19.2.8. permit ip host mac host

This command configures a rule for a valid IP address and MAC address combination used in ARP packet validation.

To delete a rule for a valid IP and MAC combination, use the no form of this command.

Format permit ip host <sender-ip> mac host <sender-mac>

no permit ip host <sender-ip> mac host <sender-mac>

Term	Definition
<sender-ip>	Specifies IP address in the ARP ACL rule.
<sender-mac>	Specifies MAC address in the ARP ACL rule.

Default None

Mode ARP Access-list Config

5.19.2.9. clear ip arp inspection statistics

This command resets the statistics for Dynamic ARP Inspection on all VLANs.

Format clear ip arp inspection statistics

Default None

Mode Privileged Exec

5.20. Differenciated Service Commands

This Switching Command function can only be used on the QoS software version.

This chapter contains the CLI commands used for the QoS Differentiated Services (DiffServ) package.

The user configures DiffServ in several stages by specifying:

1. Class
   - creating and deleting classes
   - defining match criteria for a class

The only way to remove an individual match criterion from an existing class definition is to delete the class and re-create it.

2. Policy
   - creating and deleting policies
   - associating classes with a policy
   - defining policy statements for a policy/class combination
3. Service
   - adding and removing a policy to/from a directional (that is, inbound, outbound) interface

Packets are filtered and processed based on defined criteria. The filtering criteria are defined by a class. The processing is defined by a policy's attributes. Policy attributes may be defined on a per class instance basis, and it is these attributes that are applied when a match occurs.

Packet processing begins by testing the match criteria for a packet. A policy is applied to a packet when a class match within that policy is found.

Note that the type of class - all, any, or acl - has a bearing on the validity of match criteria specified when defining the class. A class type of 'any' processes its match rules in an ordered sequence; additional rules specified for such a class simply extend this list. A class type of ‘acl’ obtains its rule list by interpreting each ACL rule definition at the time the Diffserv class is created. Differences arise when specifying match criteria for a class type 'all', since only one value for each non-excluded match field is allowed within a class definition. If a field is already specified for a class, all subsequent attempts to specify the same field fail, including the cases where a field can be specified multiple ways through alternative formats. The exception to this is when the 'exclude' option is specified, in which case this restriction does not apply to the excluded fields.

The following class restrictions are imposed by the LB8 Series L3 Switch DiffServ design:

- nested class support limited to:
  - 'all' within 'all'
  - no nested 'not' conditions
  - no nested 'acl' class types
  - each class contains at most one referenced class

- hierarchical service policies not supported in a class definition
- access list matched by reference only, and must be sole criterion in a class
  - that is, ACL rules copied as class match criteria at time of class creation, with class type 'any'
  - implicit ACL 'deny all' rule also copied
  - no nesting of class type 'acl'

Regarding nested classes, referred to here as class references, a given class definition can contain at most one reference to another class, which can be combined 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 change is rejected. A class reference may be removed from a class definition.

The user can display summary and detailed information for classes, policies, and services. All configuration information is accessible via the CLI, and SNMP user interfaces.

5.20.1. General commands

The following characteristics are configurable for the platform as a whole.

5.20.1.1. 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 diffsev

Default None

Mode Global Config

5.20.1.2. 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 diffsev

Default None

Mode Global Config

5.20.2. Class commands

The 'class' command set is used in DiffServ to define:

Traffic Classification specifies Behavior Aggregate (BA) based on DSCP, and Multi- Field (MF) classes of traffic (name, match criteria)

Service Levels specifies the BA forwarding classes / service levels. Conceptually, DiffServ is a two-level hierarchy of classes: 1. Service/PHB, 2. Traffic Class

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 belonging to the class. Note that once a class match criterion is created for a class, it cannot be changed or deleted - the entire class must be deleted and re-created.

The CLI command root is ***class-map***.

5.20.2.1. class-map

This command defines a new DiffServ class of type match-all, match-any or match-access-group.

Format class-map [match-all] <class-map-name> [{ipv4 | ipv6}]

Parameter	Description
<class-map-name>	Case sensitive alphanumeric string from 1 to 31 characters uniquely identifying the class.

When used without any match condition, this command enters the class-map mode. The **<class-map-name>** is the name of an existing DiffServ class.

The class name 'default' is reserved and is not allowed here. The class type of **match-all** indicates all of the individual match conditions must be true for a packet to be considered a member of the class.

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.

The CLI mode is changed to Class-Map Config or Ipv6-Class-Map Config when this command is successfully executed depending on the [{ipv4 | ipv6}] keyword specified.

Default None

Mode Global Config

5.20.2.2. no class-map

This command eliminates an existing DiffServ class.

Format no class-map <class-map-name>

Parameter	Description
<class-map-name>	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, this deletion attempt shall fail.

Default None

Mode Global Config

5.20.2.3. rename

This command changes the name of a DiffServ class.

Format rename <new-class-map-name>

Parameter	Description
<new-class-map-name>	Case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the class.

The class name ‘default’ is reserved and must not be used here.

Default None

Mode Class-Map Config / Ipv6-Class-Map Config

5.20.2.4. match any

This command adds to the specified class definition a match condition whereby all packets are considered to belong to the class.

Format match any

Default None

Mode Class-Map Config / Ipv6-Class-Map Config

5.20.2.5. match class-map

This command adds to the specified class definition the set of match conditions defined for another class.

Format match class-map <refclassname>

Parameter	Description
<refclassname>	The name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

i There is no [**not**] option for this match command.

Default None

Mode Class-Map Config / Ipv6-Class-Map Config

Restrictions

The class types of both <***classname>*** and <***refclassname>*** must be identical (that is, any vs. any, or all vs. all). A class type of acl is not supported by this command.

Cannot specify ***<refclassname>*** the same as <***classname>*** (that is, self-referencing of class name not allowed). At most one other class may be referenced by a class. Any attempt to delete the <***refclassname>*** class while still referenced by any <***classname***> shall fail.

The combined match criteria of <***classname>*** 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 shall fail. The total number of class rules formed by the complete reference class chain (includes 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.

5.20.2.6. no match class-map

This command removes from the specified class definition the set of match conditions defined for another class.

Format no match class-map <refclassname>

Parameter	Description
<refclassname>	The name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

There is no [**not**] option for this match command.

Default None

Mode Class-Map Config / Ipv6-Class-Map Config

5.20.2.7. 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.

Format match cos <0-7>

Parameter	Description
<0-7>	Integer in the range of 0 to 7 specifying the COS value.

Default None

Mode Class-Map Config

5.20.2.8. 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.

Format match secondary-cos <0-7>

Parameter	Description
<0-7>	Integer in the range of 0 to 7 specifying the COS value.

Default None

Mode Class-Map Config

5.20.2.9. 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 <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 <mac-mask> 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).

Format match destination-address mac <address> <mac-mask>

Parameter	Description
<address>	Specifies any layer 2 MAC address.
<mac-mask>	Specifies a layer 2 MAC address bit mask.

Default None

Mode Class-Map Config

5.20.2.10. match dstip

This command adds to the specified class definition a match condition based on the destination IP address of a packet.

Format match dstip <ipaddr> <ipmask>

Parameter	Description
<ipaddr>	Specifies an IP address.
<ipmask>	Specifies an IP address bit mask; note that although similar to a standard subnet mask, this bit mask need not be contiguous.

Default None

Mode Class-Map Config

5.20.2.11. 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 or a numeric range notation.

Format match dstl4port {<port-key> | <0-65535>}

Parameter	Description
<port-key>	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, http, 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.

<0-65535>	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. To specify the match condition using a numeric range notation, two layer 4 port numbers are required and together they specify a contiguous port range. Each port number is an integer from 0 to 65535, but with the added requirement that the second number be equal to or greater than the first.

Default None

Mode Class-Map Config / Ipv6-Class-Map Config

5.20.2.12. 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, ipv6, ipx, mplsmcast, mplsucast, netbios, novell, pppoe, rarp** or as a custom ethertype value in the range of 0x0600-0xFFFF.

Format match ethertype {<keyword> | <0x0600-0xFFFF>}

Parameter	Description
<keyword>	Specifies appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast etc.
<0x0600-0xFFFF>	Specifies ethertype value.

Default None

Mode Class-Map Config

5.20.2.13. 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).

Format match {ip | ipv6} dscp <value>

Parameter	Description
<value>	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 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. To specify a match on all DSCP values, use the match [not] ip tos <tosbits> <tosmask> command with <**tosbits**> set to 0 and <**tosmask**> set to 03 (hex).

Default None

Mode Class-Map Config / Ipv6-Class-Map Config

5.20.2.14. 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.

Format match ip precedence <0-7>

Parameter	Description
<0-7>	Integer from 0 to 7.

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.

To specify a match on all Precedence values, use the match [not] ip tos <tosbits> <tosmask> command with <**tosbits>** set to 0 and <**tosmask>** set to 1F (hex).

Default None

Mode Class-Map Config

5.20.2.15. 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.

Format match ip tos <tosbits> <tosmask>

Parameter	Description
<tosbits>	Two-digit hexadecimal number from 00 to ff.
<tosmask>	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).

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.

In essence, this the “free form” version of the IP DSCP/Precedence/TOS match specification in that the user has complete control of specifying which bits of the IP Service Type field are checked.**Default** None

Mode Class-Map Config

5.20.2.16. match protocol

This command adds to the specified class definition a match condition based on the value of the IP Protocol field in a packet using a single keyword notation or a numeric value notation.

Format match protocol {<protocol-name> | <0-255>}

Parameter	Description
<protocol-name>	One of the supported protocol name keywords . The currently supported values are: **icmp, igmp, ip, tcp, udp**. Note that a value of **ip** is interpreted to match all protocol number values.
<0-255>	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.

This command does not validate the protocol number value against the current list defined by IANA.**Default** None

Mode Class-Map Config / Ipv6-Class-Map Config

5.20.2.17. 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).

Format match source-address mac <address> <macmask>

Parameter	Description
<address>	Specifies any layer 2 MAC address.
<macmask>	Specifies a layer 2 MAC address bit mask.

Default None

Mode Class-Map Config

5.20.2.18. match scrip

This command adds to the specified class definition a match condition based on the source IP address of a packet.

Format match srcip <ipaddr> <ipmask>

Parameter	Description
< ipaddr >	Specifies an IP address .
< ipmask >	specifies an IP address bit mask; note that although it resembles a standard subnet mask, this bit mask need not be contiguous.

Default None

Mode Class-Map Config

5.20.2.19. 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 or a numeric range notation.

Format match srcl4port {<port-key> | <0-65535>}

Parameter	Description
<port-key>	One of the supported port name keywords (listed below). The currently supported <portkey> values are: domain, echo, ftp, ftpdata, http, 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.
<0-65535>	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.

	To specify the match condition as a range, two layer 4 port numbers are required and together they specify a contiguous port range. Each port number is an integer from 0 to 65535, but with the added requirement that the second number be equal to or greater than the first.

Default None

Mode Class-Map Config / IPv6-Class-Map Config

5.20.2.20. 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 1 to 4093.

Format match vlan <1-4093>

Parameter	Description
<1-4093>	The VLAN ID is an integer from 1 to 4093.

Default None

Mode Class-Map Config

5.20.2.21. 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 VLAN ID is an integer from 1 to 4093.

Format match secondary-vlan <1-4093>

Parameter	Description
<1-4093>	The VLAN ID is an integer from 1 to 4093.

Default None

Mode Class-Map Config

5.20.2.22. match dstipv6

This command adds to the specified class definition a match condition based on the destination IPv6 address of a packet.

Format match dstip6 <destination-ipv6-prefix/prefix-length>

Parameter	Description
<destination-ipv6-prefix/prefix-length>	IPv6 address and prefix length.

Default None

Mode IPv6-Class-Map Config

5.20.2.23. match srcipv6

This command adds to the specified class definition a match condition based on the source IP address of a packet.

Format match srcip6 <source-ipv6-prefix/prefix-length>

Parameter	Description
<source-ipv6-prefix/prefix-length>	IPv6 address and prefix length.

Default None

Mode IPv6-Class-Map Config

5.20.2.24. match ip6flowlbl

This command adds to the specified class definition a match condition based on the IPv6 flow label value.

Format match ip6flowlbl <label>

Parameter	Description
<label>	IPv6 flow label value in the range of 0 to 1048575.

Default None

Mode IPv6-Class-Map Config

5.20.3. Policy commands

The 'policy' command set is used in DiffServ to define:

Traffic Classification Specify traffic conditioning actions (policing, marking, shaping) to apply to traffic classes.

Service Provisioning Specify bandwidth and queue depth management requirements of service levels (EF, AF, etc.).

The policy commands are used to associate a traffic class, which was defined by the class command set, with one or more QoS policy attributes. This association is then assigned to an interface in a particular direction to form a service. The user specifies the policy name when the policy is created.

The DiffServ CLI does not necessarily require that users associate only one traffic class to one policy. In fact, multiple traffic classes can be associated with a single policy, each defining a particular treatment for packets that match the class definition. When a packet satisfies the conditions of more than one class, preference is based on the order in which the classes were added to the policy, with the foremost class taking highest precedence.

This set of commands consists of policy creation/deletion, class addition/removal, and individual policy attributes. Note that the only way to remove an individual policy attribute from a class instance within a policy is to remove the class instance and re-add 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***.

5.20.3.1. 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 <0-7>

Parameter	Description
<0-7>	Queue ID .

Default None

Mode Policy-Class-Map Config

Incompatibilities Drop

5.20.3.2. drop

This command specifies that all packets for the associated traffic stream are to be dropped at ingress.

Format drop

Default None

Mode Policy-Class-Map Config

Incompatibilities Assign Queue, Mark (all forms), Mirror, Police, Redirect

5.20.3.3. 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> | port-channel <port-channel-intf-num>}

Parameter	Description
<slot/port>	Specifies the physical interface where the mirrored packet send to .
<port-channel-intf-num>	Specifies the port-channel interface where the mirrorred packet send to. The range of the port-channel ID is 1 to 64.

Default None

Mode Policy-Class-Map Config

Incompatibilities Drop, Redirect

5.20.3.4. 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> | port-channel <port-channel-intf-num>}

Parameter	Description
<slot/port>	Specifies which physical **i**nterface that traffic stream are redirected to.
<port-channel-intf-num>	Specifies which port-channel interface that traffic stream are directed to. The range of the port-channel ID is 1 to 64.

Default None

Mode Policy-Class-Map Config

Incompatibilities Drop, Mirror

5.20.3.5. conform-color

This command is used to enable color-aware traffic policing and define the conform-color class maps used. Used in conjunction with the police command where the fields for the conform level (for simple, single-rate, and two-rate policing) are specified. The <class-map-name> parameter is the name of an existing Diffserv class map, where different ones must be used for the conform and exceed colors.

Format conform-color <class-map-name> exceed-color <class-map-name>

Parameter	Description
<class-map-name>	Name of an existing Diffserv class map, where different ones must be used for the conform colors.

Default None

Mode Policy-Class-Map Config

Incompatibilities Drop, Mirror

5.20.3.6. mark cos

This command marks all packets for the associated traffic stream with the specified class of service value in the priority field of the 802.1p header. If the packet does not already contain this header, one is inserted. The CoS value is an integer from 0 to 7.

Format mark cos <0-7>

Parameter	Description
<0-7>	The range of COS value is 0 to 7.

Default None

Mode Policy-Class-Map Config

Incompatibilities Drop, Mark IP DSCP, IP Precedence, Police

5.20.3.7. 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

Default None

Mode Policy-Class-Map Config

Incompatibilities Drop, Mark IP DSCP, IP Precedence, Police

5.20.3.8. 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.

Format class <classname>

Parameter	Description
<classname>	The name of an existing DiffServ class. Note that this command causes the specified policy to create a reference to the class definition.

Default None

Mode Policy-Map Config

5.20.3.9. no class

This command deletes the instance of a particular class and its defined treatment from the specified policy.

Format no class <classname>

Parameter	Description
<classname>	The name of an existing DiffServ class. Note that this command removes the reference to the class definition for the specified policy.

Default None

Mode Policy-Map Config

5.20.3.10. mark ip-dscp

This command marks all packets for the associated traffic stream with the specified IP DSCP value.

Format mark ip-dscp <value>

Parameter	Description
<value>	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.

Default None

Mode Policy-Class-Map Config

Incompatibilities Drop, Mark CoS, Mark IP Precedence, Police

5.20.3.11. 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>

Parameter	Description
<0-7>	IP precedence value in the range of 0 to 7

Default None

Mode Policy-Class-Map Config

Incompatibilities Drop, Mark (all forms)

5.20.3.12. 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-transmit, set-dscp-transmit, setprec-transmit, or transmit. In this simple form of the police command, the conform action defaults to transmit and the violate action defaults to drop.

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-dscp-transmit <value> | set-prec-transmit <0-7> | transmit} [violate-action { drop | set-cos-as-sec-cos | set-cos-transmit <0-7> | set-dscp-transmit <value> | set-prec-transmit <0-7> | transmit }]}

The simple form of the police command uses a single data rate and burst size, resulting in two outcomes:

Parameter	Description
<conform-action & violate-action>	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-dscp-transmit, set-prec-transmit, or set-cos-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. Beside, the set-cos-transmit is to combine only with drop between the conform-action and the violate-action.
<set-cos-transmit>	Priority value is required and is specified as an integer from 0-7.
<set-dscp-transmit>	Required and 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**.
<set-prec-transmit>	IP Precedence value is required and is specified as an integer from 0-7

Default None

Mode Policy-Class-Map Config

Incompatibilities Drop, Mark (all forms)

5.20.3.13. 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-cos, 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-dscp-transmit <value> | set-prec-transmit <0-7> | transmit} exceed-action { drop | set-cos-as-sec-cos | set-cos-transmit <0-7> | set-dscp-transmit <value> | set-prec-transmit <0-7> | transmit} [violate-action { drop | set-cos-as-sec-cos | set-cos-transmit <0-7> | set-dscp-transmit <value> | set-prec-transmit <0-7> | transmit }]}

Parameter	Description
<conform-action & violate-action & exceed-action>	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-dscp-transmit, set-prec-transmit, or set-cos-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. Beside, the set-cos-transmit is to combine only with drop between the conform-action and the violate-action.
<set-cos-transmit>	Priority value is required and is specified as an integer from 0-7.
<set-dscp-transmit>	Required and 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**.
<set-prec-transmit>	IP Precedence value is required and is specified as an integer from 0-7

Default None

Mode Policy-Class-Map Config

5.20.3.14. 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> <1-128> <1-4294967295> <1-128> conform-action {drop | set-cos-as-sec-cos | set-cos-transmit <0-7> | set-dscp-transmit <value> | set-prec-transmit <0-7> | transmit} exceed-action { drop | set-cos-as-sec-cos | set-cos-transmit <0-7> | set-dscp-transmit <value> | set-prec-transmit <0-7> | transmit } [violate-action { drop | set-cos-as-sec-cos | set-cos-transmit <0-7> | set-dscp-transmit <value> | set-prec-transmit <0-7> | transmit}]}

Parameter	Description
<conform-action & violate-action & exceed-action>	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-dscp-transmit, set-prec-transmit, or set-cos-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. Beside, the set-cos-transmit is to combine only with drop between the conform-action and the violate-action.
<set-cos-transmit>	Priority value is required and is specified as an integer from 0-7.
<set-dscp-transmit>	Required and 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**.
<set-prec-transmit>	IP Precedence value is required and is specified as an integer from 0-7

Default None

Mode Policy-Class-Map Config

5.20.3.15. 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.

Format policy-map <policyname> [{in | out}]

no policy-map <policyname>

Parameter	Description
<policyname>	Policy name up to 31 alphanumeric characters.
no	Delete this policy

Default None

Mode Global Config

5.20.3.16. 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>

Parameter	Description
<policyname>	Old Policy name.
<newpolicyname>	New policy name.

Default None

Mode Global Config

5.20.4. Service commands

The 'service' command set is used in DiffServ to define:

Traffic Classification Assign a DiffServ traffic conditioning policy (as specified by the policy commands) to an interface in the incoming direction.

Service Provisioning Assign a DiffServ service provisioning policy (as specified by the policy commands) to an interface in the outgoing direction.

The service commands attach a defined policy to a directional interface. Only one policy may be assigned at any one time to an interface in a particular direction. The policy type (in, out) must match the interface direction to which it is attached.

This set of commands consists of service addition/removal.

The CLI command root is ***service-policy.***

5.20.4.1. service-policy

This command attaches a policy to an interface in a particular direction.

Format service-policy {in | out} <policy-map-name>

Parameter	Description
<policy-map-name>	The name of an existing DiffServ policy, whose type must match the interface direction. Note that this command causes a service to create a reference to the policy.

The command can be used in the **Interface Config** mode to attach a policy to a specific interface. Alternatively, the command can be used in the **Global Config** mode to attach this policy to all system interfaces. The direction value is either in or out.**Default** None

Mode Global Config, Interface Config

Restrictions Only a single policy may be attached to a particular interface in a particular direction at any one time.

5.20.4.2. no service-policy

This command detaches a policy from an interface in a particular direction.

Format no service-policy {in | out} <policy-map-name>

Parameter	Description
<policy-map-name>	The name of an existing DiffServ policy. Note that this command causes a service to remove its reference to the policy.

The command can be used in the **Interface Config** mode to detach a policy from a specific interface. Alternatively, the command can be used in the **Global Config** mode to detach this policy from all system interfaces to which it is currently attached. The direction value is either in or out.

This command effectively disables DiffServ on an interface (in a particular direction).There is no separate interface administrative 'mode' command for DiffServ.**Default** None

Mode Global Config, Interface Config

5.20.5. Show commands

The 'show' command set is used in DiffServ to display configuration and status information for:

- Classes
- Policies
- Services

This information can be displayed in either summary or detailed formats. The status information is only shown when the DiffServ administrative mode is enabled; it is suppressed otherwise. There is also a 'show' command for general DiffServ information that is available at any time.

5.20.5.1. show class-map

This command displays all configuration information for the specified class.

Format show class-map [<classname>]

Parameter	Description
<classname>	The name of an existing DiffServ class.

Default None

Mode Privileged Exec

Display Message

Fields	Definition
Class Name	The name of this class.
Class Type	The class type (all, any, or acl) indicating how the match criteria are evaluated for this class. A class type of all means every match criterion defined for the class is evaluated simultaneously they must all be true to indicate a class match. For a type of any each match criterion is evaluated sequentially and only one need be true to indicate a class match. Class type acl rules are evaluated in a hybrid manner, with those derived from each ACL Rule grouped and evaluated simultaneously, while each such grouping is evaluated sequentially.
L3 Protocol	The Layer 3 protocol for this class. Possible values are IPv4 and IPv6.
Match Criteria	The Match Criteria fields will only be displayed if they have been configured. They will be displayed in the order entered by the user. These are evaluated in accordance with the class type. The possible Match Criteria fields are: Class of Service, Destination IP Address, Destination Layer 4 Port, Destination MAC Address, Every, IP DSCP, IP Precedence, IP TOS, Protocol Keyword, Reference Class, Source IP Address, Source Layer 4 Port, Source MAC Address, and VLAN.
Values	This field displays the values of the Match Criteria.
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	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.
Reference Class Name	The name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

5.20.5.2. 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.

Format show diffserv

Default None

Mode Privileged Exec

Display Message

Fields	Definition
DiffServ Admin mode	The current value of the DiffServ administrative mode.
Class Table Size Current/Max	The current or maximum number of entries (rows) in the Class Table.
Class Rule Table Size Current/Max	The current or maximum number of entries (rows) in the Class Rule Table.
Policy Table Size Current/Max	The Layer 3 protocol for this class. Possible values are IPv4 and IPv6.
Policy Instance Table Size Current/Max	The current or maximum number of entries (rows) in the Policy Instance Table.
Policy Attribute Table Size Current/Max	The current or maximum number of entries (rows) in the Policy Attribute Table.
Service Table Size Current/Max	The current or maximum number of entries (rows) in the Service Table.

5.20.5.3. show diffserv service

This command displays policy service information for the specified interface and direction.

Format show diffserv service <slot/port> {in | out}

Parameter	Description
<slot/port>	Specifies a valid slot number and port number for the system. The direction parameter indicates the interface direction of interest.

Default None

Mode Privileged Exec

Display Message

Fields	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	The slot number and port number of the 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.

5.20.5.4. show diffserv service brief

This command displays all interfaces in the system to which a DiffServ policy has been attached. The direction parameter is optional; if specified, only services in the indicated direction are shown.

Format show diffserv service brief [in | out]

Default None

Mode Privileged Exec

Display Message

Fields	Definition
DiffServ Admin 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):

Fields	Definition
Interface	The slot number and port number of the 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.

5.20.5.5. show policy-map

This command displays all configuration information for the specified policy.

Format show policy-map [<policy-map-name>]

Parameter	Description
< policy-map-name >	The name of an existing DiffServ policy.

Default None

Mode Privileged Exec

Display Message

Fields	Definition
Policy Name	The name of this policy.
Policy Type	The policy type, namely whether it is an inbound or outbound policy definition.

The following information is repeated for each class associated with this policy

(only those policy attributes actually configured are displayed):

Fields	Definition
Class Name	The name of this class.
Mark CoS	Denotes the class of service value that is set in the 802.1p header of outbound packets. This is not displayed if the mark cos was not specified.
Mark IP DSCP	Denotes the mark/re-mark value used as the DSCP for traffic matching this class. This is not displayed if mark ip description is not specified using the police-two-rate command, or if policing is in use for the class under this policy.
Mark IP Precedence	Denotes the mark/re-mark value used as the IP Precedence for traffic matching this class. This is not displayed if either mark DSCP or policing is in use for the class under this policy.
Policing Style	This field denotes the style of policing, if any, used simple.
Committed Rate (Kbps)	This field displays the committed rate, used in simple policing, single-rate policing, and two-rate policing.
Committed Burst Size (KB)	This field displays the committed burst size, 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 COS Value	This field shows the priority mark value if the conform action is markcos.
Conform DSCP Value	This field shows the DSCP mark value if the conform action is markdscp.
Conform IP Precedence Value	This field shows the IP Precedence mark value if the conform action is markprec.

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 DSCP Value	This field displays the DSCP mark value if this action is markdscp.
Non-Conform IP Precedence Value	This field displays the IP Precedence mark value if this action is markprec.
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.
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.
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.
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.
Policy Name	The name of this policy. (Note that the order in which the policies are displayed is not necessarily the same order in which they were created.)
Policy Type	The policy type, namely whether it is an inbound or outbound policy definition.
Class Members	List of all class names associated with this policy.

5.20.5.6. show policy-map interface

This command displays policy-oriented statistics information for the specified interface and direction.

Format show policy-map interface {<slot/port> | port-channel <1-64 >} {in | out}

Parameter	Description
<slot/port>	Specifies a valid slot number and port number for the system. The direction parameter indicates the interface direction of interest.
<1-64 >	Specifies the port-channel interface. The range of port-channel ID is 1 to 64.

Default None

Mode Privileged Exec

Display Message

Fields	Definition
Interface	The slot number and port number of the interface (slot/port)
Direction	The traffic direction of this interface service, either in or out.
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:

Fields	Definition
Class Name	The name of this class instance.
In Offered Packets	Count of the packets offered to this class instance before the defined DiffServ treatment is applied. Only displayed for the 'in' direction.
In Discarded Packets	Count of the packets discarded for this class instance for any reason due to DiffServ treatment of the traffic class. Only displayed for the 'in' direction.

i None of the counters listed here are guaranteed to be supported on all platforms. Only supported counters are shown in the display output.

5.20.5.7. show service-policy

This command displays a summary of policy-oriented statistics information for all interfaces in the specified direction. The direction parameter indicates the interface direction of interest. This command enables or disables the route reflector client. A route reflector client relies on a route reflector to re-advertise its routes to the entire AS. The possible values for this field are ***enable*** and ***disable.***

Format show service-policy {in | out}

Default None

Mode Privileged Exec

Display Message

The following information is repeated for each interface and direction (only those interfaces configured with an attached policy are shown):

Fields	Definition
Interface	The slot number and port number of the interface (slot/port).
Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface.

i None of the counters listed here are guaranteed to be supported on all platforms. Only supported counters are shown in the display output.

5.21. ACL Commands

This chapter contains the CLI commands used for showing and configuring MAC Access Control List (ACL) and IP Access Control List (ACL).

5.21.1. Show commands

5.21.1.1. show mac access-lists name

This command displays a MAC access list and all of the rules that are defined for the ACL. The command output varies based on the match criteria configured within the rules of the ACL.

Format show mac access-lists <name>

Parameter	Description
name	The ACL name which is used to identify a specific MAC ACL to display.

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
ACL Name	The name of the MAC ACL rule.
Sequence Number	The ordered rule number identifier defined within the ACL.
Action	Displays the action associated with each rule. The possible values are Permit or Deny.
Source MAC Address	Displays the source MAC address for this rule.
Source MAC Mask	Displays the source MAC mask for this rule.

Destination MAC Address	Displays the destination MAC address for this rule.
Destination MAC Mask	Displays the destination MAC mask for this rule.
Ethertype	Displays the Ethertype keyword or custom value for this rule.
VLAN ID	Displays the VLAN identifier value or range for this rule.
CoS Value	Displays the COS (802.1p) value for this rule.
Assign Queue	Displays the queue identifier to which packets matching this rule are assigned.
Redirect Interface	Displays the slot/port to which packets matching this rule are forwarded.
Mirror Interface	Displays the slot/port to which packets matching this rule are copied.
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.
Redirect External AgentId	Indicates whether matching flow packets are allowed to be sent to external applications running alongside the switch on a control CPU.
Committed Rate	The committed rate defined by the rate-limit attribute.
Committed Burst size	The committed burst size defined by the rate-limit attribute.

5.21.1.2. show mac access-lists

This command displays a summary of all defined MAC access lists in the system.

Format show mac access-lists

Mode Privileged EXEC

Display Message

Fields	Definition
Current number of all ACLs	The number of user-configured rules defined for this ACL
Maximum number of all ACLs	The maximum number of ACL rules.
MAC ACL Name	The name of the MAC ACL rule.
Rules	The number of rules in this ACL.

Direction	Denotes the direction in which this MAC ACL is attached to the set of interfaces listed. The value is Inbound or Outbound.
Interface(s)	Displays the list of interfaces (slot/port) to which this MAC ACL is attached in a given direction.
VLAN(s)	Displays VLAN(s) to which the MAC ACL applies

5.21.1.3. 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 indentify the IP ACL.

Format show ip access-lists [<1-199> | <name>]

Parameter	Description
1-199	The ACL ID used to identify a specific IP ACL to display.
name	The ACL name used to identify a specific IP ACL to display.

Default None

Mode Privileged EXEC , User Exec

Display Message

Fields	Definition
Current number of all ACLs	The number of user-configured rules defined for this ACL
Maximum number of all ACLs	The maximum number of ACL rules.
ACL ID/Name	The identifier or Name of this ACL.
Rules	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)	The interface(s) to which the ACL is applied(ACL interface Bindings)
VLAN(s)	The VLAN(s) to which the ACL is applied(ACL VLAN Bindings)
Sequence Number	The ordered rule number identifier defined within the ACL.
Action	Displays the action associated with each rule. The possible values are Permit or Deny.

Match ALL	Indicates whether this ACL applies to every packet. The possible values are True or False.
IPv4 Protocol	Displays the protocol to filter for this rule.
Source IP Address	Displays the source IP address for this rule.
Source IP Wildcard Mask	Displays the source IP mask for this rule.
Source L4 Port Keyword	Displays the source port for this rule.
Destination IP Address	Displays the destination IP address for this rule.
Destination MAC Mask	Displays the destination IP mask for this rule.
Destination L4 Port Keyword	Displays the destination port for this rule.
IP DSCP	The value specified for IP DSCP.
IP Precedence	The value specified for IP Precedence .
IP TOS	The value specified for IP TOS .
Log	Displays when you enable logging for this rule.
Redirect Interface	The slot/port to which packets matching this rule are forwarded.
Mirror Interface	The slot/port to which packets matching this rule are copied.
Time Range Name	Displays the name of the time-range if the IP ACL rule has referenced a time range.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
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.

5.21.1.4. show access-lists interface

This command displays ACL 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> | port-channel <1-64> } in | out } | control-plane }

Parameter	Description
slot/port	The interface number

1-64	The port-channel ID. The port-channel ID is range from 1 to 64.
in | out	The direction value is either in or out

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
ACL Type	The type of access list (IP,IPv6 or MAC)
ACL ID	The identifier of this ACL.
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).

5.21.1.5. show access-lists vlan

This command displays ACL information for a particular VLAN ID.

Format show access-lists vlan <vlan-id> {in | out}

Parameter	Description
vlan-id	The VLAN ID
in | out	The direction value is either in or out

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
ACL Type	The type of access list (IP,IPv6 or MAC)
ACL ID	The identifier of this ACL.
Sequence Number	The ordered rule number identifier defined within the ACL.

5.21.2. Configuration commands

5.21.2.1. 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.

If a MAC ACL by this name already exists, this command enters Mac-Access-List config mode to allow updating the existing ACL.

Format [no] mac access-list extended <name>

Parameter	Description
name	The ACL name which is used to identify a specific MAC ACL. It is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.
no	Remove this MAC ACL.

Default None

Mode Global Config

5.21.2.2. mac access-list extended rename

This command changes the name of a MAC Access Control List (ACL). The command fails if a MAC ACL by the name *newname* already exists.

Format mac access-list extended rename <oldname> <newname>

Parameter	Description
oldname	The name of an existing MAC ACL to be changed.
newname	New name which uniquely identifies the MAC access list.

Default None

Mode Global Config

5.21.2.3. 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.

Format mac access-list resequence {<name>} <1-2147483647> <1-2147483647>

Parameter	Description
name	The ACL name which is used to identify a specific MAC ACL. It is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.
<1-2147483647>	The sequence number from which to start. The range is 1-2147483647. The default is 1.
<1-2147483647>	The amount to increment. The range is 1-2147483647. The default is 1.

Default 1

Mode Global Config

5.21.2.4. mac access-list

This command creates a new rule for the current MAC access list. Each rule is appended to the list of configured rules for the list. Note that an implicit 'deny all' MAC rule always terminates the access list.

Note: The 'no' form of this command is not supported, as the rules within an ACL cannot be deleted individually. Rather, the entire ACL must be deleted and re-specified.

A rule may either deny or permit traffic according to the specified classification fields. At a minimum, the source and destination MAC value and mask pairs must be specified, each of which may be substituted using the keyword any to indicate a match on any value in that field. The bpdu keyword may be specified for the destination MAC value/mask pair indicating a well-known BPDU MAC value of 01-80-c2-xx-xx-xx (hex), where 'xx' indicates a don't care. The remaining command parameters are all optional.

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).

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 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 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.

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.

Format [1-2147483647] {deny | permit} {{<srcmac> <srcmask>} | any} {{<dstmac> <dstmask>} | any | bpdu} [<ethertypekey> | <0x0600-0xFFFF>] [vlan {{eq <0-4095>}} [cos <0-7>] [log] [time-range time-range-name] [assign-queue <queue-id>] [{mirror | redirect} {<slot/port> | port-channel <portchannel-id>}] [rate-limit <1-4294967295><1-128>]

Parameter	Description
1-2147483647	The sequence number of the ACL.
deny | permit	To deny or permit the matching rule.
srcmac srcmask | any	Specifies designated source MAC address and mask pair or any for this rule
destmac destmask | any | bpdu	Specifies designated destination MAC address and mask pair or any or well-known bpdu for this rule
ethertypekey	Appletalk,arp,ibmsna,ipv4,ipv6,ipx,mplsmcast,mplsucast,netbios,novell,pppoe,rarp.
log	Enable logging for this access list rule
time-range-name	Specify the name of the time-range if the MAC ACL rule has referenced a time range.
queue-id	Specify the queue identifier to which packets matching this rule are assigned
mirror | redirect	Specify the traffic matching the rule to be copied/redirected to the specific slot/port or port-channel.
slot/port	The interface number to be mirrored or redirected to.
portchannel-id	The port channel ID to be mirrored or redirected to.
rate-limit	Specify the allowed rate of traffic as per the configured rate in <1-4294967295> kb/s, and burst-size in <1-128> kilobytes.

Default None

Mode Mac Access-list Config

To remove the rule with the specified ID, use the below **no** form command.

Format no rule-id <ID>

Parameter	Description
ID	The rule with ID to be removed.

Default None

Mode Mac Access-list Config

Format [no] remark <remark>

Parameter	Description
remark	To Add an ACL rule remark
<remark>	The rule ID to be removed.
no	To remove an ACL rule remark

Default None

Mode Mac Access-list Config

5.21.2.5. mac access-group

This command attaches a specific MAC Access Control List (ACL) identified by <name> to an interface, 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 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 for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction will be 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 'Interface Config' mode command is only available on platforms that support independent per-port class of service queue configuration. The VLAN keyword is only valid in the 'Global Config' mode.

The command with out direction does not apply to the packets generated by own-device. For example, the ping packets from device cannot be filtered by this command with out direction.

Format mac access-group <name> [vlan <vlan-id>] {in |out} [<1-4294967295>]

Parameter	Description
name	The ACL name which is used to identify a specific MAC ACL. It is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.
vlan-id	The VLAN ID. The VLAN keyword is only valid in the 'Global Config' mode.
in | out	The direction value is either in or out

1-4294967295	The sequence number of the ACL.

Default None

Mode Global Config

Interface Config

5.21.2.6. ip access-list

Use this command to create an extended IP Access Control List (ACL) identified by <name>, consisting of classification fields defined for the IP header of an IPv4 frame.

If an IP ACL by this name already exists, this command enters IPv4-Access_List config mode to allow updating the existing IP ACL.

Format [no] ip access-list <name>

Parameter	Description
name	The ACL name which is used to identify a specific IP ACL. It is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.
no	Remove this IP ACL identified by <name> from the system.

Default None

Mode Global Config

5.21.2.7. ip access-list rename

This command changes the name of a IP Access Control List (ACL). The command fails if a IP ACL by the name *newname* already exists. The *newname* must be a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.

Format ip access-list rename <oldname> <newname>

Parameter	Description
oldname	The name of an existing IP ACL to be changed.
newname	New name which uniquely identifies the IP access list.

Default None

Mode Global Config

5.21.2.8. 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.

Format ip access-list resequence {name | id } <1-2147483647> <1-2147483647>

Parameter	Description
name	The ACL name which is used to identify a specific IP ACL. It is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.
id	The ACL ID used to identify a specific IP ACL .The value is 1~199.
<1-2147483647>	The sequence number from which to start. The range is 1-2147483647. The default is 1.
<1-2147483647>	The amount to increment. The range is 1-2147483647. The default is 10.

Default 1

Mode Global Config

5.21.2.9. access-list (ip)

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.

Format IP standard ACL

access list <1-99> {remark <remark>} | { [<1-2147483647>] } {deny | permit} {every | <srcip> <srcmask> | host <srcip>} [log] [time-range time-range-name] [assign-queue <queue-id>] [{mirror | redirect} {<slot/port>}] [rate-limit <1-4294967295> <1-128>]

Parameter	Description
1-99	The access list number for the IP standard ACL.
remark	Adds a comment (remark) to an IP standard or IP extended ACL.
1-2147483647	Specifies a sequence number for the IP ACL rule. Every rule is assigned a sequence number which is configured by user or generated by the system.

deny | permit	To deny or permit the matching rule.
every	Matches every packet
<srcip> <srcmask>	Specify a source ip address and source netmask pair for the match condition of this IP ACL rule.
host <srcip>	Specify host designated source ip address for this rule.
log	Enable logging for this access list rule
time-range-name	Specify the name of the time-range if the IP ACL rule has referenced a time range.
queue-id	Specify the queue identifier to which packets matching this rule are assigned
mirror | redirect	Specify the traffic matching the rule to be copied/redirected to the specific slot/port or port-channel.
slot/port	The interface number to be mirrored or redirected to.
portchannel-id	The port channel ID to be mirrored or redirected to.
rate-limit <1-4294967295> <1-128>	Specifies the allowed rate of traffic as per the configured rate in <1-4294967295> kb/s, and burst-size in <1-128> kilobytes

Mode Global Config

Format IP extended ACL

access list <100-199> {remark <remark>} | { [<1-2147483647>] } {deny | permit} {every | { { <0-255> | eigrp | gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp } {<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>] [dscp <value> | precedence <0-7> | tos <tos> [<tosmask>]] [fragments]} [log] [time-range time-range-name] [assign-queue <queue-id>] [{mirror | redirect} {<slot/port> | port-channel <portchannel-id>}] [rate-limit <1-4294967295> <1-128>]

Parameter	Description
100-199	The access list number for the IP extended ACL.
remark	Adds a comment (remark) to an IP standard or IP extended ACL.
1-2147483647	Specifies a sequence number for the IP ACL rule. Every rule is assigned a sequence number which is configured by user or generated by the system.
deny | permit	To deny or permit the matching rule.
every	Matches every packet

{ <0-255> | eigrp | gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp }	Specifies the protocol to filter for an extended IP ACL rule.
srcip srcmask | any | host	Specifies a source IP address and source netmask pair for matching condition of this rule. The parameter *any* specifies srcip as 0.0.0.0 and srcmask as 255.255.255.255. The parameter *host* A.B.C.D specifies srcip as A.B.C.D and srcmask as 0.0.0.0.
dstip dstmask | any | host	Specifies a destination IP address and netmask pair for matching condition of this rule. The parameter *any* specifies srcip as 0.0.0.0 and srcmask as 255.255.255.255. The parameter *host* A.B.C.D specifies srcip as A.B.C.D and srcmask as 0.0.0.0.
Range {<*portkey*> |<*startport*>} {<*portkey*>|<*endport*>}	Specifies the source layer 4 port match condition for the IP ACL rule. You can use the port number ranging from 0-65535 , or specify the *portkey,* which can be one of the following keywords: ● For TCP: bgp,domain,echo,ftp,ftpdata,http,pop2,pop3,smtp,telnet,www. ● For UDP: domain,echo,ntp,rip,snmp,tftp,time,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 the parameter *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 parts of the 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. Note: This option is available only if the protocol is TCP or UDP.
{eq | neq | lt | gt} {<portkey>|<0-65535>}	Specifies the layer 4 port match condition as comparison form for the rule. You can use the port number ranging from 0-65535, or specify the *portkey.* eq: equal to ; lt: less than ; gt: great than ; neq: not equal to. 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 only 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 ot portkey. Note: This option is available only if the protocol is TCP or UDP. Port number matches only apply to unfragmented or first fragments.

flag <value>	Specifies that the IP ACL rule matches on the TCP flags. The *value* parameter represents : +fin, -fin, +syn, -syn, +rst, -rst,+psh, -psh, +ack, -ack, +urg, -urg, established. When + is specified, a match occurs if the specified flag is set in the TCP header. When - is specified, a match occurs if the specified 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. Note: This option is available only if the protocol is TCP.
icmp-type <icmp-type> [icmp-code <icmp-code> | icmp-message <icmp-message>]	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.
dscp <value>	Specifies the TOS for an IP ACL rule depending on a match of DSCP value using parameters dscp.
precedence <0-7>	Specifies the TOS for an IP ACL rule depending on a match of precedence values using parameters <0-7>
tos <tos> [<tosmask>]	Specifies the TOS for an IP ACL rule depending on a match value using parameters *tos/tosmask.*
fragments	Specifies that the IP ACL rule matches on fragmented IP packets.
log	Enable logging for this access list rule
time-range-name	Specify the name of the time-range if the IP ACL rule has referenced a time range.
queue-id	Specify the queue identifier to which packets matching this rule are assigned
mirror | redirect	Specify the traffic matching the rule to be copied/redirected to the specific slot/port or port-channel.
slot/port	The interface number to be mirrored or redirected to.
portchannel-id	The port channel ID to be mirrored or redirected to.

rate-limit <1-4294967295> <1-128>	Specifies the allowed rate of traffic as per the configured rate in <1-4294967295> kb/s, and burst-size in <1-128> kilobytes

Mode Global Config

To remove the rule with the specified ID, use the below **no** form command.

Format no rule-id <ID>

Parameter	Description
ID	The rule with ID to be removed.

Default None

Mode IP Access-list Config

5.21.2.10. no access-list

This command deletes an ACL that is identified by the parameter IP ACL <1-99> *or* <100-199> from the system or remove an ACL rule that is identified by the parameter <1-n> from the an IP ACL <1-99> *or* <100-199>.

Format no access-list {<1-99> | <100-199>} [<rule-id>]

Parameter	Description
1-99	The access list number for the IP standard ACL.
100-199	The access list number for the IP extended ACL.
rule-id	Specifies the access list rule ID. The value is 1~n, where n is the maximum number of user configurable rules per ACL.

Default None

Mode Global Config

5.21.2.11. ip access-group

This command attaches a specified access-control list to an interface, range of interfaces, or all interfaces: or associates it with a VLAN ID in a given direction.

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.

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 command with out direction does not apply to the packets generated by own-device. For example, the ping packets from device cannot be filtered by this command with out direction.

Format ip access-group {<1-199> | <name>} [vlan <vlan-id>] {in | out} [<1-4294967295>]

Parameter	Description
name	The ACL name which is used to identify a specific IP ACL. It is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.
<1-199>	The identifier of this ACL. 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.
vlan-id	The VLAN ID. The VLAN keyword is only valid in the 'Global Config' mode.
in | out	The direction value is either in or out.
1-4294967295	The sequence number of the ACL.

Default None

Mode Global Config
Interface Config

5.21.2.12. no ip access-group

This command removes a specified access-control list from an interface, range of interfaces, or all interfaces: or associates it with a VLAN ID in a given direction.

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.

Format no ip access-group {<1-199> | <name>} [vlan <vlan-id>] {in | out}

Parameter	Description
name	The ACL name which is used to identify a specific IP ACL. It is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.
<1-199>	The identifier of this ACL. 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.
vlan-id	The VLAN ID. The VLAN keyword is only valid in the 'Global Config' mode.
in | out	The direction value is either in or out.

Default None

Mode Global Config

Interface Config

5.21.2.13. {deny|permit}

This command creates a new rule for the current IP access list. Each rule is appended to the list of configured rules for the list.

The 'no' form of this command is not supported, since the rules within an IP ACL cannot be deleted individually. Rather, the entire IP ACL must be deleted and respecified.

An implicit 'deny all' IP rule always terminates the 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.

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 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.

The time-range parameter allows imposing time limitation on the IP ACL rule as defined by the parameter time-range-name . If a time range with the specified name does not exist and the IP 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 IP 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.

Format {deny | permit} {{every [rule-id] [assign-queue <queue-id>] [log] [{{mirror | redirect} <slot/port> | port-channel <port-channel-group-id>}] [rate-limit <1-4294967295> <1-128>] [sequence <1-2147483647>] [time-range <name>]} | {{<0-255> | icmp | ip | tcp | udp} {<source-ip/source-mask> | any | host <srcip>} [eq {<0-65535> | <portkey>}] {<destination-ip/destination-mask> | any | host <dstip>} [eq {<0-65535> | <portkey>}] [flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]] [dscp <value>] [flow-label <vlaue>] [icmp-type <icmp-type> [icmp-code <icmp-code>] | icmp-message <icmp-message>] [fragments] [routing] [rule-id] [assign-queue <queue-id>] [log] [{{mirror | redirect} <slot/port> | port-channel <port-channel-group-id>}] [rate-limit <1-4294967295> <1-128>] [sequence <1-2147483647>] [time-range <name>] }}

Parameter	Description
deny or permit	Specifies whether the IP ACL rule permits or denies the matching traffic.
every	Specifies to match every packet.
[rule-id]	Specifies a rule ID, the value range from 1 to 1023.
[assign-queue <queue-id>]	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned, the value range from 0 to 7.
[log]	Specifies that this rule is to be logged.
{mirror | redirect} {<slot/port> | port-channel <port-channel-group-id>}	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 range from 1 to 4294967295, and burst-size in kbytes range from 1 to 128.
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, the value range from 1 to 2147483647.
time-range <name>	Specifies a time limitation on the ACL rule as defined by the parameter time-range-name.
<0-255>	Specifies the protocol to match for the IP ACL rule, the value range from 0 to 255.
<source-ip/source-mask>	Specifies a source IP address and mask to match for the IP ACL rule.
<destination-ip/destination-mask>	Specifies a destination IP address and mask to match for the IP ACL rule.
Any	Specifying any implies specifying “0.0.0.0“ with mask “255.255.255.255”.
host <srcip>	Specifying host source IP address implies matching the specified IP address.
host <dstip>	Specifying host destination IP address implies matching the specified IP address.

eq {<0-65535> | <portkey>}	Specifies the layer 4 port match condition for the IP 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.
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 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".
dscp <value>	Specifies the dscp value to match for for the IP rule. The value range from 0 to 63 or a DSCP keyword (af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, s1, cs2, cs3, cs4, cs5, cs6, cs7, ef).
flow-label <vlaue>	Specifies the flow-label value to match for for the IP rule. The value range from 0 to 1048575.
icmp-type <icmp-type> [icmp-code <icmp-code> | icmp-message <icmp-message>]	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: 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 IP ACL rule matches on fragmented IP packets.
[routing]	Specifies that IP ACL rule matches on IP packets that have the routing extension header.

Default None

Mode IP-Access-List Config

5.22. IPv6 ACL Commands

5.22.1. Show commands

5.22.1.1. show ipv6 access-lists

This command displays an IPv6 access list and all of the rules that are defined for the IPv6 ACL. Use the [name] parameter to identify a specific IPv6 ACL to display.

Format show ipv6 access-lists [<name>]

Parameter	Description
<name>	ACL name which uniquely identifies the IPv6 ACL to display.

Default None

Mode Privileged EXEC
User EXEC

Display Message

If the "**<name>**" parameter is not specified, the following fields are displayed:

Fields	Definition
Current number of all ACLs	The current number of all ACLs.
Maximum number of all ACLs	The maximum number of all ACLs.
IPv6 ACL Name	The access-list name.
Rules	The number of rules in this ACL.
Direction	The applied direction of the ACL on the interface, inbound or outbound.
Interface(s)	The interfaces which the ACL applied on.
VLAN(s)	The VLAN which the ACL applied on

If the "**<name>**" parameter is specified, the following fields are displayed:

Fields	Definition
ACL Name	The access-list name.
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 Every	Indicates whether this access list applies to every packet. Possible values are True or False.
IPv6 Protocol	The protocol to filter for this rule.
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.
Fragments	Specifies that IPv6 ACL rule matches on fragmented IPv6 packets or not.
Routing	Specifies that IPv6 ACL rule matches on IPv6 packets that have the routing extension header or not.
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.
Redirect External AgentId	The agent-id is a unique identifier for the external receive client application . Indicates whether matching flow packets are allowed to be sent to external applications running alongside ICOS on a control CPU.
Time Range Name	Displays the name of the time-range if the Ipv6 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.
Committed Burst	The committed burst size defined by the rate-limit attribute.

5.22.2. Configuration Commands

5.22.2.1. 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.

To delete the IPv6 ACL identified by <name> from the system, use the no form of this command.

Format ipv6 access-list <name>

no ipv6 access-list <name>

Parameter	Description
<name>	access-list name up to 31 characters in length.

Default None

Mode Global Config

The CLI mode changes to IPv6-Access-List Config mode when you successfully execute this command.

5.22.2.2. 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 <oldname> <newname>

Parameter	Description
<oldname>	Current Access Control List name.
<newname>	New Access Control List name.

Default None

Mode Global Config

5.22.2.3. 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.

Format ipv6 access-list resequence <name> <1-2147483647> <1-2147483647>

Parameter	Description
name	The ACL name which is used to identify a specific IP ACL. It is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.
<1-2147483647>	The sequence number from which to start. The range is 1-2147483647. The default is 1.
<1-2147483647>	The amount to increment. The range is 1-2147483647. The default is 10.

Default 1

Mode Global Config

5.22.2.4. {deny|permit}

This command creates a new rule for the current IPv6 access list. Each rule is appended to the list of configured rules for the list.

The 'no' form of this command is not supported, since the rules within an IPv6 ACL cannot be deleted individually. Rather, the entire IPv6 ACL must be deleted and respecified.

An implicit 'deny all' IPv6 rule always terminates the 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.

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 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.

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.

Format {deny | permit} {{every [rule-id] [assign-queue <queue-id>] [log] [{{mirror | redirect} <slot/port> | port-channel <port-channel-group-id>}] [rate-limit <1-4294967295> <1-128>] [sequence <1-2147483647>] [time-range <name>]} | {{<0-255> | icmpv6 | ipv6 | tcp | udp} {<source-ipv6-prefix/prefix-length> | any | host <ipv6 srcip>} [eq {<0-65535> | <portkey>}] {<destination-ipv6-prefix/prefix-length> | any | host <ipv6 dstip>} [eq {<0-65535> | <portkey>}] [flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]] [dscp <value>] [flow-label <vlaue>] [icmp-type <icmp-type> [icmp-code <icmp-code>] | icmp-message <icmp-message>] [fragments] [routing] [rule-id] [assign-queue <queue-id>] [log] [{{mirror | redirect} <slot/port> | port-channel <port-channel-group-id>}] [rate-limit <1-4294967295> <1-128>] [sequence <1-2147483647>] [time-range <name>] }}

Parameter	Description
deny or permit	Specifies whether the IPv6 ACL rule permits or denies the matching traffic.
every	Specifies to match every packet.
[rule-id]	Specifies a rule ID, the value range from 1 to 1023.
[assign-queue <queue-id>]	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned, the value range from 0 to 7.
[log]	Specifies that this rule is to be logged.
{mirror | redirect} {<slot/port> | port-channel <port-channel-group-id>}	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 range from 1 to 4294967295, and burst-size in kbytes range from 1 to 128.
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, the value range from 1 to 2147483647.
time-range <name>	Specifies a time limitation on the ACL rule as defined by the parameter time-range-name.
<0-255>	Specifies the protocol to match for the IPv6 ACL rule, the value range from 0 to 255.
<source-ipv6-prefix/prefix-length>	Specifies a source IPv6 source address and prefix length to match for the IPv6 ACL rule.
<destination-ipv6-prefix/prefix-length>	Specifies a source IPv6 destination address and prefix length to match for the IPv6 ACL rule.
Any	Specifying any implies specifying “::/0 “
host <ipv6 srcip>	Specifying host source-ipv6-address implies matching the specified IPv6 address.
host <ipv6 dstip>	Specifying host destination-ipv6-address implies matching the specified IPv6 address.

eq {<0-65535> | <portkey>}	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.
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".
dscp <value>	Specifies the dscp value to match for for the IPv6 rule. The value range from 0 to 63 or a DSCP keyword (af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, s1, cs2, cs3, cs4, cs5, cs6, cs7, ef).
flow-label <vlaue>	Specifies the flow-label value to match for for the IPv6 rule. The value range from 0 to 1048575.
icmp-type <icmp-type> [icmp-code <icmp-code> | icmp-message <icmp-message>]	This option is available only if the protocol is ICMPv6. Specifies a match condition for ICMP packets. When *icmp-type* is specified, the IPv6 ACL rule matches on the specified ICMP message type, a number from 0 to 255. When *icmp-code* is specified, the IPv6 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: 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).

Default None

Mode IPv6-Access-List Config

5.22.2.5. no rule-id

This command removes a rule for the current IPv6 access list.

Format no rule-id <ID>

Parameter	Description
<ID>	Specifies a rule ID, the value range from 1 to 2147483647.

Default None

Mode IPv6-Access-List Config

5.22.2.6. ipv6 traffic-filter

This command either attaches a specific IPv6 ACL identified by <name> to an interface or associates 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 control-plane and 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.

To remove an IPv6 ACL identified by <name> from the interface(s) in a given direction, use the no form of this command.

Format ipv6 traffic-filter <name> {{control-plane | in | out} | vlan <vlan-id> {in | out}} [<1-4294967295>]

no ipv6 traffic-filter <name> {{control-plane | in | out} | vlan <vlan-id> {in | out}}

Parameter	Description
in|out	The direction value is either in or out.
<vlan-id>	VLAN ID. The range of VLAN ID is 1 to 4093.
<1-4294967295>	The sequence number (greater than 0) to rank precedence for this interface and direction. A lower sequence number has higher precedence. The range of sequence is 1 to 4294967295.

Default None

Mode Global Config
Interface Config

5.23. CoS (Class of Service) Command

5.23.1. Show commands

5.23.1.1. show queue cos-map

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 queue cos-map {<slot/port> | port-channel <id>}

Parameter	Description
slot/port	The interface number.
id	Specified the port channel ID

Default None

Mode Privileged EXEC

Display Message

The following information is repeated for each user priority.

Fields	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.

5.23.1.2. show queue 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 show queue ip-dscp-mapping

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
IP DSCP	Displays IP DSCP value.
Traffic Class	Displays the queue mapping.

5.23.1.3. show queue 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 specified, the port trust mode of the interface is displayed. If omitted, the port trust mode of each interface in the system is shown. If the platform does not support independent per-port class of service mappings, the output represents the system-wide port trust mode used for all interfaces.

Format show queue trust {<slot/port> | port-channel <id>}

Parameter	Description
slot/port	The interface number.
id	Specified the port channel ID

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
Class of Service Trust Mode	The trust mode of this interface.
Non-IP Traffic Class	The traffic class used for non-IP traffic. This is only displayed when the COS trust mode is set to either 'trust ip-dscp' or 'trust ip-precedence'.
Untrusted Traffic Class	The traffic class used for all untrusted traffic. This is only displayed when the COS trust mode is set to 'untrusted'.

5.23.1.4. show queue 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 queue trust {<slot/port> | port-channel <id>}

Parameter	Description
slot/port	The interface number.
id	Specified the port channel ID

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
Interface	This displays 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.

The following information is repeated for each queue on the interface.

Fields	Definition
Queue Id	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 Mgmt Type	The queue depth management technique used for this queue, either tail drop or weighted random early discard (WRED). This is a configured value.

5.23.1.5. show queue 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.

Format show queue random-detect {<slot/port> | port-channel <id>}

Parameter	Description
slot/port	The interface number.
id	Specified the port channel ID

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
Queue Id	Interface supports n queues numbered 0 to (n-1). The specific 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 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.

5.23.2. Configuration commands

5.23.2.1. queue cos-map

This command maps an 802.1p priority to an internal traffic class on a "per-port" basis.

Format queue cos-map <0-7> <0-7>

no queue cos-map

Parameter	Description
<0-7>	The range of queue priority is 0 to 7.
<**0-7>**	The range of mapped traffic class is 0 to 7**.**
no	Reset to the default mapping of the queue priority and the mapped traffic class.

Default None

Mode Interface Config

This command maps an 802.1p priority to an internal traffic class for a device.

Format queue cos-map all <0-7> <0-7>

no queue cos-map all

Parameter	Description
<0-7>	The range of queue priority is 0 to 7.
<**0-7>**	The range of mapped traffic class is 0 to 7**.**
no	Reset to the default mapping of the queue priority and the mapped traffic class.

Default None

Mode Global Config

5.23.2.2. queue trust

This command sets the class of service trust mode of an interface. You can set the mode to trust one of the Dot1p (802.1p) or IP DSCP 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.

Format queue trust {dot1p | ip-dscp | untrusted} all

no queue trust all

Parameter	Description
no	Sets the class of service trust mode to untrusted for all interfaces.

Default dot1p

Mode Global Config

Format queue trust {dot1p | ip-dscp | untrusted}

no queue trust

Parameter	Description
no	Sets the class of service trust mode to untrusted for an interfaces.

Default dot1p

Mode Interface Config

5.23.2.3. queue cos-queue min-bandwidth

This command specifies the minimum transmission bandwidth guarantee for each interface queue.

Format queue cos-queue min-bandwidth <bw-0> <bw-1> ⋯ <bw-7>

no queue cos-queue min-bandwidth

Parameter	Description
<bw-0> <bw-1> <bw-7>	Each Valid range is (0 to 100) in increments of 5 and the total sum is less than or equal to 100.
no	Restores the default for each queue's minimum bandwidth value.

Default None

Mode Interface Config

This command specifies the minimum transmission bandwidth guarantee for each interface queue in the device.

Format queue cos-queue min-bandwidth all <bw-0> <bw-1> ⋯ <bw-7>

no queue cos-queue min-bandwidth all

Parameter	Description
<bw-0> <bw-1> <bw-7>	Each Valid range is (0 to 100) in increments of 5 and the total sum is less than or equal to 100.
no	Restores the default for each queue's minimum bandwidth value in the device.

Default None

Mode Global Config

5.23.2.4. queue cos-queue strict

This command activates the strict priority scheduler mode for each specified queue on a "per-port" basis.

Format queue cos-queue strict <queue-id-0> [<queue-id-1> ⋯ <queue-id-7>]

no queue cos-queue strict <queue-id-0> [<queue-id-1> ⋯ <queue-id-7>]

Parameter	Description
<queue-id>	Queue ID from 0 to 7.
no	Restores the default weighted scheduler mode for each specified queue on a "per-port" basis.

Default None

Mode Interface Config

This command activates the strict priority scheduler mode for each specified queue on a device.

Format queue cos-queue strict all <queue-id-0> [<queue-id-1> ⋯ <queue-id-7>]

no queue cos-queue strict all <queue-id-0> [<queue-id-1> ⋯ <queue-id-7>]

Parameter	Description
<queue-id>	Queue ID from 0 to 7.
no	Restores the default weighted scheduler mode for each specified queue on a device.

Default None

Mode Global Config

5.23.2.5. queue cos-queue traffic-shape

This command specifies the maximum transmission bandwidth limit for the interface as a whole. Also known as rate shaping, this has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded.

Format queue cos-queue traffic-shape <bw>

no queue cos-queue traffic-shape

Parameter	Description
<bw>	Valid range is (0 to 100) in increments 1.
no	Restores the default shaping rate value.

Default None

Mode Interface Config

This command specifies the maximum transmission bandwidth limit for all interfaces. Also known as rate shaping, this has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded.

Format queue cos-queue traffic-shape all <bw>

no queue cos-queue traffic-shape all

Parameter	Description
< bw >	Valid range is (0 to 100) in increments 1.
no	Restores the default shaping rate value for all interfaces.

Default None

Mode Global Config

5.23.2.6. queue cos-queue random-detect

This command activates weighted random early discard (WRED) for each specified queue on the interfaces. Specific WRED parameters are configured using the random-detect queue-parms and the random-detect exponential-weighting-constant commands.

Format queue cos-queue random-detect <queue-id-0> [<queue-id-1> ⋯ <queue-id-7>]

no queue cos-queue random-detect <queue-id-0> [<queue-id-1> ⋯ <queue-id-7>]

Parameter	Description
<queue-id>	Queue ID from 0 to 7.
no	Restores the default value.

Default None

Mode Global Config

Interface Config

5.23.2.7. 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 <exponent>

no random-detect exponential-weighting-constant

Mode Global Config

Interface Config

5.23.2.8. 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 <maxthresh-green> <maxthresh-yellow> <maxthresh-red> <maxthresh-nontcp> drop-prob <drop-prob-green> <drop-prob-yellow> <drop-prob-red> <drop-prob-nontcp> [ecn]

no random-detect queue-parms <queue-id> [<queue-id> …]

Mode Global Config

Interface Config

Parameter	Description
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 class of service 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 S queues. When ECN is enabled, packets not marked as ECN capable are dropped when selected for discard by WRED.

5.24. iSCSI Optimization Commands

This section describes commands you use to monitor iSCSI sessions and prioritize iSCSI packets. iSCSI Optimzation provides a means of giving traffic between iSCSI initiator and target systems special Quality of Service (QoS) treatment. This is accomplished by monitoring traffic to detect packets used by iSCSI stations to establish iSCSI sessions and connections. Data from these exchanges is used to create classification rules that assign the traffic between the stations to a configured traffic class. Packets in the flow are queued and scheduled for egress on the destination port based on these rules.

5.24.1. show iscsi

Use this command to display the iSCSI settings.

Format show iscsi

Mode Privileged EXEC

Display Message

Fields	Definition
iSCSI enabled/disabled	Displays if iSCSI session monitor is enabled or disabled.
iSCSI Egress queue	Indicates the egress queue for the iSCSI session.
Session aging time	The number of minutes a session must be inactive prior to its removal. Range: 1-43,200
Maximum number of sessions	Indicates the maximum number of the iSCSI sessions. The value is 192.
TCP Port	iSCSI target TCP port.
Target IP Address	iSCSI target IP address.
Name	iSCSI target Name

5.24.2. show iscsi sessions

Use this command to display the iSCSI sessions.

Format show iscsi sessions [detailed]

Mode Privileged EXEC

Display Message

Fields	Definition
Session #	The iSCSI sequence number
Target	The target Name
Initiator	The initiator Name
ISID	The iSCSI session ID
Up Time	The starting time for the iSCSI session connected
Time for aging out	The time left to be inactive, in mins.
Target IP Address	The IP address for the target
Target TCP Port	The TCP port number for the target
Initiator IP Address	The IP address for the initiator.
Initiator TCP Port	The TCP port number for the initiator

5.24.3. iscsi enable

Use this command to globally enables iSCSI awareness.

Format iscsi enable

Default Disable

Mode Global Config

5.24.4. no iscsi enable

The command disables iSCSI awareness. When you use the no iscsi enable command, iSCSI resources will be released.

Format no iscsi enable

Default Disable

Mode Global Config

5.24.5. iscsi aging time

Use this command to configure the aging time for iSCSI sessions. Behavior when changing aging time:

- When aging time is increased, current sessions will be timed out according to the new value.
- When aging time is decreased, any sessions that have been dormant for a time exceeding the new setting will be immediately deleted from the table. All other sessions will continue to be monitored against the new time out value.

Format iscsi aging time <time>

Parameter	Description
<time>	Time in minutes. The range of session id is 1 to 43200.

Default 10

Mode Global Config

5.24.6. no iscsi aging time

The command recovery iSCSI aging time to default value.

Format no iscsi aging time

Default 10

Mode Global Config

5.24.7. iscsi queue

Use this command to configure iSCSI egress queue value.

Format iscsi queue <queue>

Parameter	Description
<queue>	iSCSI egress queue value. The range of session id is 0 to 7.

Default 3

Mode Global Config

5.24.8. no iscsi queue

The command recovery iSCSI egress queue out parameter.

Format no iscsi queue

Default 3

Mode Global Config

5.24.9. iscsi target

Use this command to configures an iSCSI target port and, optionally, a target system's IP address and IQN name. When working with private iSCSI ports (not IANA-assigned ports 3260/860), it is recommended to specify the target IP address as well, so that the switch will only snoop frames with which the TCP destination port is one of the configured TCP ports, and the destination IP is the target's IP address. This way the CPU will not be falsely loaded by non-iSCSI flows (if by chance other applications also choose to use these un-reserved ports.

When a port is already defined and not bound to an IP address, and you want to bind it to an IP address, you should first remove it by using the no form of the command and then add it again, this time together with the relevant IP address.

Target names are only for display when using the show iscsi command. These names are not used to match with the iSCSI session information acquired by snooping.

A maximum of 16 TCP ports can be configured either bound to IP or not.

Format iscsi target port <tcp-port1> [<tcp-port2> ... <tcp-port16>] [address <ip-address>] [name <target-name>]

Fields	Definition
tcp-port **1 [** tcp-port **2** tcp-port **16]**	TCP port number or list of TCP port numbers on which the iSCSI target listens to requests. Up to 16 TCP ports can be defined in the system in one command or by using multiple commands.
ip-address	IP address of the iSCSI target. When the no form of this command is used, and the tcp port to be deleted is one bound to a specific IP address, the address field must be present.
target-name	iSCSI name of the iSCSI target. The name can be statically configured; however, it can be obtained from iSCSI or from sendTargets response. The initiator must present both its iSCSI Initiator Name and the iSCSI Target Name to which it wishes to connect in the first login request of a new session or connection. The iSCSI target name containing up to 223 characters.

Default iSCSI well-known ports 3260 and 860 are configured as default but can be removed as any other configured target.

Mode Global Config

5.24.10. no iscsi target

The command delete an iSCSI target port, address, and name.

Format no iscsi target port <tcp-port1> [<tcp-port2> ... <tcp-port16>] [address <ip-address>]

Default iSCSI well-known ports 3260 and 860 are configured as default but can be removed as any other configured target

Mode Global Config

5.25. Domain Name Server Client Commands

5.25.1. show hosts

This command displays the static host name-to-address mapping table.

Format show hosts [<hostname>]

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
DNS Client Source Interface	The source interface of the DNS client.
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 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 examples of the CLI display output for the commands.

```
(M4500-48XF8C) #show hosts

Host name..................................... M4500-48XF8C

Default domain................................ Domain name is not configured

Default domain list........................... Domain Name List is not configured

Domain Name Lookup............................ Enabled

Number of retries............................. 2

Retry timeout period.......................... 3

Name servers (Preference order)............... 10.1.1.7, 10.1.1.6
```

```
Dns Client Source Interface..................... (not configured)


Configured host name-to-address mapping:


 Host                                Addresses

------------------------ ----------------------

No host name is configured to IP address


 Host                    Total   Elapsed    Type        Addresses

---------------------- -------  -------    ----        --------------

No hostname is mapped to an IP address
```

5.25.2. ip host

This command creates a static entry in the DNS table that maps a host name to an IP address.

Format ip host <name> <ipaddr>

Parameter	Definition
<name>	Host name.
<ipaddr>	IPv4 address of the host.

Default None

Mode Global Config

5.25.3. no ip host

Remove the corresponding name to IP address mapping entry.

Format no ip host <name>

Mode Global Config

5.25.4. clear host

This command clears the entire static host name-to-address mapping table.

Format clear host <hostname | all>

Default None

Mode Privileged Exec

5.25.5. ip domain-name

This command defines the default domain name to be appended to incomplete host names (i.e., host names passed from a client are not formatted with dotted notation).

Format ip domain-name <name>

Parameter	Definition
<name>	Default domain name used to complete unqualified host names. Do not include the initial period that separates an unqualified name from the domain name. (Range: 1-64 characters)

Default None

Mode Global Config

5.25.6. no ip domain-name

This command removes the default domain name.

Format no ip domain-name

Mode Global Config

5.25.7. ip domain-list

This command defines the domain list of default domain names to complete unqualified names.

Format ip domain-list <name>

Parameter	Definition

<name>	Domain list indicates list of default domain names to complete unqualified names.

Default None

Mode Global Config

5.25.8. no ip domain-list

This command removes the default domain list.

Format no ip domain-list <name>

Mode Global Config

5.25.9. ip name-server

This command specifies the address of one or more domain name servers to use for name-to-address resolution.

Note: The listed name servers are queried in the specified sequence until a response is received, or the end of the list is reached with no response.

Format ip name-server <ipaddr>

Parameter	Definition
<ipaddr>	IP address of the Domain Name Servers.

Default None

Mode Global Config

5.25.10. no ip name-server

Remove the corresponding Domain Name Server entry from the table.

Format no ip name-server [<ipaddr>]

Mode Global Config

5.25.11. ip name-server source-interface

This command specifies the source address of dns client to use for name-to-address resolution.

Format ip name-server source-interface {<slot/port> | loopback <loopback-id> | serviceport | tunnel <tunnel-id> | vlan <vlan-id>}

Parameter	Definition
<slot/port>	Specifies the interface 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 63.
serviceport	Specifies the serviceport interface to use as the source interface.
<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 interface to use as the source interface. The range of the VLAN ID is 1 to 4093.

Default None

Mode Global Config

5.25.12. no ip name-server source-interface

This command will reset the DNS source interface to the default settings.

Format no ip name-server source-interface

Mode Global Config

5.25.13. ip domain-lookup

This command enables the IP Domain Naming System (DNS)-based host name-to-address translation.

Format ip domain-lookup

Default None

Mode Global Config

5.25.14. no ip domain-lookup

This command disables the IP Domain Naming System (DNS)-based host name-to-address translation.

Format no ip domain-lookup

Mode Global Config

5.25.15. ip domain-retry

This command specifies the number of times to retry sending Domain Name System (DNS) queries.

Format ip domain-retry <0-100>

Parameter	Definition
<0-100>	The number of times to retry sending a DNS query to the server.

Default 2

Mode Global Config

5.25.16. no ip domain-retry

This command will reset the number of retry times to the default settings.

Format no ip domain-retry

Mode Global Config

5.25.17. ip domain-retry-timeout

This command specifies the amount of time to wait for a response to a DNS query.

Format ip domain-retry-timeout <0-3600>

Default 3

Mode Global Config

5.25.18. no ip domain-retry-timeout

This command will reset the timeout to the default setting.

Format no ip domain-retry-timeout

Mode Global Config

5.25.19. ipv6 host

This command creates a static entry in the DNS table that maps a host name to an IPv6 address.

Format ipv6 host <name> <ipv6-address>

Parameter	Definition
<name>	Host name.
<ipv6-address>	IPv6 address of the host.

Default None

Mode Global Config

5.25.20. no ipv6 host

This command removes the corresponding host name from an IPv6 address mapping entry.

Format no ipv6 host <name>

Mode Global Config

5.26. Unidirectional Link Detection Commands

This section describes the commands you use to configure and display Unidirectional Link Detection (UDLD). 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.

5.26.1. udld enable (Global Config)

Use this command to enable UDLD globally on the switch.

Format udld enable

Default Disable

Mode Global Config

5.26.2. no udld enable (Global Config)

Use this command to disable UDLD globally on the switch.

Format no udld enable

Mode Global Config

5.26.3. udld message time

Use this command to configure the interval value (in seconds) between UDLD probe messages on ports that are in the advertisement phase.

Format udld message time <7-90>

Default 15

Mode Global Config

5.26.4. no udld message time

For the interval between UDLD probe messages on ports that are in the advertisement phase, use this command to restore the interval value to the default value.

Format no udld message time

Mode Global Config

5.26.5. udld timeout interval

Use this command to configure the time interval value (in seconds) after which the UDLD link is considered to be unidirectional.

Format udld timeout interval <5-60>

Default 5

Mode Global Config

5.26.6. no udld timeout interval

Use this command to restore the time interval value after which the UDLD link is considered to be unidirectional to the default value.

Format no udld timeout interval

Mode Global Config

5.26.7. udld enable (Interface Config)

Use this command to enable UDLD on the specified interface.

Format udld enable

Default Disable

Mode Interface Config

5.26.8. no udld enable (Interface Config)

Use this command to disable UDLD on the specified interface.

Format no udld enable

Mode Interface Config

5.26.9. udld port

Use this command to select the UDLD mode operating on this interface.

Format udld port [aggressive]

Default normal

Mode Interface Config

5.26.10. udld reset

Use this command to reset all interfaces that have been shutdown by UDLD.

Format udld reset

Mode Privileged EXEC

5.26.11. show udld

Use this command to display the global settings of UDLD. If you specify a slot and port, the command displays the UDLD setting for the specified slot and port.

Format show udld [slot/port | all]

Mode Privileged EXEC
User EXEC

Display Message for the global settings

Parameter	Definition
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) between the decision that the link is unidirectional.

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

```
(M4500-32C) #show udld

Admin Mode..................................... Enabled

Message Interval............................... 15
```

```
Timeout Interval.............................. 5
```

Display Message for a specified slot and port

Parameter	Definition
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 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 switch.

Example: The following example shows the CLI display output for the command show udld 0/3.

(M4500-32C) #show udld 0/3

```
Port         Admin Mode     UDLD Mode      UDLD Status

-------      ----------     -----------     --------------

0/3          Enabled        Aggressive      Bidirectional


 Host device ID: NTGROZ534000A

 Host port ID: 0/3


 Echo entry 1

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

```
Time-To-Live: 39

Neighbor echo 1 device: NTGROZ5200014

Neighbor echo 1 port: 0/3


Message Interval: 15

Timeout Interval: 5

Neighbor Device Name: SW2
```

5.27. Multi-chassis Link Aggregation Commands

This section describes the commands you use to configure and display Multi-Chassis Link Aggregation (MLAG). MLAG allows links that are physically connected to two different devices to appear as a single Port Channel to a third device.

Note: MLAG can support RSTP and IGMP Snooping. The configuration of RSTP and IGMP Snooping on peers of MLAG must be the same to guarantee that MLAG can work correctly.

5.27.1. mlag

This command enables Multi-Chassis Link Aggregation (MLAG) globally.

Format mlag

Default Disable

Mode Global Config

5.27.2. no mlag

This command disables MLAG globally.

Format no mlag

Mode Global Config

5.27.3. mlag domain

This command creates a MLAG domain with the specified domain ID. Only one MLAG domain can be created on a given device. The domain-id of the MLAG domain should be equal to the one configured on the other MLAG peer with which this device wants to form a MLAG pair. The configured MLAG domain-ids are exchanged during role election and if they are configured differently on the peer devices, the MLAG does not become operational. Domain-id is used to derive the auto-generated MLAG virtual MAC address that is used in the actor ID field in the LACP PDUs.

Format mlag domain <1-255>

Default None

Mode Global Config

5.27.4. no mlag domain

This command deletes the MLAG domain with the specified domain ID.

Format no mlag domain <1-255>

Mode Global Config

5.27.5. mlag system-mac

Use this command to manually configure the MAC address for the MLAG domain. The specified MAC address should be a unicast MAC and cannot be equal to the MAC address of either the primary MLAG or secondary MLAG device. The configured MLAG MAC address is exchanged during role election and, if they are configured differently on the peer devices, MLAG does not become operational.

The <mac-address> used in the LACP PDUs and STP BPDUs that are sent out on MLAG member ports, if MLAG primary device election takes place after the MLAG MAC address is configured. When the MLAG MAC address is configured after the MLAG primary device is elected, the operational MLAG MAC address is used in the LACP PDUs and STP BPDUs instead of the configured MLAG MAC address.

Format mlag system-mac < mac-address>

Default 00:00:00:00:00:00

Mode Global Config

5.27.6. no mlag system-mac

This command returns the MLAG system MAC address to the default settings.

Format no mlag system-mac

Mode Global Config

5.27.7. mlag system-priority

This command manually configures a system priority for the MLAG domain. The system-priority is used in the LACPPDU and BPDU. If the configured MLAG system priority is different on MLAG peers, the MLAG will not come up.

Format mlag system-priority <1-65535>

Default 32767

Mode Global Config

5.27.8. no mlag system-priority

This command restores the MLAG system priority to the default settings.

Format no mlag system-priority

Mode Global Config

5.27.9. mlag role priority

This command configures a role priority for the MLAG domain. This value is used for the MLAG role election. The MLAG switch with lower priority becomes the Primary and the switch with higher priority becomes the Secondary. If both MLAG peer switches have the same role priority, the device with the lower system MAC address becomes the Primary.

Format mlag role priority <1-255>

Default 100

Mode Global Config

5.27.10. no mlag role priority

This command resets the MLAG role priority to the default settings.

Format no mlag system-priority

Mode Global Config

5.27.11. mlag peer-link

This command configures a port channel as the MLAG peer link.

Format mlag peer-link

Default None

Mode Port Channel Interface Config

5.27.12. no mlag peer-link

This command removes the MLAG peer link.

Format no mlag peer-link

Mode Port Channel Interface Config

5.27.13. mlag id

This command configures a port channel as part of a MLAG. Upon issuing this command, the port channel is down until the port channel member information is exchanged and agreed between the MLAG peer switches.

Format mlag <1-63>

Default None

Mode Port Channel Interface Config

5.27.14. no mlag id

This command returns the MLAG id to the default settings.

Format no mlag <1-63>

Mode Port Channel Interface Config

5.27.15. mlag peer detection interval

This command configures the DCPDP transmission interval and reception timeout (in mini seconds).

The configurable transmission interval range is 200ms - 4000ms (Default is 1000ms). The configurable reception timeout range is 700ms - 14000ms (Default is 3500ms).

Format mlag peer detection interval <200-4000> timeout <700-14000>

Default Transmission interval: 1000ms
Reception timeout: 3500ms

Mode Global Config

5.27.16. no mlag peer detection interval

This command resets the DCPDP transmission interval and reception timeout to default values.

Format no mlag peer detection interval <200-4000> timeout <700-14000>

Mode Global Config

5.27.17. mlag peer-keepalive destination

This command configures the IP address of the peer MLAG switch, which is the destination IP address of the DCPDP on the peer MLAG switch.

The configurable range for the UDP port is 1 to 65535 (Default is 50000)

Format mlag peer-keepalive destination <ipaddress> source <ipaddress> [udp-port <1-65535>]

Parameter	Description
destination <ipaddress>	The IP address of the peer MLAG switch.
source <ipaddress>	The IP address of the self MLAG switch.
udp-port	The UDP port on which the MLAG switch listens to the DCPDP messages.

Default UDP port: 50000

Mode Global Config

5.27.18. no mlag peer-keepalive destination

This command removes the self IP address and the peer IP address, and returns the UDP port to the default settings.

Format no mlag peer-keepalive destination <ipaddress> switch <ipaddress>

Mode Global Config

5.27.19. mlag peer-keepalive enable

This command starts the keepalive state machine on the MLAG device if MLAG is globally enabled.

Default Disable

Format mlag peer-keepalive enable

Mode Global Config

5.27.20. no mlag peer-keepalive enable

This command stops the MLAG peer keepalive state machine.

Format no mlag peer-keepalive enable

Mode Global Config

5.27.21. mlag peer-keepalive timeout

This command configures the peer keepalive timeout value (in seconds). If a MLAG switch does not receive a keepalive message from the peer for the duration of this timeout value, it transitions its role (if required).

Format mlag peer-keepalive timeout <2-15>

Default 5

Mode Global Config

5.27.22. no mlag peer-keepalive timeout

This command returns the MLAG peer keepalive timeout value to the default settings.

Format no mlag peer-keepalive timeout

Mode Global Config

5.27.23. show mlag brief

This command displays the MLAG global status and current MLAG operational mode including the peer link, keepalive status, number of configured MLAG members, operational MLAG, the system MAC, and role state. If the MLAG operational status is disabled, the reason would be displayed in the brackets of MLAG operational status.

Format show mlag brief

Mode Privileged EXEC

Example1: The following example shows the CLI display output for the command *show mlag brief*. In this example, the MLAG operational status is enabled.

```
(M4500-32C) #show mlag brief


MLAG domain ID.............................. 1

MLAG admin status........................... Enabled

Keep-alive admin status..................... Enabled

MLAG operational status..................... Enabled

Self role................................... Secondary

Peer role................................... Primary

Peer detection admin status................. Disabled

Operational MLAG MAC........................ BC:A5:11:EA:AA:01

Operational MLAG system priority............ 32767


Peer-Link details

-----------------


Interface................................... ch64

Peer-link admin status...................... Up

Peer-link STP admin status.................. Enabled

Configured VLANs............................ 1

Egress tagged VLANs......................... none


MLAG Details

-----------


Number of MLAGs configured.................. 1

Number of MLAGs operational................. 1
```

```
MLAG id# 1

-----------

Interface..................................... ch1

Configured VLANs.............................. 1

MLAG interface state.......................... Active


Local Members        Status

-----------------    ------

0/3                  Up


Peer Members         Status

---------------      ------

0/3                  Up
```

Example2: The following example shows the CLI display output for the command *show mlag brief*. In this example, MLAG operational status is disabled because of disabling MLAG admin status. (The Peer-link would be down if the MLAG operational status or Keep-alive admin status is Disabled, so the peer switch would displayed Peer-link is down in the brackets of MLAG operational status)

```
(M4500-32C) #show mlag brief


MLAG domain ID................................ 1

MLAG admin status............................. Disabled

Keep-alive admin status....................... Enabled

MLAG operational status....................... Disabled(Mlag admin status is disable)

Self role..................................... none

Peer role..................................... none

Peer detection admin status................... Disabled

Operational MLAG MAC.......................... 00:00:00:00:00:00

Operational MLAG system priority.............. 0
```

5.27.24. show mlag

This command displays information about a MLAG. The configuration and operational modes of the MLAG are displayed; the MLAG is operationally enabled if all the preconditions are met. The port-channel that is configured as a MLAG interface is also displayed with the member ports on the current switch and peer switch (with their link status).

Format show mlag <1-63>

Mode Privileged EXEC

Example: The following example shows the CLI display output for the command *show mlag 1*.

```
(M4500-32C) #show mlag 1

MLAG id# 1

-----------------

Config mode..................................... Enabled

Operational mode................................ Enabled

Port channel.................................... ch1


Local Members        Status

-----------------    ------

0/3                  Up


Peer Members         Status

----------------     ------

0/3                  Up
```

5.27.25. show mlag role

This command displays information about the keepalive status and parameters. The role of the MLAG switch as well as the system MAC address and priority are displayed.

Format show mlag role

Mode Privileged EXEC

Example: The following example shows the CLI display output for the command *show mlag role*.

```
(M4500-32C) #show mlag role

Self

----

MLAG domain ID.............................. 1

Keep-alive admin status..................... Enabled

Keep-alive operational status.................. Enabled

Role Priority............................... 100

Configured MLAG MAC......................... 00:00:00:00:00:00

Operational MLAG MAC........................ BC:A5:11:EA:AA:01

Configured MLAG system priority............... 32767

Operational MLAG system priority.............. 32767

Local System MAC............................ 2C:60:0C:8B:63:3B

Time-out.................................... 5

MLAG state.................................. Secondary

MLAG role................................... Secondary

Peer

----

MLAG domain ID.............................. 1

Role Priority............................... 100

Configured MLAG MAC......................... 00:00:00:00:00:00

Operational MLAG MAC........................ BC:A5:11:EA:AA:01

Configured MLAG system priority............... 32767

Operational MLAG system priority.............. 32767

Role........................................ Primary

Local System MAC............................ 2c:60:0c:8b:65:09
```

5.27.26. show mlag consistency-parameters

This command displays the global parameters of the self and peer devices which should be the identical in MLAG domain.

‘ * ‘ means that the parameters between self and peer device configurations are different. “MST VLAN Configuration“ displays associated vlans with MSTP (Multiple Spanning Tree Protocol) instance 0. “IGMP Snooping VLAN Configuration“ displays associated vlans with IGMP Snooping. “MLD Snooping VLAN Configuration“ displays associated vlans with MLD Snooping.

Format show mlag consistency-parameters {global | {interface port-channel <portchannel-id>}}

Mode Privileged Exec

User Exec

Example:

```
(M4500-32C) (Config)#show mlag consistency-parameters global

Parameter                 Self Value              Peer Value              diff
------------------------- ----------------------- ----------------------- -----
STP Mode                  Disabled                Disabled
STP Version               IEEE 802.1w             IEEE 802.1s               *
BPDU Guard Mode           Disabled                Disabled
FDB Age Time (seconds)    1000000                 1000000
ARP Age Time (seconds)    1200                    1200
LACP system priority      32768                   32768
MLAG system MAC address   00:00:00:00:00:00       00:00:00:00:00:00
MLAG system priority      32767                   32767
MLAG domain ID            1                       1
IGMP Admin Mode           Enabled                 Enabled
MLD Admin Mode            Disabled                Disabled

 MST VLAN Configuration

 Instance            Associated VLANS
----------  ------  ------------------------------------------------
 0          Self    1
            Peer    1

 IGMP Snooping VLAN Configuration
             Associated VLANS
----------  ------------------------------------------------
 Self        1
 Peer        1

 MLD Snooping VLAN Configuration
             Associated VLANS
----------  ------------------------------------------------
 Self       1
 Peer       1
```

5.27.27. show mlag peer-keepalive

This command displays the peer MLAG 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 mlag peer-keepalive

Mode Privileged EXEC

Example: The following example shows the CLI display output for the command *show mlag peer-keepalive.*

```
(M4500-32C) #show mlag peer-keepalive

Peer IP address.............................. 172.16.2.33

Source IP address............................ 172.16.2.52

UDP port..................................... 50000

Peer detection admin status.................. Enabled

Peer detection operational status............ Up

Peer is detected............................. TRUE

Configured Tx interval....................... 1000 milliseconds

Configured Rx timeout........................ 3500 milliseconds

Operational Tx interval...................... 1000 milliseconds

Operational Rx timeout....................... 3500 milliseconds
```

5.27.28. show mlag statistics

This command to displays counters for the keepalive and peer-link messages transmitted and received by the MLAG switch.

Format show mlag statistics {peer-keepalive | peer-link}

Mode Privileged EXEC

Example: The following example shows the CLI display output for the command *show mlag statistics peer-keepalive*.

```
(M4500-32C) # show mlag statistics peer-keepalive

Total transmitted............................ 63341

Tx successful................................ 63341
```

```
Tx errors.....................................     0

Total received.............................. 63342

Rx successful............................... 63342

Rx Errors.................................... 0

Timeout counter.............................. 0
```

Example: The following example shows the CLI display output for the command *show mlag statistics peer-link*.

```
(M4500-32C) # show mlag statistics peer-link

Peer link control messages transmitted......... 16

Peer link control messages Tx errors........... 0

Peer link control messages Tx timeout.......... 0

Peer link control messages ACK transmitted..... 64

Peer link control messages ACK Tx errors....... 0

Peer link control messages received............ 64

Peer link data messages transmitted............ 642

Peer link data messages Tx errors.............. 0

Peer link data messages Tx timeout............. 0

Peer link data messages received............... 1298

Peer link BPDU's transmitted to peer........... 0

Peer link BPDU's Tx errors..................... 0

Peer link BPDU's received from peer............ 14

Peer link BPDU's Rx errors..................... 0

Peer link LACPDU's tranmsitted to peer......... 0

Peer link LACPDU's Tx errors................... 0

Peer link LACPDU's received from peer.......... 642

Peer link LACPDU's Rx errors................... 0
```

5.27.29. show mlag core-config

This command displays information about the core configurations to ensure this device can form a MLAG pair.

This command displays two sections: required configurations and optional configurations. In the required configurations section, all the required configurations that starts the MLAG peer keepalive state machine are displayed. In the optional configurations section, the configurations that might change the roles of devices which form MLAG pair are displayed.

Format show mlag core-config

Mode Privileged Exec

User Exec

Example:

```
M4500-32C) (Config)#show mlag core-config

Required configurations
-----------------
MLAG domain ID.............................. 1
MLAG admin status........................... Enabled
Keep-alive admin status..................... Enabled
Peer-link interface......................... ch64
Peer-link admin status...................... Up

Optional configurations
-----------------
Configured MLAG MAC......................... 00:00:00:00:00:00
Role Priority............................... 100
Time-out.................................... 5
```

5.27.30. clear mlag statistics

This command clears all the keepalive and peer-link statistics.

Format clear mlag statistics {peer-keepalive | peer-link}

Mode Privileged EXEC

5.28. Control Plane Policing Commands

Control plane packets are generated or received from network device that are used for the operation of the network itself. Therefore, control plane packets always have a receive destination IP address and are handled by the CPU in the network device. Examples include protocols such as ARP, BGP, OSPF, and other protocols that glue the network together.

Main purpose of Control Plane Policing (CoPP) is to enhance security on the switch to prohibit unnecessary or DoS traffic and giving priority to important control plane and management traffic.

To use CoPP feature needs to set Access Control List (ACL) which matches your purpose and bind it to control-plane interface. Binding ACL to control-plane interface is always considered as “out direction”, so CoPP doesn’t support some ACL conditions which uses for “in direction” only, for example, condition “mirror”, or “redirect”.

You must ensure that the CoPP policy does not filter critical traffic such as routing protocols or interactive access to the switches. If you want to prevent access some of switch services, for example: SSH, it should set destination IP address to switch IP address in associating ACL rules. Since unassigned destination IP address (destination IP address is “any”) will filter out all service associating packets, and make them fail to route to remote server.

5.28.1. interface control-plane

To enter control-plane configuration mode and apply an IP, IPv6 or MAC access list to police traffic destined for the CPU port.

Format interface control-plane

Default None

Mode Global Config

Example: To deny all GRE packets which come from host 10.3.1.1

```
(M4500-32C) #configure

(M4500-32C) (Config)#ip access-list acl001

(M4500-32C) (Config-ipv4-acl)# deny gre host 10.3.1.1 any

Create ACL 1000 : Rule ID 1

(M4500-32C) (Config-ipv4-acl)#permit every

Create ACL 1000 : Rule ID 2

(M4500-32C) (Config-ipv4-acl)#exit
```

```
(M4500-32C) (Config)#interface control-plane

(M4500-32C) (if-control-plane)#ip access-group acl001

(M4500-32C) (if-control-plane)#
```

5.28.2. show access-lists interface control-plane

This command displays IP, IPv6, and MAC ACLs configurations for CPU port.

Format show access-lists interface control-plane

Default None

Mode Privilege EXEC

Example:

```
(M4500-32C) #show access-lists interface control-plane


ACL Type             ACL ID              Sequence Number

-------- ------------------------------- ---------------

IP       acl001                          1


(M4500-32C) #
```

5.29. VXLAN and RIOT Commands

This section describes the commands you use to configure VXLAN and RIOT settings.

5.29.1. vxlan mode

Use this command to set VXLAN mode on the switch.

VXLAN mode must be enabled prior to performing any VXLAN configuration on the switch.

A VXLAN supports two different modes for flood traffic:

1. Multicast mode—A VXLAN uses an IP multicast address as the destination IP address to send broadcast, multicast, and unknown unicast flood frames.

2. Unicast mode—A VXLAN uses each VTEP's single unicast IP address as the destination IP address to send broadcast, multicast, and unknown unicast flood frames.

By default, the mode is disabled. VXLAN mode must be disabled prior to performing any VXLAN mode changed.

Format vxlan mode {unicast | multicast}

Default Disabled

Mode VXLAN Config

Parameter	Description
unicast	Set VXLAN to unicast mode
multicast	Set VXLAN to multicast mode

5.29.2. no vxlan mode

Use this command to return the VXLAN mode to the default settings.

Format no vxlan mode

Mode VXLAN Config

5.29.3. vxlan source-interface

Use this command to configure VXLAN source interface on the switch.

The "vxlan source-interface" command specifies an interface from which the VTEP derives the source address (IP) that it uses when exchanging VXLAN frames. This address is used by UDP headers to specify source and destination addresses of hosts that send or receive VXLAN encapsulated packets.

A valid VXLAN configuration requires the assignment of an interface to the VTEP and the assignment of a valid IP address to the specified interface.

There is no default source interface assignment.

Format vxlan source-interface {<slot/port> | loopback <loopback-id>| vlan <vlan-id>}

Parameter	Description
<slot/port>	The Logic interface number.
<loopback-id>	The Loopback ID. (Range: 0-63)
<vlan-id>	The VLAN ID. (Range: 1-4093)

Default None

Mode VXLAN Config

5.29.4. no vxlan source-interface

Use this command to return VXLAN source interface to the default settings.

Format no vxlan source-interface

Mode VXLAN Config

5.29.5. vxlan udp-port

Use this command to configure VXLAN UDP port on the switch.

Packets bridged to the switch from a specific VLAN are encapsulated with a VXLAN header, sent through a pre-configured UDP port. Packets that arrive through this port are assumed be VXLAN encapsulated packet and forward to the bridging domain of the recipient VLAN which determined by the VNI in the VXLAN header and the VNI and VLAN mapping.

Notice that the UDP port between various VTEPs must be the same, the VXLAN packets can’t forward if the UDP port between source and destination VTEPs are different.

By default, the UDP port is 4789.

Format vxlan udp-port <port-id>

Parameter	Description
<port-id>	The Udp port ID. (Range : 1-65535)

Default 4789

Mode VXLAN Config

5.29.6. no vxlan udp-port

Use this command to return VXLAN udp port to the default settings.

Format no vxlan udp-port

Mode VXLAN Config

5.29.7. vxlan unicast-group

Use this command to configure VXLAN unicast group on the switch.

The setting is available when VXLAN mode is unicast mode. Switch uses each VTEP's source IP address as the destination IP address to send broadcast, multicast, and unknown unicast flood frames. Flood frames are replicated, and encapsulated with a VXLAN header. Packets that have a unicast MAC address will sent directly to the destination VTEP IP address.

There is no default unicast group assignment. The maximum number of unicast group is 32

Format vxlan unicast-group <ipaddr>

Default None

Mode VXLAN Config

5.29.8. no vxlan unicast-group

Use this command to return VXLAN unicast group to the default settings.

Format no vxlan unicast-group <ipaddr>

Mode VXLAN Config

5.29.9. default vxlan multicast-group

Use this command to configure VXLAN default multicast group on the switch.

The setting is available when VXLAN mode is in multicast mode. Switch uses the value as a default multicast group. The default value applied when user creates a new tenant.There is no default multicast group assignment.

Format vxlan default-multicast-group <ipaddr>

Parameter	Description
<ipaddr>	**Configure multicast-group IP address**

Default None

Mode VXLAN Config

5.29.10. no vxlan default-multicast-group

Use this command to return default VXLAN multicast group to the default settings.

Format no vxlan default-multicast-group

Default None

Mode VXLAN Config

5.29.11. vxlan vni multicast-group

Use this command to configure VXLAN multicast group on the switch.

The setting is available when VXLAN mode is multicast mode. Switch uses a specified multicast group as the destination IP address to send broadcast, multicast, and unknown unicast flood frames. Flood frames are encapsulated with a VXLAN header and forwarded. Inter-VTEP multicast communications include all VTEPs that are associated with the specified multicast group.

There is no default multicast group assignment.

Format vxlan vni <vn-id> multicast-group <ipaddr>

Parameter	Description
<vn-id>	**The VNI ID. (Range:1-16777214)**

<ipaddr>	**Configure multicast-group IP address**

Default None

Mode VXLAN Config

5.29.12. no vxlan vni multicast-group

Use this command to return VXLAN multicast group to the default settings.

Format no vxlan vni <vn-id> multicast-group

Mode VXLAN Config

5.29.13. vxlan vlan vni

Use this command to configure VXLAN VLAN to VNI mapping on the switch.

The “vxlan vlan vni” command associates a VLAN ID with a virtual network identifier (VNI). When a VLAN bridges a packet to the VTI, the packet is encapsulated with a VXLAN header that includes the VNI associated with the VLAN. Packets that arrive on the VTI’s UDP socket are bridged to the VLAN that is associated with the VNI specified by the VXLAN header that encapsulates the packet.

All ports belong the VLAN ID will be configured as VXLAN access port.

Format vxlan vlan <vlan> vni <vn-id>

Parameter	Description
<vlan>	The VLAN ID. (Range:1-4093)
<vn-id>	The VNI ID. (Range:1-16777214)

Default None

Mode VXLAN Config

5.29.14. no vxlan vlan vni

Use this command to delete a specific mapping, which is VXLAN VLAN to VNI mapping.

Format no vxlan vlan <vlan> vni <vn-id>

Mode VXLAN Config

5.29.15. interface vxlan

Use this command to configure VXLAN interface on the switch.

Format interface vxlan <vxlan-id>

Parameter	Description
<vxlan-id>	The VXLAN ID. (Range: 1-1)

Default NA

Mode Global Config

5.29.16. show vxlan

Use this command to display detailed information about the VXLAN configured on the switch.

Format show vxlan

Mode Privileged EXEC

Display Message

Parameter	Definition
Interface	VXLAN interface
Mode	VXLAN mode (unicast or multicast)
RIOT Mode	RIOT mode (Enable or disable)
RIOT Physical Loopback Interface	The loopback interface used for RIOT routing
UDP Destination Port	The UDP port which VXLAN uses to send/receive packets
Source Interface	The source interface of VXLAN
VXLAN and VLAN Mapping	The mapping of VLAN to VNI
Unicast Group Address	The IP address used to send broadcast, multicast, and unknown unicast flood frames

Multicast Group Address	The multicast group IP address used to send broadcast, multicast, and unknown unicast flood frames

5.29.17. show vxlan vtep

Use this command to display IP address about the VXLAN remote VTEPs on the switch.

This command only shows remote VTEPs which really have communication with local device. If system doesn't receive any packet from remote VTEPs, it means there is no communication in the environment, this command shows nothing.

Format show vxlan vtep

Mode Privileged EXEC

Display Message

Parameter	Definition
Remote VTEPs for Vxlan	Remote VTEPs which really have communication with local device

5.29.18. show vxlan address-table

Use this command to display MAC address that VXLAN learning on the switch.

If system doesn't learn any MAC address from VXLAN, this command shows nothing.

Format show vxlan address-table

Mode Privileged EXEC

Display Message

Parameter	Definition
Tenant ID	The tenant ID of VXLAN packet
Tenant MAC	Then source MAC address of VXLAN packet
VTEP	The source VTEP of VXLAN packet
Interface	The interface which receive VXLAN packet
Entry Type	Learned or static address

5.29.19. vxlan riot

Use this command to enable RIOT mode on the switch.

VXLAN must be enabled prior to enabling RIOT on the switch. RIOT is supported only under VXLAN unicast mode.

Format vxlan riot

Default Disabled

Mode VXLAN Config

5.29.20. no vxlan riot

Use this command to return the RIOT mode to the default settings.

Format no vxlan riot

Mode VXLAN Config

5.29.21. vxlan riot-physical-loopback

Use this command to assign an interface as the VXLAN RIOT loopback interface on the switch.

VXLAN RIOT must be enabled prior to assigning an VXLAN RIOT loopback interface on the switch. Switch uses a specified physical port (or port-channel) as an VXLAN loopback port to be an VXLAN access port as well as an L3 router port. Therefore, the VXLAN loopback port need to join the VLAN mapped to VXLAN tenant. This VLAN should be a VLAN routing interface and the other front-end ports should not join to this VLAN.

Note: The outgoing packets on the riot loopback port need to be VLAN tagging.

Format vxlan riot-physical-loopback {<slot/port> | port-channel <1-64>}

Parameter	Description
<slot/port>	The Logic interface number.
<port channel id>	The interface number of the port channel. (Range: 1-64)

Default None

Mode VXLAN Config

Here is the configuration example:

```
( Switch ) (Config)#interface 0/8
( Switch ) (Interface 0/8)#switchport allowed vlan add tagged 200
( Switch ) (Interface 0/8)#exit
```

```
( Switch ) (Config)#interface vlan 200
( Switch ) (if-vlan200)# ip address 192.168.20.1 255.255.255.0
( Switch ) (if-vlan200)#exit
( Switch ) (Config)#interface vxlan 1
( Switch ) (if-vxlan-1)#vxlan riot
( Switch ) (if-vxlan-1)#vxlan riot-physical-loopback 0/8
( Switch ) (if-vxlan-1)#vxlan vlan 200 vni 2001
```

5.29.22. no vxlan riot-physical-loopback

Use this command to delete the VXLAN RIOT loopback interface on the switch.

Format no vxlan riot-physical-loopback

Mode VXLAN Config

5.30. 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. Auto Recovery re-enables the interface after the expiry of configured time interval.

5.30.1. 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.

Format errdisable recovery cause {all | arp-inspection | bpduguard | bcast-storm | bpdustrom | dhcp-rate-limit | mcast-storm | port-security | sfp-mismatch | ucast-storm | udld | link-flap | loop-detection}

Default None

Mode Global Config

5.30.2. 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 | bcast-storm | bpdustrom | dhcp-rate-limit | mcast-storm | port-security | sfp-mismatch | ucast-storm | udld | link-flap | loop-detection}

Mode Global Config

5.30.3. errdisable recovery interval

Use this command to configure the auto recovery time interval. The auto recovery time interval is common for all causes. When the recovery interval expires, the system attempts to bring interfaces in the diag-disable state back into service (link up).

Format errdisable recovery interval <30-86400>

Default 300s

Mode Global Config

5.30.4. no errdisable recovery interval

Use this command to return the auto recovery interval to the default settings.

Format no errdisable recovery interval

Mode Global Config

5.30.5. show errdisable recovery

Use this command to display the errdisable configuration status of all configurable causes.

Format show errdisable recovery

Mode Privileged EXEC

Display Message

Parameter	Definition
arp-inspection	Enable/Disable status of arp-inspection auto recovery.
bcast-storm	Enable/Disable status of broadcast storm auto recovery.
mcast-storm	Enable/Disable status of multicast storm auto recovery.
ucast-storm	Enable/Disable status of unicast storm auto recovery.
bpduguard	Enable/Disable status of BPDU guard auto recovery.
port-security	Enable/Disable status of port security 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.
time interval	Time interval for auto recovery in seconds.
link-flag	Enable/Disable status of link-flap.

loop-detection	Enable/Disable status of loop protection.

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

```
#show errdisable  recovery

Errdisable Reason           Auto-recovery Status

------------------          --------------------

dhcp-rate-limit             Disabled

arp-inspection              Disabled

udld                        Disabled

bcast-storm                 Disabled

mcast-storm                 Disabled

ucast-storm                 Disabled

bpdustorm                   Disabled

sfp-mismatch                Disabled

port-security               Disabled

Timeout for Auto-recovery from D-Disable state  300
```

5.30.6. show interfaces status err-disabled

Use this command to display the interfaces that are error disabled and auto-recovery enabled (auto-recovery timer left more than zero).

Format show interface status err-disabled

Mode Privileged EXEC

Display Message

Parameter	Definition
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.

5.31. Role-Based Access Control

Role-Based Access Contro (RBAC) allows you to create roles which define CLI executive permissions of individual functions, and assign roles to a user let him own the suitable authorization to manage and operate the system

User Role

A role contains one or multiple rules that define the operations allowed for the user who is assigned the role, and one user can have multiple roles. For example, if role1 allows managing layer 3 routing functions and role2 allows managing VLAN function, then a user who has both role1 and role2 can manage routing and VLAN functions.

By default, the switch supports the following user roles, which you cannot change or delete:

- **network-admin**: it has full access commands to the entire system.
- **network-operator**: it can access read-only commands to the entire system.

CLI command string inside a rule

A CLI command string is used to define a rule whether to allow one or one kind of CLI commands to execute. The format of command string may be whole and explicit CLI command, likes “ip igmp snooping querier vlan 1”, or use wildcard character ‘*’ on the tail of command string to match any string after prefix string, likes “ip igmp snooping *”.

Feature

Features are system predefined sets of CLI commands which are divided by related functions.

Feature Group

Feature group provides to bond multiple features into a group name and assign to a role. The system administrator could customize different feature groups according to functional categories and give it an appropriate nickname.

Rule

A rule defines what operation could be allowed to execute for a role, in other words, a role is made up of one or many rules. A rule can be applied only one action which is a CLI command string, a feature, or a feature group. Every role has an invisible default rule “deny all commands”, if a user enters a command which can’t match any rule of its roles, this command won’t be permitted to execute.

Each rule must be assigned rule ID which is a unique integer between 1 and 256. All Rules in one role are applied in descending order of role ID, and it means when one role has many rules and some of their definition are conflicting, then the greater ID will be higher priority than less one.

For example, below role1 can execute all related commands about “show ip igmp”, except the command and sub-commands of “show ip igmp snooping”:

Switch(config)# role name role1
*Switch(config-role)# rule 1 permit command “show ip igmp *”*
*Switch(config-role)# rule 2 deny command “show ip igmp snooping *”*

One user could have many roles and there isn’t any different priority between roles. However, if rules are conflicting between roles, the rule that is “permit” action will be higher priority than another rule that is “deny” action.

For example, below User1 has role1 and role2, therefore, User1 can show all related commands of “ip igmp”. Since rule1 of role2 conflicts to rule1 of role1 and “permit” action is higher priority, the rule1 of role2 is invalid.

Switch(config)# role name role1
*Switch(config-role)# rule 1 permit command “show ip igmp *”*

Switch(config)# role name role2
*Switch(config-role)# rule 1 deny command “show ip igmp groups *”*

Switch(config)# username User1 role role1
Switch(config)# username User1 role role2

5.31.1. role based access control enable

This command is used to enable RBAC function.

When enabling RBAC function, only users who have the role 'network-admin' will build rule merged table immediately, other login users won't allow to execute any CLI command until he logout and login again to rebuild its rule merged table.

Format role based access control enable

Default Disabled

Mode Global Config

5.31.2. no role based access control enable

This command is used to disable RBAC function.

Format no role based access control enable

Mode Global Config

5.31.3. role name

This command is used to create a new role or configure an existing role.

- Role name only allows to include alphabetic, numeric, dash, dot or underscore characters only. Name must start with a letter and the size of the name string must be less than or equal to 31 characters.
- Role name is case sensitive.
- System default role “network-admin” and “network-operator” can’t be destroyed or modified.
- The maximum number of roles is 256.
- A role can’t be deleted, if any user still uses it.

Format role name <role-name>

Default None

Mode Global Config

5.31.4. no role name

This command is used to destroy an existing role.

Format no role name <role-name>

Mode Global Config

5.31.5. role description

This command is used to set a description to a role.

- Description could use single quotation mark (‘) or double quotation marks (“) to wrap the text which includes space character.
- The maximum length of description is 255 characters.

Format description <text>

Default None

Mode Role Interface

5.31.6. no role description

This command is used to clear a description to a role.

Format no description

Mode Role Interface

5.31.7. rule command

This command is used to add a rule of command string to a role.

- Rule ID is an integer between 1 and 256, and it shall be unique inside one role.
- Maximum length of rule command string is 255 characters.
- Rule command isn't case sensitive and it's converted to lower case automatically. All space characters put to the head or tail of command string will be deleted, and multiple space characters inside a command string will convert to a single space character.
- Wildcard character '*' can match any string after prefix string, and it shall put to the tail of command string.
- Every word inside a command string must be a whole command word, except the last word with wildcard character '*' could be incomplete, likes "show mac-addr*.
- RBAC doesn't support "No form" format of rule command string, because normal command (e.g. "shutdown") and "No form" command (e.g. "no shutdown") are bonded together to deal with access permission.
- RBAC Rule command shall not start with keyword "do", because keyword "do" will be removed before a command is executed.

Format rule <rule-id> <deny | permit> command <command-string>

Default None

Mode Role Interface

5.31.8. no rule (to delete a rule of command string)

This command is used to delete a rule of command string from a role.

Format no rule <rule-id>

Mode Role Interface

5.31.9. rule feature

This command is used to add a rule of feature to a role.

- Rule ID is an integer between 1 and 256, and it shall be unique inside one role.
- Feature name comes from an existing feature.

Format rule <rule-id> <deny | permit> <read | read-write> feature <name>

Default None

Mode Role Interface

5.31.10. no rule (to delete a rule of feature)

This command is used to delete a rule of feature from a role.

Format no rule <rule-id>

Mode Role Interface

5.31.11. rule feature group

This command is used to add a rule of feature group to a role.

- Rule ID is an integer between 1 and 256, and it shall be unique inside one role.
- Feature group name comes from an existing feature group.
- Feature group name is case sensitive.

Format rule <rule-id> <deny | permit> <read | read-write> feature-group <name>

Default None

Mode Role Interface

5.31.12. no rule (to delete a rule of feature group)

This command is used to delete a rule of feature group from a role.

Format no rule <rule-id>

Mode Role Interface

5.31.13. rule <rule-id> <deny | permit> <read | read-write>

This command is used to add a rule which denies or permits to execute all “show commands” or all commands.

Rule ID is an integer between 1 and 256, and it shall be unique inside one role

Format rule <rule-id> <deny | permit> <read | read-write>

Default None

Mode Role Interface

5.31.14. no rule (to delete a rule of read-write commands)

This command is used to delete a rule of read or read-write commands from a role.

Format no rule <rule-id>

Mode Role Interface

5.31.15. rule renumber

This command is used to change a rule ID to another one.

- Rule ID is an integer between 1 and 256, and it shall be unique inside one role.
- Old rule ID comes from an existing rule, and new rule ID shall not overlap to an existing rule ID.

Format rule <old-rule-id> renumber <new-rule-id>

Default None

Mode Role Interface

5.31.16. role feature-group name

This command is used to create a new feature group or configure an existing feature group.

- Feature group name only allows to include alphabetic, numeric, dash, dot or underscore characters only. Name must start with a letter and the size of the name string must be less than or equal to 63 characters.
- Feature group name is case sensitive.
- The maximum number of feature groups is 256.
- A feature group can’t be deleted, if any rule of a role still uses the feature group.

Format role feature-group name <name>

Default None

Mode Global Config

5.31.17. no role feature-group name

This command is used to delete an existing feature group.

Format no role feature-group name <name>

Mode Global Config

5.31.18. feature

This command is used to add a feature into a feature group.

Feature name is a system pre-defined name, and you need to assign the existing feature name.

Format feature <feature-name>

Default None

Mode Feature Group Interface

5.31.19. no feature

This command is used to remove a feature from a feature group.

Format no feature <feature-name>

Mode Feature Group Interface

5.31.20. username role

This command is used to to assign a role to a user.

- Username comes from an existing user.
- Role name comes from an existing role
- User 'admin' is a system account of administrator and it shall always own the system default role 'network-admin'.
- When RBAC function enables, a user can't access any command if he doesn’t be assigned any role.

Format username <user-name> role <role-name>

Default None

Mode Global Config

5.31.21. no username role

This command is used to remove a role from a user.

Format no username <user-name> role <role-name>

Mode Global Config

5.31.22. show role

This command is used to to display information about roles.

Format show role [name <role-name>]

Default None

Mode Privileged EXEC

Display Message

Parameter	Definition
Role Based Access Control	Indicates RBAC function is enabled or disabled now.
Current numbers of roles	Indicates how many numbers of roles are created now.
Maximum numbers of roles	Indicates maximum numbers of roles can be created on the device.
Role	The role name.
Description	Description of this role.
ID	Rule ID
Permit	Indicates permit or deny this role to execute this rule.
Read & Write	Indicate this rule is “read” or “read-write”. The “read” means “it can execute ‘show command’ only”, and “read-write” means “it can execute ‘all commands’.
Type	Indicates type of this rule is command string, feature, or feature group.
Content	Detailed definition of this rule.

5.31.23. show role feature

This command is used to to display information about features.

Format show role feature [detail | name <feature-name>]

Default None

Mode Privileged EXEC

Display Message

Parameter	Definition
Feature name	The system pre-defined feature name.
Command strings of feature	This feature contains related command strings.

5.31.24. show role feature group

This command is used to to display information about feature groups.

Format show role feature-group [detail | name <feature-group-name>]

Default None

Mode Privileged EXEC

Display Message

Parameter	Definition
Current numbers of feature group	Indicates how many numbers of feature groups are created now.
Maximum numbers of feature group	Indicates maximum numbers of feature groups can be created on the device.
feature group name	The name of this feature group.
Feature name	The system pre-defined feature name.
Command strings of feature	This feature contains related command strings.

5.31.25. show role user

This command is used to to display information of roles according to users.

Commands “show role user current”, “show role feature *”, and “show role feature groups *” are RBAC common permitted commands, and that is in order to get what commands can be executed for every user.

Format show role user [current | name <username>]

Default None

Mode Privileged EXEC

Display Message

Parameter	Definition
Username	The name of assigned user.
Authenticated method	Indicates what kind of login authenticated method to use by this user. Possible values are LOCAL, RADIUS, and TACACS
Current numbers of total commands per user	The total command strings which include rule commands, features, and feature-groups of all roles are assigned to this user.

Maximum numbers of total commands per user	The maximun numbers of total commands can be set to one user.
Role	The role name.
Description	Description of this role.
ID	Rule ID
Permit	Indicates permit or deny this role to execute this rule.
Read & Write	Indicate this rule is “read” or “read-write”. The “read” means “it can execute ‘show command’ only”, and “read-write” means “it can execute ‘all commands’.
Type	Indicates type of this rule is command string, feature, or feature group.
Content	Detailed definition of this rule.

5.32. Application Commands

Use the application commands to manage applications on switches.

5.32.1. show application

This command displays the applications installed and their parameters.

Format show application

Mode Privileged EXEC

Display Message

Fields	Definition
Name	The name of the application.
StartOnBoot	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.
AutoRestart	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.
CPU Sharing	The configured application CPU utilization limit expressed as a percentage. 0 if unlimited.
Max Memory	The configured application memory limit in megabytes. 0 if unlimited.

5.32.2. 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

Display Message

Fields	Definition
File size	Number of bytes the file occupies in the file system.

filename	Name of the file.
Total bytes for all files	Number of bytes all the files in the application directory.

5.32.3. application install

This command starts the application through the designated executable file available for configuration and execution. The parameters of this command determine how the application runs 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 pre-configuration 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>]

no application install <filename>

Default Enabled

Mode Global Config

Fields	Definition
<filename>	The name of the file containing the executable or script that is started as a Linux process for the application.
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.
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.
cpu-sharing	Sets the CPU share allocated to this application, expressed as a percentage between 0 and 99. If 0 is specified, the application prcess(es) are not limited. If this keyword is not specified, the default value 0 is used.
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 keyword is not specified, the default value 0 is used.

5.32.4. 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

5.32.5. application stop

This command stops the execution of the specified application.

Format application stop <filename>

Mode Privileged EXEC

5.33. Precision Time Protocol Transparant Clock Commands

The switch supports Precision Time Protocol (PTP) Transparant Clock (TC).

5.33.1. ptp clock e2e-transparent

Use this command to enable the PTP E2E transparent clock at system level (that is, globaly) or for an interface. In Global Config mode, the command applies the PTP transparent clock configuration to all physical ports and LAGs on the switch. In Interface Config mode, the command provides a next-level control so that you can disable this feature selectively for an individual physical port or LAG.

You can configure the PTP transparent clock for physical ports and LAGs, but not for another type of interface, such as a VLAN, loopback, or tunnel. If you configure the PTP transparent clock on a LAG, the configuration is applied to all member ports. For example, if a member port is enabled and the LAG is disabled, the operational mode of that member is disabled because the LAG configuration takes precedence over the administrative mode of the member port.

To disable the PTP E2E transparent clock at system level or for an interface, use the no form of this command.

Format ptp clock e2e-transparent

no ptp clock e2e-transparent

Default Enabled at system level and for all interfaces

Mode Global Config

Interface Config

5.33.2. show ptp clock e2e-transparent

Use this command to display the operational and configuration status of the PTP E2E transparent clock, both at system level and at interface level.

Format show ptp clock e2e-transparent

Mode Privileged Exec

Display Message

Fields	Definition
Interface	The interface on which the feature is configured.
Configured Mode	The configuration status of the PTP E2E transparent clock on the interface.
Operational Mode	The operational status of the PTP E2E transparent clock on the interface.

Example:

```
(M4500-48XF8C) # show ptp clock e2e-transparent

PTP TC global mode..................................... Enabled

Interface   Configured Mode Operational Mode

---------   --------------- ----------------

0/1         Disabled        Disabled

0/2         Disabled        Disabled

0/3         Disabled        Disabled

0/4         Disabled        Disabled

0/5         Disabled        Disabled

0/6         Disabled        Disabled

0/7         Disabled        Disabled

0/8         Disabled        Disabled

0/9         Disabled        Disabled

0/10        Disabled        Disabled

0/11        Disabled        Enabled

0/12        Disabled        Enabled

0/13        Disabled        Disabled

0/14        Disabled        Disabled
```

6. Routing Commands

6.1. Address Resolution Protocol (ARP) Commands

6.1.1. Show commands

6.1.1.1. show ip arp

This command displays the Address Resolution Protocol (ARP) cache. If the VRF is not specified, the shown ARP cache is in the default VRF. If the VRF is specified, the ARP cache in the specified VRF is shown.

Format show ip arp [vrf <vrf-name>]

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
Age Time	Is the time it takes for an ARP entry to age out. This value was configured into the unit. Age time is measured in seconds.
Response Time	Is the time it takes for an ARP request timeout. This value was configured into the unit. Response time is measured in seconds.
Retries	Is the maximum number of times an ARP request is retried. This value was configured into the unit.
Cache Size	Is the maximum number of entries in the ARP table. This value was configured into the unit.
Dynamic renew mode	Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they aged out.
Total Entry Count Current/Peak	Field listing the total entries in the ARP table and the peak entry count in the ARP table.
Static Entry Count Configured/Active/Max	Field listing configured static entry count, active static entry count, and maximum static entry count in the ARP table.

The following are displayed for each ARP entry.

Fields	Definition
IP Address	Is the IP address of a device on a subnet attached to an existing routing interface.

MAC Address	Is the hardware MAC address of that device.
Interface	Is the routing slot/port associated with the device ARP entry.
Type	Is the type that was configured into the unit. The possible values are Local, Gateway, Dynamic and Static.
Age	This field displays the current age of the ARP entry since last refresh (in hh:mm:ss format).

6.1.1.2. show ip arp brief

This command displays the brief Address Resolution Protocol (ARP) table information. If the VRF is not specified, the shown ARP cache is in the default VRF. If the VRF is specified, the ARP cache in the specified VRF is shown.

Format show ip arp [vrf <vrf-name>] brief

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
Age Time	Is the time it takes for an ARP entry to age out. This value was configured into the unit. Age time is measured in seconds.
Response Time	Is the time it takes for an ARP request timeout. This value was configured into the unit. Response time is measured in seconds.
Retries	Is the maximum number of times an ARP request is retried. This value was configured into the unit.
Cache Size	Is the maximum number of entries in the ARP table. This value was configured into the unit.
Dynamic renew mode	Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they aged out.
Total Entry Count Current/Peak	Field listing the total entries in the ARP table and the peak entry count in the ARP table.
Static Entry Count Configured/Active/Max	Field listing configured static entry count, active static entry count, and maximum static entry count in the ARP table.

6.1.1.3. show ip arp static

This command displays the static Address Resolution Protocol (ARP) table information.

Format show ip arp static

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
VRF-ID	The VRF ID to which the IP address belongs.
VRF-Name	The VRF name for the VRF ID.
IP address	The IP address of a device on a subnet attached to an existing routing interface.
MAC address	The MAC address for that device.

6.1.2. Configuraton commands

6.1.2.1. arp

This command creates an ARP entry. The value for <ipaddress> is the IP address of a device on a subnet attached to an existing routing interface. The value for <macaddress> is a unicast MAC address for that device.

Format arp [vrf <vrf-name>] <ipaddr> <macaddr> [interface {<slot/port> | vlan <1-4093>}]

no arp <ipaddr> [interface {<slot/port> | vlan <1-4093>}]

Fields	Definition
vrf-name	The specified VRF in which the ARP entry is going to be created.
IP address	Is the IP address of a device on a subnet attached to an existing routing interface.
MAC address	Is a MAC address for that device. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example, 00:06:29:32:81:40.
no	This command deletes an ARP entry.

Default None

Mode Global Config

6.1.2.2. ip proxy-arp

This command enables proxy ARP on a router interface or range of interfaces. Without proxy ARP, a device only responses to an ARP request if the target IP address is an address configured on the interface where the ARP request arrived. With proxy ARP, the device may also response if the target IP address is reachable. The device only responses if all next hops in its route to the destination are through interfaces other than the interface that received the ARP request.

To disable proxy ARP on a router interface, use the **no** form of this command.

Format ip proxy-arp
no ip proxy-arp

Default Enable.

Mode Interface Config

6.1.2.3. ip local-proxy-arp

This command allows an interface to response to ARP request for IP address within the subnet and to forward traffic between hosts in the subnet.

To reset the local proxy ARP mode on the interface to the default value, use the **no** form of this command.

Format ip local-proxy-arp
no ip local-proxy-arp

Default Disable.

Mode Interface Config

6.1.2.4. arp cashesize

This command configures the maximum number of entries in the ARP cache. The ARP cache size value is platform dependency.

Format arp cachesize <1152-8192> or arp cachesize <1152-6144>
no arp cachesize

Fields	Definition
<1152-8192>	The range of cache size is 1152 to 8192 for the following platform • ipv4-routing data-center default • ipv4-routing dcvpn-data-center

	• dual-ipv4-and-ipv6 default • dual-ipv4-and-ipv6 alpm • dual-ipv4-and-ipv6 alpm-mpls-data-center • dual-ipv4-and-ipv6 data-center • dual-ipv4-and-ipv6 dcvpn-data-center • dual-ipv4-and-ipv6 mpls-data-center
<1152-6144>	The range of cache size is 1152 to 6144 for the following platform: • ipv4-routing default • ipv4-routing data-center plus
no	This command configures the default ARP cache size.

Default The default cache size is 8192 or 6144, which depends on the platform currently used.

Mode Global Config

6.1.2.5. arp dynamicrenew

This command enables ARP component to automatically renew ARP entries of type dynamic when they age out.

Format arp dynamicrenew
no arp dynamicrenew

Fields	Definition
no	This command disables ARP component from automatically renewing ARP entries of type dynamic when they age out.

Default Disable

Mode Global Config

6.1.2.6. arp resptime

This command configures the ARP request response timeout.

Format arp resptime <1-10>
no arp resptime

Fields	Definition
<1-10>	The range of default response time is 1 to 10 seconds.

no	This command configures the default response timeout time.

Default The default response time is 1.

Mode Global Config

6.1.2.7. arp retries

This command configures the ARP count of maximum request for retries.

Format arp retries <0-10>

no arp retries

Fields	Definition
<1-10>	The range of maximum request for retries is 0 to 10.
no	This command configures the default count of maximum request for retries.

Default The default value is 4.

Mode Global Config

6.1.2.8. arp timeout

This command configures the ARP entry ageout time.

Format arp timeout <15-21600>

no arp timeout

Fields	Definition
<15-21600>	Represents the IP ARP entry ageout time in seconds. The range is 15 to 21600 seconds.
no	This command configures the default ageout time for IP ARP entry.

Default The default value is 1200.

Mode Global Config

6.1.2.9. arp access-list

Use this command to create an ARP ACL

Format arp access-list <name>

no arp access-list <name>

Fields	Definition
<name>	Enter ARP access-list name <1-31> alphanumeric characters in length.
no	Use this command to delete a configured ARP ACL.

Default None

Mode Global Config

6.1.2.10. permit ip host mac host

Use this command to configure a rule for a valid IP address and MAC address combination used in ARP packet validation.

Format permit ip host <sender-ip> mac host <sender-mac>

no permit ip host <sender-ip> mac host <sender-mac>

Fields	Definition
<sender-ip>	Specifies IP address in the ARP ACL rule.
<sender-mac>	Specifies MAC address in the ARP ACL rule.
no	Use this command to delete a rule for a valid IP and MAC combination.

Default None

Mode ARP Access-list Config

6.1.2.11. clear ip arp-cache

This command causes all ARP entries of type dynamic to be removed form the ARP cache. If the [gateway] parameter is specified, the dynamic entries of type gateway are purged as well.

Format clear ip arp-cache [gateway | interface {<slot/port> | vlan <vlan-id>}]

Default None

Mode Privileged Exec

6.2. IP Routing Commands

6.2.1. Show commands

6.2.1.1. show ip brief

This command displays all the summary information of the IP.

Format show ip brief

Default None

Mode Privileged EXEC
User EXEC

Display Message

Fields	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 is enabled or disabled.
Maximum Next Hops	The maximum number of hops supported by this switch.
Maximum Routes	The maximum number of routes the packet can travel.
Maximum Static Routes	The maximum number of static routes supported by this switch.
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.

6.2.1.2. show ip interface port

This command displays all pertinent information about the IP interfaces.

Format show ip interface port <slot/port>

Default None

Mode Privileged EXEC

User EXEC

Display Message

Fields	Definition
Routing Interface Status	Determine the operational status of IPv4 routing Interface. The possible values are Up or Down.
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 “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.
Proxy ARP	Displays whether Proxy ARP is enabled or disabled on the system.
Local Proxy ARP	Displays whether Local Proxy ARP is enabled or disabled on the interface. 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.
Active State	An interface is considered active if it has link up, 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).
Interface Suppress Status	Displays whether the interface suppressed or not.
Interface Name	Displays the routing interface name.

6.2.1.3. show ip interface vlan

This command displays all pertinent information about the VLAN routing interfaces.

Format show ip interface vlan <1-4093>

Default None

Mode Privileged EXEC
User EXEC

Display Message

Fields	Definition
Routing Interface Status	Determine the operational status of IPv4 routing Interface. The possible values are Up or Down.
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 “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.
Proxy ARP	Displays whether Proxy ARP is enabled or disabled on the system.

Local Proxy ARP	Displays whether Local Proxy ARP is enabled or disabled on the interface. 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.
Active State	Displays whether an interface is active with its link up and 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).
Interface Suppress Status	Displays whether the interface suppressed or not.
Auto-State Mode	Displays the mode of the AutoState feature of the interface.
Interface Name	Displays the routing interface name.

6.2.1.4. show ip interface lookback

This command displays information about configured loopback interfaces.

Format show ip interface loopback <0-63>

Default None

Mode Privileged EXEC
User EXEC

Display Message

Fields	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:

Fields	Definition
Routing Interface Status	The operational status of IPv4 routing Interface. The possible values are Up or Down.
Primary IP Address	The primary IP address and subnet masks for the interface. This value appears only if you configure it.
Secondary IP Address(es)	One or more secondary IP addresses and subnet masks for the interface. This value appears only if you configure it.
Routing Mode	The administrative mode of router interface participation. The possible values are enable or disable. This value is configurable.
Interface Name	The routing interface name.

6.2.1.5. show ip interface brief

This command displays summary information about IP configuration settings for all ports in the router.

Format show ip interface brief

Default None

Mode Privileged EXEC
User EXEC

Display Message

Fields	Definition
Interface	Valid slot, and port number separated by forward slashes or VLAN routing interface.
State	Indicate the operational state of the routing interface.
IP Address	The IP address of the routing interface.
IP Mask	The IP mask of the routing interface.
Method	Is the way to get the IP Address. The possible value is “Manual”, “DHCP” or “None”.
Netdir Bcast	Indicates if IP forwards net-directed broadcasts on this interface. Possible values are Enable or Disable.
MultiCast Fwd	Indicates the multicast forwarding administrative mode on the interface. Possible values are Enable or Disable.

6.2.1.6. show ip route

This command displays the routing table. 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 **connected, bgp, ospf, static,** or **kernel**. Use the <all> parameter to display all routes including best and nonbest routes. If you do not use the <all> parameter, the command only displays the best route. If you use **static** as <protocol>, a **description** option can be used to show the description of the static route.

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}]

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
Route Codes	Displays the key for the routing protocol codes that might appear in the routing table output. 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, D - Database Route
State	Indicate the operational state of the routing interface.
IP Address	The IP address of the routing interface.
IP Mask	The IP mask of the routing interface.
Method	Is the way to get the IP Address. The possible value is “Manual”, “DHCP” or “None”.
Netdir Bcast	Indicates if IP forwards net-directed broadcasts on this interface. Possible values are Enable or Disable.

MultiCast Fwd	Indicates the multicast forwarding administrative mode on the interface. Possible values are Enable or Disable.

The command displays the routing tables in the following format:

Code IP-Address/Mask [Preference/Metric] via Next-Hop, Interface

Fields	Definition
Code	The codes for the routing protocols that created the routes.
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.
Interface	The outgoing router interface to use when forwarding traffic to the next destination.

6.2.1.7. show ip route bestroutes

This command displays router route table information for the best routes.

Format show ip route bestroutes

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
Total Number of Routes	The total number of routes.
Network Address	Is an IP route prefix for the destination.
Subnet Mask	Is a mask of the network and host portion of the IP address for the router interface.
Protocol	Tells which protocol added the specified route. The possibilities are: local, static, OSPF.

For each next hop:

Fields	Definition
Next Hop Intf	The outgoing router interface to use when forwarding traffic to the next destination.
Next Hop IP Address	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.

6.2.1.8. show ip route entry

This command displays the router route entry information.

Format show ip route entry <networkaddress>

Fields	Definition
<networkaddress>	Is a valid network address identifying the network on the specified interface.

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
Network Address	Is a valid network address identifying the network on the specified interface.
Subnet Mask	Is a mask of the network and host portion of the IP address for the attached network.
Protocol	Tells which protocol added the specified route. The possibilities are: local, static, OSPF.
Total Number of Routes	The total number of routes.

For each next hop:

Fields	Definition
Next Hop Intf	The outgoing router interface to use when forwarding traffic to the next destination.
Next Hop IP Address	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.
Metric	Specifies the metric for this route entry.

Pref	The preference value that is used for this route entry.

6.2.1.9. show ip route connected

This command displays directly connected routes.

Format show ip route [vrf <vrf-name>] connected

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
Route Codes	Displays the key for the routing protocol codes that might appear in the routing table output.

The command displays the routing tables in the following format:

Code IP-Address/Mask [Preference/Metric] via Next-Hop, Interface

Fields	Definition
Code	The codes for the routing protocols that created the routes.
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.
Interface	The outgoing router interface to use when forwarding traffic to the next destination.

6.2.1.10. show ip route ospf

This command displays Open Shortest Path First (OSPF) routes. The option **all** command displays all (best and non-best) routes.

Format show ip route [vrf <vrf-name>] ospf [all]

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
Route Codes	Displays the key for the routing protocol codes that might appear in the routing table output.

The command displays the routing tables in the following format:

```
Code        IP-Address/Mask      [Preference/Metric]       via Next-Hop,        Interface
```

Fields	Definition
Code	The codes for the routing protocols that created the routes.
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.
Interface	The outgoing router interface to use when forwarding traffic to the next destination.

6.2.1.11. show ip route static

This command displays Static Routes. The option **all** command displays all (best and non-best) routes.

Format show ip route [vrf <vrf-name>] static [all]

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
Route Codes	Displays the key for the routing protocol codes that might appear in the routing table output.

The command displays the routing tables in the following format:

Code IP-Address/Mask [Preference/Metric] via Next-Hop, Interface

Fields	Definition
Code	The codes for the routing protocols that created the routes.
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.
Interface	The outgoing router interface to use when forwarding traffic to the next destination.

6.2.1.12. show ip route ecmp-groups

This command displays all the 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 the next hops.The output lists the IPv4 address and the outgoing interface of each next hop in each group.

Format show ip route [vrf <vrf-name>] ecmp-groups

Default None

Mode Privileged EXEC

6.2.1.13. show ip route hw-failure

This command displays the routes that failed to be added to the hardware due to the hash errors or a table full condition.

Format show ip route hw-failure

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
Route Codes	Displays the key for the routing protocol codes that might appear in the routing table output.

The command displays the routing tables in the following format:

Code IP-Address/Mask [Preference/Metric] via Next-Hop, Interface

Fields	Definition
Code	The codes for the routing protocols that created the routes.
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.
Interface	The outgoing router interface to use when forwarding traffic to the next destination.

6.2.1.14. show ip route summary

This command displays the routing table summary. Use the optional **all** parameter to show the number of all routes, including best and non-best routes. To include only the number of best routes, do not use the optional parameter.

Format show ip route [vrf <vrf-name>] summary [all]

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
Connected Routes	The total number of connected routes in the routing table.
Static Routes	Total number of static routes in the routing table.
Kernel Routes	Total number of kernel routes in the routing table.
Unnumbered Peer Routes	Total number of unnumbered peer routes in the routing table.
BGP Routes	Total number of routes installed by 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.
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 after counters were last cleared.
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.
Leaked Routes	The number of leaked routes currently in the routing table. This leaked routes are the routes leaked into RTO from other VRF.
RFC5549 Routes - IPv4 with IPv6 nexthop	The number of RFC5549 routes currently in the routing table. This RFC5549 routes are advertising BGP IPv4 NLRI with an IPv6 Next Hop.
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 hop were on a local subnet. Note that static routes can fail to be added to the routing table at startup because ther 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.
Failed Kernel Route Adds	The number of kernel routes that failed to be added to the routing table because of a kernel error or a table full condition.

Hardware Failed Route Adds	The number of routes failed to be inserted into the hardware because of 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 the local routes can be installed when a routing interface is up.
Unique Next Hop (High)	The number of the distinct next hops used among all routes currently in the routing table. This number includes local interfaces for local routes and neighbors for indirect routes. The value in the parentheses indicates the highest count of unique next hops after 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 the parentheses indicates the highest count of next hop groups after counters were last cleared.
ECMP Groups (High)	The number of next hop groups with multiple next hops. The value in the parentheses indicates the highest count of next hop groups after counters were last cleared.
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 Hop	The current number of routes with specific number (n) of next hops.

6.2.1.15. clear ip route counters

This command resets the IPv4 routing table counters reported in the command “show ip route summary” to zero. This 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 [vrf <vrf-name>]

Default None

Mode Privileged EXEC

6.2.1.16. show ip route preferences

This command displays detailed information about the route preferences. Route preferences are used in determining the best route. Lower router preference values are preferred over higher router preference values.

Format show ip route [vrf <vrf-name>] preferences

Default None

Mode Privileged EXEC
User EXEC

Display Message

Fields	Definition
Local	This field displays the local route preference value.
Static	This field displays the static route preference value.
BGP External	This field displays the BGP external route preference value.
OSPF Intra	This field displays the OSPF intra route preference value.
OSPF Inter	This field displays the OSPF inter route preference value.
OSPF External	The OSPF External 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.

6.2.1.17. show ip stats

This command displays IP statistical information. Refer to RFC 1213 for more information about the fields that are displayed.

Format show ip stats [vrf <vrf-name>]

Default None

Mode Privileged EXEC

6.2.1.18. 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 protocols.

Format show routing heap summary

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
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.

6.2.1.19. show ip load-sharing

This command displays the currently configured IP ECMP load balancing mode.

Format show ip load-sharing

Mode Privileged EXEC

6.2.1.20. show bfd neighbors

This command displays the BFD adjacency list showing the active BFD neighbors. The parameter **details** provides additional details with the routing protocol BFD has registered.

Format show bfd neighbors [{details [{<ip-address> | <ipv6-address>}] | interface {<slot/port> | vlan <vlan-id>} [details]}]

Mode Privileged Exec

Display Message

Fields	Definition
Our IP address	The current IP address.
Neighbor IP address	The IP address of the active BFD neighbor.
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 release.
Minimum transmit interval	The minimum interval to use when transmitting BFD control packets.
Minimum receive interval	The minimum interval at which the system can receive 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.
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.
Tx Fail Count	The number of transmitted failed BFD packets.
Rx Count	The number of received BFD packets.
Drop Count	The number of dropped packets.
Echo Mode	Show whether the BFD echo mode is enabled or disabled.
Echo Tx Count	The number of transmitted BFD echo packets.
Echo Rx Count	The number of received BFD echo packets.

6.2.2. Configuration commands

6.2.2.1. routing

This command enables routing for an interface.

Format routing

no routing

Fields	Definition
no	Disable routing for an interface.

Default Disable

Mode Interface Config

6.2.2.2. ip routing

This command enables the IP Router Admin Mode for the master switch.

Format ip routing
no ip routing

Fields	Definition
no	Disable the IP Router Admin Mode for the master switch.

Default Disable

Mode Global Config

6.2.2.3. ip address

This command configures an IP address on an interface. The IP address may be a secondary IP address.

Format ip address <ipaddr> {<subnet-mask> | <prefix-lengh>} [secondary]
no ip address <ipaddr> <subnet-mask> [secondary]

Fields	Definition
<ipaddr>	IP address of the interface.
<subnet-mask>	Subnet mask of the interface.
<prefix-lengh>	Implements RFC 3021 via using the / notation of the subnet mask. This integer indicates the length of the subnet mask. Range is from 1 to 31.
[secondary]	It is a secondary IP address.
no	Delete an IP address from an interface.

Default None

Mode Interface Config

6.2.2.4. 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** command in interface configuration mode.

Format ip address dhcp [{restart | client-id}]

no ip address dhcp [client-id]

Fields	Definition
[restart]	To restart the DHCPv4 client to acquire an IP Address from DHCP server.
[client-id]	To send the DHCPv4 messages with the DHCP client identifier.
no	This command releases a leased address and disables DHCPv4 on an interface.

Default Disable

Mode Interface Config

6.2.2.5. ip default-gateway

This command manually configures a global default gateway address. Only one default gateway can be configured. If you invoke this commands several times, each command replaces the previous configuration.

Format ip default-gateway <ipaddr>

no ip default-gateway

Fields	Definition
<ipaddr>	A valid IPv4 address.
no	Remove the default gateway address from the configuration.

Default None

Mode Global Config

6.2.2.6. ip load-sharing

This command manually configures the IP ECMP load balancing mode.

Format ip load-sharing <1-6> {inner | outer}

no ip load-sharing

Fields	Definition
<1 - 6>	The load balancing or sharing mode for all ECMP 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.
no	Reset the load balancing or sharing mode to the defaulte mode, 6.

Default 6 inner

Mode Global Config

6.2.2.7. ip route

This command configures a static route. Use the optional *vrf* parameter to configure the static route in the specified virtual router instance.

Format ip route [vrf <vrf-name>] <networkaddr> <subnetmask> {<nexthopip> | Null0 | interface {<slot/port> | vlan <vlan-id>} [<nexthopip>]} [[<1-255 >] [description <description>]

no ip route <networkaddr> <subnetmask> [{{<nexthopip> [<1-255 > | description]} | {Null0 [<1-255 > | description]}}]

Fields	Definition
<vrf-name>	Specify the name of the VRF in which this static route is installed.
<networkaddr>	A valid IP address.

<subnetmask>	A valid subnet mask.
<nexthopip>	IP address of the next hop router.
<vlan-id>	The VLAN ID used for this interface. The range of the VLAN ID is from 1 to 4093.
<1-255>	The preference value of this route. The range is 1 to 255.
<description>	The description for the route.
Null0	Null interface.
no	Delete all next hops to a destination static route. If the optional <nextHopRtr> parameter is designated, the next hop is deleted and if the optional preference value is designated, the preference value of the static route is reset to its default value, 1.

Default None

Mode Global Config

6.2.2.8. ip route default

This command configures the default route. Use the optional *vrf* parameter to configure the static route in the specified virtual router instance.

Format ip route [vrf <vrf-name>] default <nexthopip> [1-255]

no ip route [vrf <vrf-name>] default [{<nexthopip> | <1-255>}]

Fields	Definition
vrf-name	Specify the name of the VRF in which this static route is installed.
<nexthopip>	IP address of the next hop router.
<1-255>	Precedence value of this route.

Default None

Mode Global Config

6.2.2.9. ip route distance

This command sets the default distance (preference) for static routes. Use the optional *vrf* parameter to configure the default distance (preference) for static routes in the specified virtual router instance.

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.

Format ip route [vrf <vrf-name>] distance <1-255>

no ip route [vrf <vrf-name>] distance

Fields	Definition
vrf-name	Specify the name of the VRF in which this static route is installed.
<1-255>	Default the Distance value of static routes. The range is 1 to 255.

Default The default preference value is 1

Mode Global Config

6.2.2.10. ip route static bfd

This command configures the BFD for static route. To remove the BFD for static route, use **no** form of this command.

The switch BFD supports single-hop mode and multiple-hop mode.

Depending on status of the BFD session, static routes are added to or removed from the IP routing table. When a BFD session with a specific next hop goes down, all the static routes with the same next hop will be removed from the IP routing table. Once the BFD session comes up, all the static routes with the same next hop will be added into the IP routing table.

Format ip route static bfd <next-hop-ip-addr> <src-ip-addr>

no ip route static bfd <nexthopip> <srcip>

Fields	Definition
<nexthopip>	IP address of the next hop router.
<srcip>	Local IP address of static route for BFD. This IP address must be one of the interface IP address.

Default None

Mode Global Config

6.2.2.11. ip route vrf static bfd

This command configures the BFD for static route with specific VRF. To remove the BFD for static route with specific VRF, use **no** form of this command.

Format ip route vrf <vrf-name> static bfd <next-hop-ip-addr> <src-ip-addr>

no ip route vrf <vrf-name> static bfd <nexthopip> <srcip>

Fields	Definition
<vrf-name>	VRF Name in which the the static route is configured
<nexthopip>	IP address of the next hop router.
<srcip>	Local IP address of static route for BFD.

Default None

Mode Global Config

6.2.2.12. 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.)

Format ip mtu <68-9394>

no ip mtu

Fields	Definition
<68-9394>	The IP MTU on a routing interface. The range is 68 bytes to the <Interface MTU value-18> bytes.

Default The default value is 1500.

Mode Interface Config

6.2.2.13. ip unnumbered gratuitous-arp accept

This command enables the configuration of static interface routes to the unnumbered peer dynamically on receiving gratuitous ARP.

Format ip unnumbered gratuitous-arp accept

no ip unnumbered gratuitous-arp accept

Fields	Definition
no	Disable interface route configuration on receiving gratuitous ARP.

Default Interface route installation for receiving gratuitous ARP is enabled by default.

Mode Interface Config

6.2.2.14. ip unnumbered loopback

This command identifies unnumbered interfaces and specifies the numbered interface providing the borrowed address.

Format ip unnumbered loopback <0-63>

no ip unnumbered

Fields	Definition
<0-63>	The loopback interface number. The loopback interface provides the borrowed address and cannot be unnumbered.
no	Removes the unnumbered configuration.

Default Interface are numbered by default.

Mode Interface Config

6.2.2.15. encapsulation

This command configures the link layer encapsulation type for the packet.

Format encapsulation {ethernet | snap}

Fields	Definition
ethernet	The link layer encapsulation type is ethernet.

snap	The link layer encapsulation type is SNAP.

Default The default value is ethernet.

Mode Interface Config

Restrictions Routed frames are always Ethernet encapsulated when a frame is routed to a VLAN.

6.2.2.16. fpti

Use this command to enable FPTI mode either globally (in Global Config mode) or for a specific interface (in Interface Config mode).

Format fpti

no fpti

Default Enabled

Mode Global Config

Interface Config

6.3. Open Shortest Path First (OSPF) Commands

6.3.1. Show commands

6.3.1.1. show ip ospf

This command displays information relevant to the OSPF router.

Format show ip ospf [vrf <vrf-name>]

Default None

Mode Privileged Exec

Display Message

Some of the information below displays only if you enable OSPF and configure certain features.

Fields	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 non-default 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 timers pacing flood command.
LSA Refresh Group Pacing Time	The size of the LSA refresh group window, in seconds. This is the value configured with the 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.
Prefix Suppression	Whether the prefix-suppression is enabled or disabled.
Maximum Paths	The maximum number of paths that OSPF can report for a given destination.
Maximum Routes	The number of maximum IPv4 routes in a VRF.
Default Metric	Default value for redistributed routes.
Stub Router Configuration	One of Always, Startup, or 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.
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	Show source protocol/routes that are being redistributed. Possible values are static, connected, or BGP.
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.
Number of Active Areas	The number of OSPF areas to which the router is attached on interfaces that are 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 learnt 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	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 re-originates its own router LSAs, setting the cost of all non-stub interfaces to infinity. To restore OSPF to normal operation, disable and re-enable OSPF. One of Active, Inactive.
Stub Router Reason	One of Configured, Startup, or Resource Limitation. This row is only listed if stub router is active.
Stub Router Startup Time Remaining	The remaining time, in seconds, until OSPF exists 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 the stub mode because of a resource limitation. 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.
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	Length of global flood list for LSAs with AS scope.
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.
NSF Helper Support	Whether this router is configured to act as a graceful restart helpful neighbor. Possible values are: Helper Support Always, Disabled, or Planned.
NSF Helper Strict LSA Checking	As a graceful restart helpful neighbor, whether to terminate the helper relationship if a topology change occurs during a neighbor's graceful restart.

6.3.1.2. show ip ospf abr

This command displays the internal OSPF routing table entries to Area Border Routers (ABR). This command takes no options.

Format show ip ospf abr [vrf <vrf-name>]

Default None

Mode Privileged EXEC

User EXEC

Display Message

Fields	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.

6.3.1.3. show ip ospf area

This command displays information about the area. The <areaid> identifies the OSPF area that is being displayed.

Format show ip ospf area <areaid> [vrf <vrf-name>]

Default None

Mode Privileged EXEC
User EXEC

Display Message

Fields	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 LSA's.
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 length of the area's LSA flood list.
Import Summary LSAs	Shows whether summary LSAs are inmported.
Stub Area Metric Value	The metric value of the stub area.

The following OSPF NSSA specific information displays only if the area is configured as an NSSA:

Fields	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.

6.3.1.4. show ip ospf asbr

This command displays the internal OSPF routing table entries to Autonomous System Boundary Routers (ASBR). This command takes no options.

Format show ip ospf asbr [vrf <vrf-name>]

Default None

Mode Privileged EXEC

User EXEC

Display Message

Fields	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.

6.3.1.5. show ip ospf database

This command displays information about the link state database when OSPF 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 optional parameters to specify the type of link state advertisements to display.

Format show ip ospf [<areaid>] database [vrf <vrf-name>] [{asbr-summary | external | network | nssa-external | opaque-area | opaque-as | opaque-link | router | summary}] [<lsid>] [{adv-router [<ipaddr>] | self-originate}]

Fields	Definition
vrf-name	Specify the virtual router for which to display information
adv-router	Display the LSAs that are restricted by the advertising router. To specify a router, enter the IP address of the router.
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.

Default None

Mode Privileged EXEC
User EXEC

Display Message

The information below is only displayed if OSPF is enabled.

Fields	Definition
Links 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.
Chksm	The total number LSA checksum.
Options	This is an integer. It indicates that the LSA receives special handling during routing calculations.
Rtr Opt	Options are valid for router links only.

6.3.1.6. 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

Default None

Mode Privileged EXEC
User EXEC

Display Message

Fields	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.
Opaque Link	Number of opaque link LSAs in the database.
Opaque Area	Number of opaque area LSAs in the database.
Type-5 Ext	Total number of Type-5 external LSAs in the database.
Self-Originated Type-5 Ext	Total number of self originated Type-5 external 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.

6.3.1.7. show ip ospf interface

This command displays the OSPF information for the specific interface.

Format show ip ospf interface {<slot/port> | loopback <loopback-id> | vlan <vlan-id>}

Default None

Mode Privileged EXEC
User EXEC

Display Message

Fields	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.
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.
Transit Delay	A number representing the OSPF Transit Delay 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.
Prefix Suppression	Displays whether prefix suppression is enabled, disabled, or not configured on the 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 if flood blocking is enabled or disabled.

The information below is displayed only if OSPF is enabled.

Fields	Definition
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.

6.3.1.8. show ip ospf interface brief

This command displays brief information for the IFO object or virtual interface tables.

Format show ip ospf interface brief [vrf <vrf-name>]

Default None

Mode Privileged EXEC
User EXEC

Display Messages

Fields	Definition
Interface	Valid slot and port number separated by a forward slash.
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.
Retransmit Delay Interval	A number representing the OSPF Transit Delay for the specified interface.
LSA Ack Interval	A number representing the OSPF LSA Acknowledgment Interval for the specified interface.

6.3.1.9. 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> | loopback <loopback-id> | vlan <vlan-id>}

Default None

Mode Privileged EXEC
User EXEC

Display Messages

Fields	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.
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.
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.
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.
No Neighbor at Source Address	The number of OSPF packets dropped because the sender is not an existing neighbor or the sender's address does not match the previously recorded IP address for that neighbor.
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.

6.3.1.10. show ip 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 <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 <vlan-id>}] [<ip-address>]

Default None

Mode Privileged EXEC

User EXEC

Display Message

If you do not specify an IP address, a table with the following columns displays for all neighbors. If you specify a interface, only the information for that interface displays:

Fields	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 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:

Fields	Definition
Interface	Valid slot and port number separated by a forward slash.
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 IDf the specified interface.

6.3.1.11. show ip ospf range

This command displays information about the area ranges for the specified <areaid>. The <areaid> identifies the OSPF area whose ranges are being displayed.

Format show ip ospf range <areaid> [vrf <vrf-name>]

Default None

Mode Privileged EXEC

User EXEC

Display Message

Fields	Definition
Prefix	The summary prefix.
Subnet Mask	The subnetwork mask of the summary prefix.
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**).

6.3.1.12. show ip ospf statistics

This command displays information about recent Shortest Path First (SPF) calculations. 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 table lists how long ago the SPF ran, how long the SPF took, and the reasons why the SPF was scheduled.

Format show ip ospf statistics [vrf <vrf-name>]

Default None

Mode Privileged EXEC

User EXEC

Display Message

Fields	Definition
Delta T	The time since the SPF ran last time. The time is in the format hh:mm:ss, giving the hours, minutes, and seconds.
Intra	The time taken to compute the intra-area routes, in milliseconds.
Summ	The time taken to compute the inter-area routes, in milliseconds.
Ext	The time taken to compute the external routes, in milliseconds.
SPF Total	The totat time to compute the routes, in milliseconds. The total may exceed the sume 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 routing table, named Routing Information Based (RIB). The time is in milliseconds.
Reason	The reason the SPF was scheduled. Reason codes are as follows: • R - a router LSA has changed • N - a network LSA has changed • SN - a type 3 network summary LSA has changed • SA - a type 4 ASBR summary LSA has changed • X - a type 5 or type 7 external LSA has changed

6.3.1.13. show ip 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 ip ospf stub table [vrf <vrf-name>]

Default None

Mode Privileged EXEC
User EXEC

Display Message

Fields	Definition
Area ID	A 32-bit identifier for the created stub area.
Type of Service	The type of service associated with the stub metric. 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.

6.3.1.14. show ip ospf traffic

This command displays the OSPFv2 packets, the LSA statistics, and the OSPFv2 message queue statistics. Packet statistics count packets and LSAs since OSPFv2 counters were cleared last time (using the command **clear ip ospf counters**).

Format show ip ospf traffic [vrf <vrf-name>]

Default None

Mode Privileged EXEC
User EXEC

Display Message

Fields	Definition
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.
LS Update Max Recieve 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.

6.3.1.15. show ip 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 ip ospf virtual-link [vrf <vrf-name>] <areaid> <neighbor>

Default None

Mode Privileged EXEC
User EXEC

Display Message

Fields	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.

Transmit Delay Interval	The configured transit 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.
Metric	The OSPF virtual interface metric.
Neighbor State	The neighbor state.

6.3.1.16. 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 [vrf <vrf-name>] brief

Default None

Mode Privileged EXEC
User EXEC

Display Message

Fields	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.
Transit Delay	The configured transit delay for the OSPF virtual interface.

6.3.1.17. show ip ospf lsa-group

This command displays the number of self-originated LSAs within each LSA group.

Format show ip ospf lsa-group [vrf vrf-name]

Default None

Mode Privileged EXEC

User EXEC

Display Message

Fields	Definition
Total self-originated LSAs	The number of LSAs originated from self.
Average LSAs per group	The average number of self-originated LSAs per group.
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.
Number of self-originated LSAs within each LSA group	The detail number of self-originated LSAs.
Group Start Age	The start time of LSA Group aged.
Group End Age	The end time of LSA Group aged.
Count	The number of LSA Group aged.

6.3.2. Configuration commands

6.3.2.1. router ospf

Use this command to enter Router OSPF mode.

Format router ospf [vrf]

Fields	Definition
<vrf-name>	The virtual router on which to enable OSPF routing

Default None

Mode Global Config

6.3.2.2. enable

Use **enable** command resets the default administrative mode of OSPF in the router (active). **no enable** command sets the administrative mode of OSPF in the router to inactive.

Format enable

no enable

Default Enabled

Mode Router OSPF Config

6.3.2.3. network area

Use **network area** 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. Use **no network area** command to disable the OSPFv2 on a interface if the IP address of an interface was earlier covered by this network command.

Format network <ip-address> <wildcard-mask> area <area-id>

no network <ip-address> <wildcard-mask> area <area-id>

Default Disabled

Mode Router OSPF Config

6.3.2.4. ip ospf area

Use **ip ospf area** command to enable OSPFv2 and set the area ID of an interface. 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. Use **no ip ospf area** command to disable OSPF on an interface.

Format ip ospf area <area-id> [secondaries none]

no ip ospf area [secondaries none]

Default Disable

Mode Interface Config

6.3.2.5. 1583compatibility

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. **1583compatibility** command enables OSPF 1583 compatibility. **no 1583compatibility** command disables OSPF 1583 compatibility.

Format 1583compatibility

no 1583compatibility

Default Enable

Mode Router OSPF Config

6.3.2.6. area default-cost

This command configures the default cost for the stub area. You must specify the area ID and an integer value between 1-16777214.

Format area <areaid> default-cost <1-16777214>

Default None

Mode Router OSPF Config

6.3.2.7. area nssa

area nssa command configures the specified areaid to function as an NSSA. **no area nssa** command disables nssa from the specified area id.

Format area <areaid> nssa

no area <areaid> nssa

Default None

Mode Router OSPF Config

6.3.2.8. area nssa default-into-originate

area nssa default-info-originate 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). This command disables the default route advertised into the NSSA . **no area nssa default-info-originate** command disables the default route advertised into the NSSA.

Format area <areaid> nssa default-info-originate [<metric>] [{comparable | noncomparable}]

no area <areaid> nssa default-info-originate [<metric>] [{comparable | noncomparable}]

Default None

Mode Router OSPF Config

6.3.2.9. area nssa no-redistribute

area nssa no-redistribute command configures the NSSA Area Border router (ABR) so that learned external routes will not be redistributed to the NSSA. **no area nssa no-redistribute** command disables the NSSA ABR so that learned external routes are redistributed to the NSSA.

Format area <areaid> nssa no-redistribute

no area <areaid> nssa no-redistribute

Default None

Mode Router OSPF Config

6.3.2.10. area nssa no-summary

area nssa no-summary command configures the NSSA so that summary LSAs are not advertised into the NSSA. **no area nssa no-summary** command disables nssa from the summary LSAs.

Format area <areaid> nssa no-summary

no area <areaid> nssa no-summary

Default None

Mode Router OSPF Config

6.3.2.11. area nssa translator-role

area nssa translator-role 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. **no area nssa translator-role** command disables the nssa translator role from the specified area id.

Format area <areaid> nssa translator-role {always | candidate}

no area <areaid> nssa translator-role {always | candidate}

Default None

Mode Router OSPF Config

6.3.2.12. area nssa translator-stab-intv

area nssa translator-stab-intv 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. The **no area nssa translator-stab-intv** command disables the nssa translator's *<stabilityinterval>* from the specified area id. The <stabilityinterval> range is fomr 0 to 3600.

Format area <areaid> nssa translator-stab-intv <stabilityinterval>

no area <areaid> nssa translator-stab-intv <stabilityinterval>

Default None

Mode Router OSPF Config

6.3.2.13. area range

area range command configures a summary prefix that an area border router (ABR) advertises for a specified area.

Format area <areaid> range <ipaddr> <subnetmask> {summarylink | nssaexternallink} [advertise [cost <0-16777215>] | not-advertise | [cost <0-16777215>]]

no area <areaid> range <ipaddr> <subnetmask> {summarylink | nssaexternallink} [advertise | not-advertise | cost]

Fields	Definition
areaid	The aread identifier for the area whose networks are to be summarized.
ipaddr subnetmas	The summary prefix to be advised when the ABR computes a route to one or more networks within this prefixe in this area.
summarylink	When this keyword is configured, the area range is used when summarizing prefixes advertised in type 3 summary LSAs.
nssaexternallink	When this keyword is configured, the area range is used when translating type 7 LSAs to type 5 LSAs.
advertise	When this keyword is configured, the summary prefix is advertised when the area range is active. This is the default action.
not-advertise	When this keyword is configured, neither the summary prefix nor the contained prefixes are advertised when the are range is active. When this not-advertise option is given, any static cost previously configured is removed from the system configuration.
cost	When this cost is configured, 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. If the cost is set to 16777215 for type 3 summarization, a type 3 summary LSA is not advertised but contained network 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 16777215; however, other routers will not compute a route from a type 5 LSA with this metric.

Default None

Mode Router OSPF Config

6.3.2.14. area stub

area stub 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. **no area stub** command deletes a stub area for the specified area ID.

Format area <areaid> stub

no area <areaid> stub

Default None

Mode Router OSPF Config

6.3.2.15. area stub no-summary

area stub no-summary command configures the Summary LSA mode for the stub area identified by *<areaid>*. Use this command to prevent LSA Summaries from being sent. **no area stub no-summary** command configures the default Summary LSA mode for the stub area identified by *<areaid>*.

Format area <areaid> stub no-summary

no area <areaid> stub no-summary

Default Disable

Mode Router OSPF Config

6.3.2.16. area virtual-link

area virtual-link command creates the OSPF virtual interface for the specified *<areaid>* and *<neighbor>*. The *<neighbor>* parameter is the Router ID of the neighbor. **no area virtual-link** 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 area <areaid> virtual-link <neighbor>

no area <areaid> virtual-link <neighbor>

Default None

Mode Router OSPF Config

6.3.2.17. area virtual-link authentication

The **area virtual-link authentication** command configures the authentication type and key for the OSPF virtual interface identified by *<areaid>* and *<neighbor>* parameters. 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 can be configured with plain-text up to 16 characters or configured in encrypted form with option 7. 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 is configured.

The **no area virtual-link authentication** command configures the default authentication type for the OSPF virtual interface identified by *<areaid>* and *<neighbor>* parameters. The *<neighbor>* parameter is the Router ID of the neighbor.

Format area <areaid> virtual-link <neighbor> authentication {none | {simple <key>} | {encrypt [7 <keyid>]}}

no area <areaid> virtual-link <neighbor> authentication

Fields	Definition
encrypt	7 specifies the key in encrypted form. The key must be in hexadeicmal digits with a length of 32 characters.

Default None

Mode Router OSPF Config

6.3.2.18. area virtual-link dead-interval

area virtual-link dead-interval 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. **no area virtual-link dead-interval** 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 area <areaid> virtual-link <neighbor> dead-interval <seconds>

no area <areaid> virtual-link <neighbor> dead-interval

Default 40

Mode Router OSPF Config

6.3.2.19. area virtual-link hello-interval

area virtual-link hello-interval 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. **no area virtual-link hello-interval** 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 area <areaid> virtual-link <neighbor> hello-interval <seconds>

no area <areaid> virtual-link <neighbor> hello-interval

Default 10

Mode Router OSPF Config

6.3.2.20. area virtual-link retransmit-interval

area virtual-link retransmit-interval 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. **no area virtual-link retransmit -interval** 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 area <areaid> virtual-link <neighbor> retransmit-interval <seconds>

no area <areaid> virtual-link <neighbor> retransmit-interval

Default 5

Mode Router OSPF Config

6.3.2.21. area virtual-link transmit-delay

area virtual-link transmit-delay 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). **no area virtual-link transmit-delay** command resets the default transmit delay for the OSPF virtual interface to the default value.

Format area <areaid> virtual-link <neighbor> transmit-delay <seconds>

no area <areaid> virtual-link <neighbor> transmit-delay

Default 1

Mode Router OSPF Config

6.3.2.22. auto-cost reference-bandwidth

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. The different reference bandwidth can be independently configured for OSPFv2 and OSPFv3.

Use the **no auto-cost** command to set the reference bandwidth to the default value.

Format auto-cost reference-bandwidth <1 to 4294967>

no auto-cost reference-bandwidth

Default 100Mbps

Mode Router OSPF Config

6.3.2.23. bfd

This command configures BFD for all interfaces.

To reset BFD for interfaces to default, use the no form of this command.

Format bfd

no bfd

Default Disable

Mode Router OSPFv2 Config

6.3.2.24. capability opaque

Use **capability opaque** 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. Supports the storing and flooding of Opaque LSAs of different scopes. Use **no capability opaque** command to disable opaque capability on the router.

Format capability opaque

no capability opaque

Default Disable

Mode Router OSPF Config

6.3.2.25. clear ip ospf

Use this command to disable and re-enable OSPF.

Format clear ip ospf [vrf <vrf-name>]

Fields	Definition
<vrf-name>	The virtual rotuer on which the OSPF is disabled and re-enabled.

Default None

Mode Privileged Exec

6.3.2.26. clear ip ospf configuration

Use this command to reset the OSPF configuration to factory defaults.

Format clear ip ospf configuration [vrf <vrf-name>]

Fields	Definition
<vrf-name>	The virtual rotuer on which the OSPF is reset.

Default None

Mode Privileged Exec

6.3.2.27. clear ip ospf counters

Use this command to reset global and interface statistics.

Format clear ip ospf counters [vrf <vrf-name>]

Fields	Definition
<vrf-name>	The virtual rotuer on which the statistics of OSPF is reset

Default None

Mode Privileged Exec

6.3.2.28. clear ip 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 re-established. To drop all adjacencies with a specific router ID, specify the neighbor's Router ID using the optional parameter [ipaddr].

Format clear ip ospf neighbor [[vrf <vrf-name>] | <ipaddr>]

Fields	Definition
<neighbor-idipaddr>	The neighbor's Router IDIP address.
<vrf-name>	The virtual rotuer on which the adjacency with OSPF neighbors are dropped.

Default None

Mode Privileged Exec

6.3.2.29. 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 [ipaddr].

Format clear ip ospf neighbor [vrf <vrf-name> | interface {<slot/port> | vlan <vlan-id>} | <ipaddr>]

Fields	Definition
<vrf-name>	The virtual rotuer on which the adjacency with OSPF neighbors are dropped.

Default None

Mode Privileged Exec

6.3.2.30. clear ip ospf redistribution

Use this command to flush all self-originated external LSAs. Reapply the redistribution configuration and re-originate prefixes as necessary.

Format clear ip ospf redistribution [vrf <vrf-name>]

Fields	Definition
<vrf-name>	The virtual rotuer on which the adjacency with OSPF neighbors are dropped.

Default None

Mode Privileged Exec

6.3.2.31. clear ip ospf stub-router

Use this command to exit the stub router mode.

Format clear ip ospf stub-router [vrf <vrf-name>]

Fields	Definition
<vrf-name>	The virtual rotuer on which the OSPF exits stub router mode.

Default None

Mode Privileged Exec

6.3.2.32. default-information originate

default-information originate command is used to control the advertisement of default routes.

no default-information originate command is used to control the advertisement of default routes.

Format default-information originate [always] [metric <1-16777214>] [metric-type {1 | 2}]
no default-information originate [metric] [metric-type]

Default metric—unspecified
type—2

Mode Router OSPF Config

6.3.2.33. default-metric

default-metric command is used to set a default for the metric of distributed routes.

no default-metric command is used to set a default for the metric of distributed routes.

Format default-metric <1-16777214>
no default-metric

Default None

Mode Router OSPF Config

6.3.2.34. distance ospf

distance ospf 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. **no distance ospf** 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 distance ospf {intra-area <1-255> | inter-area <1-255> | external <1-255>}

no distance ospf {intra-area | inter-area | external}

Default 110

Mode Router OSPF Config

6.3.2.35. distribute-list out

Use **distribute-list out** command to specify the access list to filter routes received from the source protocol.

no distribute-list out command to specify the access list to filter routes received from the source protocol.

Format distribute-list <1-199> out {bgp | static | connected}

no distribute-list <1-199> out {bgp | static | connected}

Default None

Mode Router OSPF Config

6.3.2.36. exit-overflow-interval

exit-overflow-interval 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. **no exit-overflow-interval** command configures the default exit overflow interval for OSPF.

Format exit-overflow-interval <seconds>

no exit-overflow-interval

Default 0

Mode Router OSPF Config

6.3.2.37. external-lsdb-limit

external-lsdb-limit 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. **no external-lsdb-limit** command configures the default external LSDB limit for OSPF.

Format external-lsdb-limit <limit>

no external-lsdb-limit

Fields	Definition
<limit>	The range for limit is -1 to 2147483647. If the value is -1, then there is no limitation.

Default -1

Mode Router OSPF Config

6.3.2.38. ip ospf authentication

The **ip ospf authentication** command sets the OSPF authentication type and key for the specified interface. 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 can be configured with plain-text up to 16 characters or configured in encrypted form with option 7. 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. A default value for this command does nto exist.

The **no ip ospf authentication** command sets the default OSPF authentication type for the specified interface.

Format ip ospf authentication {none | {simple <key>} | {encrypt [7 <keyid>]}}

no ip ospf authentication

Fields	Definition
encrypt	7 specifies the key in encrypted form. The key must be in hexadeicmal digits with a length of 32 characters.

Default None

Mode Interface Config

6.3.2.39. ip ospf cost

ip ospf cost command configures the cost on an OSPF interface. The <cost> parameter has a range of 1 to 65535. **no ip ospf cost** command configures the default cost on an OSPF interface.

Format ip ospf cost <1–65535>

no ip ospf cost

Default 10

Mode Interface Config

6.3.2.40. ip ospf dead-interval

ip ospf dead-interval command sets the OSPF dead interval for the specified interface. 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. **no ip ospf dead-interval** command sets the default OSPF dead interval for the specified interface.

Format ip ospf dead-interval <seconds>

no ip ospf dead-interval

Default 40

Mode Interface Config

6.3.2.41. ip ospf hello-interval

ip ospf hello-interval 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 range from 1 to 65535. **no ip ospf hello-interval** command sets the default OSPF hello interval for the specified interface.

Format ip ospf hello-interval <seconds>

no ip ospf hello-interval

Default 10

Mode Interface Config

6.3.2.42. ip ospf network

ip ospf network command to configure OSPF to treat an interface 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..

no ip ospf network command to return the OSPF network type to the default.

Format ip ospf network {broadcast|point-to-point}

no ip ospf network

Default Broadcast

Mode Interface Config

6.3.2.43. ip ospf prefix-suppression

ip ospf prefix-suppression 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 to exclude specific interfaces from performing prefix-suppression when the featue is enabled globally.

no ip ospf prefix-suppression command removes prefix-suppression configurations at the interface level. When **no ip ospf prefix-suppression** is issued, global prefix-suppression configuration applies to the interface.

Format ip ospf prefix-suppression [disable]

no ip ospf prefix-suppression

Default Prefix-suppression is not configured

Mode Interface Config

6.3.2.44. ip ospf priority

ip ospf priority command sets the OSPF priority for the specified router interface. 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. **no ip ospf priority** command sets the default OSPF priority for the specified router interface.

Format ip ospf priority <0-255>

no ip ospf priority

Default 1, which is the highest router priority

Mode Interface Config

6.3.2.45. ip ospf retransmit-interval

ip ospf retransmit command sets the OSPF retransmit Interval for the specified interface. 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). **no ip ospf retransmit** command sets the default OSPF retransmit Interval for the specified interface.

Format ip ospf retransmit-interval <0-3600>

no ip ospf retransmit-interval

Default 5

Mode Interface Config

6.3.2.46. ip ospf transmit-delay

ip ospf transmit-delay command sets the OSPF Transit Delay for the specified interface. 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). **no ip ospf transmit-delay** command sets the default OSPF Transit Delay for the specified interface.

Format ip ospf transmit-delay <1-3600>>

no ip ospf transmit-delay

Default 1

Mode Interface Config

6.3.2.47. ip ospf mtu-ignore

ip ospf mtu-ignore command disables OSPF maximum transmission unit (MTU) mismatch detection. 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. **no ip ospf mtu-ignore** command enables the OSPF MTU mismatch detection.

Format ip ospf mtu-ignore

no ip ospf mtu-ignore

Default Enabled

Mode Interface Config

6.3.2.48. ip ospf bfd

This command enables BFD for OSPFv2 on the specified interface.

To disable BFD for OSPFv2 on the specified interface, use the no form of this command.

Format ip ospf bfd

no ip ospf bfd

Default Disabled

Mode Interface Config

6.3.2.49. router-id

router-id command sets a 4-digit dotted-decimal number uniquely identifying the router ospf id. The <ipaddress> is a configured value.

Format router-id <ipaddress>

Default None

Mode Router OSPF Config

6.3.2.50. redistribute

redistribute command configures OSPF protocol to allow redistribution of routes from the specified source protocol/routers. **no redistribute** command configures OSPF protocol to prohibit redistribution of routes from the specified source protocol/routers.

Format redistribute {bgp | static | connected} [metric <0-16777214>] [metric-type {1 | 2}] [tag <0-4294967295>] [subnets]

no redistribute {bgp | static | connected} [metric] [metric-type] [tag] [subnets]

Default metric—unspecified

type—2

tag—0

Mode Router OSPF Config

6.3.2.51. maximum-paths

maximum-paths command sets the number of paths that OSPF can report for a given destination where maxpaths is platform dependent. **no maximum-paths** command resets the number of paths that OSPF can report for a given destination back to its default value. The < maxpaths> range is 1 to 48.

Format maximum-paths <maxpaths>

no maximum-paths

Default 4

Mode Router OSPF Config

6.3.2.52. passive-interface default

passive-interface default 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. **no passive-interface default** 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 passive-interface default

no passive-interface default

Default Disabled

Mode Router OSPF Config

6.3.2.53. passive-interface

passive-interface command to set the interface or tunnel as passive. It overrides the global passive mode that is currently effective on the interface or tunnel. **no passive-interface** 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 passive-interface {<slot/port> | vlan <vlan-id>}

no passive-interface {<slot/port> | vlan <vlan-id>}

Default Disabled

Mode Router OSPF Config

6.3.2.54. timers spf

Use this command to configure the SPF delay time and hold time. The valid range for both parameters is 0-65535 seconds.

Format timers spf <delay-time> <hold-time>

Default delay-time—5

hold-time—10

Mode Router OSPF Config

6.3.2.55. max-metric

Use **max-metric** command to configure OSPF to enable stub router mode. Use **no max-metric** command to disable stub router mode.

If you configure the summary LSA metric to 16,777,215, other routers will skip the summary LSA when they compute routes.

Format max-metric router-lsa [on-startup <seconds> [summary-lsa [<metric>]] | summary-lsa [<metric> [on-startup <seconds>]]

no max-metric router-lsa [on-startup] [summary-lsa]

Fields	Definition
on-startup	OSPF starts in stub router mode after a reboot.
seconds	The number of seconds that OSPF remains in stub router mode after a reboot. The range is from 5 to 86,400 seconds. There is no default value.
summary-lsa	Set the metric in type 3 and 4 summary LSAs to LsInfinity (0xFFFFFF).
metric	Metric to send in summary LSAs when in stub router mode. Range is 1 to 16,777,215. Default is 16,711,680(0xFF0000).

Default None

Mode Router OSPF Config

6.3.2.56. log-adjacency-changes

log-adjacency-changes command logs OSPFv2 neighbor state changes. **no log-adjacency-changes** command disables logging OSPFv2 neighbor state changes.

Format log-adjacency-changes [detail]

no log-adjacency-change

Fields	Definition
detail	Log all messages for each adjacency state change, not just when transitions to FULL state and when a backwards transition occur.

Default Disabled

Mode Router OSPF Config Mode

6.3.2.57. prefix-suppression

Use **max-metric** command to suppress 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 command *ip ospf prefix-suppresion* in interface config mode. Prefixes associated with secondary IPv4 addresses can never be suppressed.

no prefix-suppression command disables prefix-suppression. No prefixes are suppressed from being advertised.

Format prefix-suppression

no prefix-suppression

Default Disabled

Mode Router OSPF Config Mode

6.3.2.58. nsf helper

Use this command to enable helper neighbor functionality for the OSPF graceful restart on an interface.

Use the no form of the command to disable helper neighbor functionality for the OSPF graceful restart.

Format nsf [ietf] [helper]

no nsf [ietf] [helper]

Fields	Definition
ieft	This keyword is accepted but not required.

Default Disabled

Mode Router OSPF Config Mode

6.3.2.59. nsf helper strict-lsa-checking

Use this command to require that an OSPF helper neighbor exit helper mode whenever a topology change occurs.

Use the no form of the command to allow OSPF to continue as a helpful neighbor in spite of topology changes.

Format nsf {[ietf] [helper] [strict-lsa-checking] | [helper] [strict-lsa-checking]}

no nsf {[ietf] [helper] [strict-lsa-checking] | [helper] [strict-lsa-checking]}

Fields	Definition
ieft	This keyword is accepted but not required.

strict-lsa-checking	Specify that an OSPF helper exits helper mode whenever a topology change occurs. OSPF continues as a helpful neighbor in spite of topology changes if this option is not set.

Default Enabled

Mode Router OSPF Config Mode

6.3.2.60. 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.

Format bandwidth <1-10000000>

no bandwidth

Default actual interface bandwith

Mode Interface Config

6.4. BOOTP/DHCP Relay Commands

6.4.1. Show commands

6.4.1.1. show bootpdhcprelay

This command displays the BootP/DHCP Relay information.

Format show bootpdhcprelay [vrf <vrf-name>]

Default None

Mode Privileged EXEC
User EXEC

Display Message

Fields	Definition
Maximum Hop Count	Is the maximum allowable relay agent hops.
Minimum Wait Time (Seconds)	Is the minimum wait time.
Admin Mode	Represents whether relaying of requests is enabled or disabled.
Circuit ID Option Mode	Is the DHCP circuit ID option which may be enabled or disabled.

6.4.2. Configuration commands

6.4.2.1. bootpdhcprelay cidoptmode

This command enables the circuit ID option mode for BootP/DHCP Relay on the system.

To disable the circuit ID option mode for BootP/DHCP Relay on the system, use the **no** form of this command.

Format bootpdhcprelay cidoptmode
no bootpdhcprelay cidoptmode

Default Disabled

Mode Global Config

6.4.2.2. bootpdhcprelay maxhopcount

This command configures the maximum allowable relay agent hops for BootP/DHCP Relay on the system.

To reset the maximum allowable relay agent hops for BootP/DHCP Relay on the system to 4, use the **no** form of this command.

Format bootpdhcprelay maxhopcount <hops>

no bootpdhcprelay maxhopcount

Parameter	Description
hops	The range of maximum hop count is 1 to 16.

Default 4

Mode Global Config

6.4.2.3. 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.

To reset the minimum wait time in seconds for BootP/DHCP Relay on the system to 0, use the **no** form of this command.

Format bootpdhcprelay minwaittime <minwaittime>

no bootpdhcprelay minwaittime

Parameter	Description
minwaittime	The range of minimum wait time is 0 to 100.

Default 0

Mode Global Config

6.5. IP Helper Commands

6.5.1. Show commands

6.5.1.1. show ip helper-address

Use this command to display the IP helper address configuration.

Format show ip helper-address [vrf <vrf-name>] [{<slot/port> | vlan <1 - 4093>}]

Default None

Mode Privileged EXEC
User EXEC

Display Message

Fields	Definition
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.
Discard	Indicate discard the UDP packets or not.
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.

6.5.1.2. show ip helper statistics

Use this command to display the number of UDP packets processed and relayed.

Format show ip helper statistics [vrf <vrf-name>]

Default None

Mode Privileged EXEC
User EXEC

Display Message

Fields	Definition
DHCP client messages received	The number of valid messages received form a DHCP client.

DHCP client messages relayed	The number of DHCP client messages relayed to a server .
DHCP server messages received	The number of DHCP responses received from the server .
DHCP server messages relayed	The number of DHCP server messages relayed to a client.
UDP client messages received	The number of valid UDP messages received.
UDP client messages relayed	The number of valid UDP messages relayed.
DHCP messages hop count exceeded max	The number of DHCP client messages received whose hop count is larger than the maximum allowed.
DHCP messages with secs field below min	The number of DHCP client messages received whose Second field is less than the minimum value.
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 address.
Packets with expired TTL	The number of packets received with TTL of 0 or 1 that otherwise have been relayed.
Packets that matched a discard entry	The number of packets ignored by the relay agent because they match a discard entry.

6.5.2. Configuration commands

6.5.2.1. 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.

To delete the address, use the **no** form of this command.

Format ip helper-address <ipaddr> [<udp-port> | dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]

no ip helper-address [<ipaddr> [<udp-port> | dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]]

Parameter	Description
ipaddr	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.
udp-port	A destination UDP port number from 1 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) • rip (port 520) • tacacs (port 49) • tftp (port 69) • time (port 37) Other ports must be specified by number.

Default None

Mode Global Config

6.5.2.2. 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.

To delete the address, use the **no** form of this command.

Format ip helper-address <ipaddr> [<udp-port> | dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]

no ip helper-address [<ipaddr> [<udp-port> | dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]]

Parameter	Description
ipaddr	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.
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) • rip (port 520) • tacacs (port 49) • tftp (port 69) • time (port 37) Other ports must be specified by number.

Default None

Mode Interface Config

6.5.2.3. ip helper-address discard

Use this command to configure the discard 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 for a given port number or to specify multiple port numbers handled by a specific server.

To delete the address, use the **no** form of this command.

Format ip helper-address discard [<udp-port> | dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]

no ip helper-address discard [<udp-port> | dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]

Parameter	Description
udp-port	A destination UDP port number from 1 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) • rip (port 520)

- tacacs (port 49)
- tftp (port 69)
- time (port 37)

Other ports must be specified by number.

Default None

Mode Interface Config

6.5.2.4. ip helper enable

This command enables the relay of UDP packets.

To disable the replay of UDP packets, use the **no** form of this command.

Format ip helper enable

no ip helper enable

Default Disabled

Mode Global Config

6.5.2.5. clear ip helper statistics

Use this command to clear the statistics data of UDP packets processed and relayed by IP helper.

Format clear ip helper statistics [vrf <vrf-name>]

Default None

Mode Privileged Exec

User Exec

6.6. Router Discovery Protocol Commands

6.6.1. Show commands

6.6.1.1. show ip irdp

This command displays the router discovery information for all interfaces, or a specified interface.

Format show ip irdp {<slot/port> | all | vlan <vlan-id>}

Fields	Definition
All	Show router discovery information for all interfaces.

Default None

Mode Privileged Exec
User Exec

Display Message

Fields	Definition
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.
Discard	Indicate discard the UDP packets or not.
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.

6.7. VLAN Routing Commands

6.7.1. Configuration commands

6.7.1.1. interface vlan

This command creates a VLAN routing interface.

To delete a VLAN routing interface, use the **no** form of this command.

Format interface vlan <vlan-id>

no interface vlan <vlan-id>

Fields	Definition
<vlan-id>	The VLAN ID used for this interface. The range of VLAN ID is from 1 to 4093.

Default None

Mode Global Config

6.8. Virtual Router Redundancy Protocol (VRRP) Commands

6.8.1. Show commands

6.8.1.1. show ip vrrp

This command displays whether VRRP functionality is enabled or disabled. It also displays some global parameters which are required for monitoring.

Format show ip vrrp

Default None

Mode Privileged Exec
User Exec

Display Message

Fields	Definition
Admin Mode	Displays the administrative mode for VRRP functionality on the switch.
Active-Active Mode	Displays the Active-Active mode for VRRP functionality on the switch.
Router Checksum Errors	Represents the total number of VRRP packets received with an invalid VRRP checksum value.
Router Version Errors	Represents the total number of VRRP packets received with Unknown or unsupported version number.
Router VRID Errors	Represents the total number of VRRP packets received with invalid VRID for this virtual router.

6.8.1.2. show ip vrrp brief

This command displays information about each virtual router configured on the switch.

Format show ip vrrp brief

Default None

Mode Privileged Exec
User Exec

Display Message

Fields	**Definition**
Interface	Valid slot and port number separated by forward slashes.

VRID	Represents the router ID of the virtual router.
IP Address	Is the IP Address that was configured on the virtual router.
Mode	Represents whether the virtual router is enabled or disabled.
State	Represents the state (Master/backup) of the virtual router.

6.8.1.3. show ip vrrp interface

This command displays all configuration information of a virtual router configured on a specific interface. Note that the information will be displayed only when the IP address of the specific interface is configured.

Format show ip vrrp interface {<slot/port> | vlan <vlan-id>} [<vrid>]

Fields	Definition
<slot/port>	Valid slot and port number separated by forward slashes.
<vrid>	Represents the router ID of the virtual router.
<vlan-id>	VLAN ID. The range of VLAN ID is 1 to 4093.

Default None

Mode Privileged Exec
User Exec

Display Message

Fields	Definition
VRID	Represents the router ID of the virtual router.
Primary IP Address	This field represents the configured IP Address for the Virtual router.
VMAC address	Represents the VMAC address of the specified router.
Authentication type	Represents the authentication type for the specific virtual router.
Priority	Represents the priority value for the specific virtual router.
Configured Priority	The priority configured through the ip vrrp vrid priority 1-254 command.
Advertisement interval	Represents the advertisement interval in seconds for the specific virtual router.
Pre-Empt Mode	Is the preemption mode configured on the specified virtual router.
Administrative Mode	Represents 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	Represents the state (Master/backup) of the specific virtual router.

6.8.1.4. 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>]

Fields	Definition
<slot/port>	Valid slot and port number separated by forward slashes.
<vrid>	Virtual router ID.
<vlan-id>	VLAN ID. The range of VLAN ID is 1 to 4093.

Default None

Mode Privileged Exec
User Exec

Display Message

Fields	Definition
VRID	Represents the router ID of the virtual router.
Uptime	Is the time that the virtual router has been up, in days, hours, minutes and seconds.
Protocol	Represents the protocol configured on the interface.
State Transitioned to Master	Represents the total number of times virtual router state has changed to MASTER.
Advertisement Received	Represents the total number of VRRP advertisements received by this virtual router.
Advertisement Interval Errors	Represents the total number of VRRP advertisements received for which advertisement interval is different than the configured value for this virtual router.
Authentication Failure	Represents the total number of VRRP packets received that don't pass the authentication check.

IP TTL errors	Represents 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	Represents the total number of VRRP packets received by virtual router with a priority of '0'.
Zero Priority Packets Sent	Represents the total number of VRRP packets sent by the virtual router with a priority of '0'.
Invalid Type Packets Received	Represents the total number of VRRP packets received by the virtual router with invalid 'type' field.
Address List Errors	Represents 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	Represents the total number of VRRP packets received with unknown authentication type.
Authentication Type Mismatch	Represents the total number of VRRP advertisements received for which 'auth type' not equal to locally configured one for this virtual router.
Packet Length Errors	Represents the total number of VRRP packets received with packet length less than length of VRRP header.
Advertisement Sent	Represents the total number of VRRP advertisement packets sent by the virtual router.

6.8.1.5. clear ip vrrp interface stat

This command clears IPv4 multicast route entries.

Format clear ip vrrp interface stat {<slot/port> <vrid> | vlan <1-4093> {<vrid>}}

Default None

Mode Privileged Exec

6.8.2. Configuration commands

6.8.2.1. ip vrrp

This command enables the administrative mode of VRRP in the router.

To disable the administrative mode of VRRP in the router, use the **no** form of this command.

Format ip vrrp

no ip vrrp

Default Disabled

Mode Global Config

6.8.2.2. ip vrrp master-backup

This command disables the active active mode of VRRP in the router.

To enable the active active mode of VRRP in the router, use the no form of this command.

Format ip vrrp master-backup

no ip vrrp master-backup

Default Disabled

Mode Global Config

6.8.2.3. ip vrrp <vrid>

This command sets the virtual router ID on an interface for Virtual Router configuration in the router.

To remove all VRRP configuration details of the virtual router configured on a specific interface, use the **no** form of this command.

Format ip vrrp <1-255>

no ip vrrp <1-255>

Fields	Definition
<1-255>	The range of virtual router ID is 1 to 255.

Default None

Mode Interface Config

6.8.2.4. ip vrrp ip

This command sets the primary or secondary IP address of the device within a VRRPv2 group.

If the secondary option is not specified, the specified IP address is set as the primary. Also the removing of the primary virtual IP 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.

To remove the secondary address, use the no form of this command.

Format ip vrrp <1-255> ip <addr> [secondary]

no ip vrrp <1-255> ip <addr> [secondary]

Fields	Definition
<1-255>	The range of virtual router ID is 1 to 255.
<addr>	Secondary IP address of the router ID.

Default None

Mode Interface Config

6.8.2.5. ip vrrp mode

This command enables the virtual router configured on the specified interface. Enabling the status field starts a virtual router. Disabling the status field stops a virtual router.

To disable the virtual router configured on the specified interface, use the **no** form of this command.

Format ip vrrp <1-255> mode

no ip vrrp <1-255> mode

Fields	Definition
<1-255>	The range of virtual router ID is 1 to 255.

Default Disabled

Mode Interface Config

6.8.2.6. 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.

To prevent the VRRP Master from accepting ping packets sent to one of the virtual router's IP addresses, use the **no** form of this command.

Format ip vrrp <1-255> accept-mode

no ip vrrp <1-255> accept-mode

Fields	Definition
<1-255>	The range of virtual router ID is 1 to 255.

Default Disabled

Mode Interface Config

6.8.2.7. ip vrrp authentication

This command sets the authorization details value for the virtual router configured on a specified interface.

To set the default authorization detailed value for the virtual router configured on a specified interface, use the **no** form of this command.

Format ip vrrp <1-255> authentication <key>

no ip vrrp <1-255> authentication

Fields	Definition
<1-255>	The range of virtual router ID is 1 to 255.
<key>	A text password used for authentication.

Default No authentication

Mode Interface Config

6.8.2.8. ip vrrp preempt

This command sets the preemption mode value for the virtual router configured on a specified interface.

To set the default preemption mode value for the virtual router configured on a specified interface, use the **no** form of this command.

Format ip vrrp <1-255> preempt

no ip vrrp <1-255> preempt

Fields	Definition
<1-255>	The range of virtual router ID is 1 to 255.
<key>	A text password used for authentication.

Default Enabled

Mode Interface Config

6.8.2.9. ip vrrp priority

This command sets the priority value for the virtual router configured on a specified interface.

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.

To set the default priority value for the virtual router configured on a specified interface, use the **no** form of this command.

Format ip vrrp <1-255> priority <1-254>

no ip vrrp <1-255> priority

Fields	Definition
<1-255>	The range of virtual router ID is 1 to 255.
<1-254>	The range of priority is 1 to 254.

Default The default priority value is 100 unless the router is the address owner, in which case its priority is automatically set to 255.

Mode Interface Config

6.8.2.10. ip vrrp timers advertise

This command sets the advertisement value for a virtual router in seconds.

To set the default advertisement value for a virtual router, use the **no** form of this command.

Format ip vrrp <1-255> timers advertise <1-255>

no ip vrrp <1-255> timers advertise

Fields	Definition
<1-255>	The range of virtual router ID is 1 to 255.
<1-255>	The range of advertisement interval is from 1 to 255 seconds.

Default 1 second

Mode Interface Config

6.8.2.11. ip vrrp track interface

This command alters 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.

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 decrement argument. When the interface is up for IP protocol, the priority will be incremented by the decrement 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 decrement 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.

To remove the interface from the tracked list or to restore the priority decrement to its default, use the **no** form of this command.

Format ip vrrp <1-255> track interface {<slot/port> | vlan <vlan-id>} [decrement <1-254>]

no ip vrrp <1-255> track interface {<slot/port> | vlan <vlan-id>} [decrement]

Fields	Definition
<1-255>	The range of virtual router ID is 1 to 255.
<vlan-id>	VLAN ID. The range of VLAN ID is 1 to 4093.
< 1-254 >	The range of decrement is 1 to 254.

Default Decrement: 10

Mode Interface Config

6.8.2.12. ip vrrp track ip route

This command tracks the route reachability. When the tracked route is deleted, the priority of the VRRP router will be decremented by the value specified in the decrement 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 decrement argument.

To remove the route from the tracked list or to restore the priority decrement to its default, use the **no** form of this command. 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 ip vrrp <1-255> track ip route <ip-address/prefix-length> [decrement <1-254>]

no ip vrrp <1-255> track ip route <ip-address/prefix-length> [decrement]

Fields	Definition
<1-255>	The range of virtual router ID is 1 to 255.

< 1-254 >	The range of decrement is 1 to 254.

Default Decrement: 10

Mode Interface Config

6.9. Policy Based Routing (PBR) Commands

6.9.1. Show commands

6.9.1.1. show ip policy

This command lists the route map associated with each interface.

Format show ip policy

Default None

Mode Privileged Exec

Display Message

Fields	Definition
Interface	The interface.
Route-map	The route map.

6.9.1.2. show ip prefix-list

This command displays configuration and status for a prefix list.

Format show ip prefix-list [[detail | summary] <listname> | <listname> [<prefix/length> [longer | first-match] | seq <1-4294967294>]]

Default None

Mode Privileged Exec

Display Message

Fields	Definition
detail | summary	(Optional) Displays detailed or summarized information about all prefix lists.
listname	(Optional) The name of a specific prefix list.
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.

6.9.1.3. show ipv6 prefix-list

This command displays configuration and status for a selected prefix list.

Format show ipv6 prefix-list [[detail | summary] <listname> | <listname> [<ipv6-prefix/length> [longer | first-match] | seq <1-4294967294>]]

Default None

Mode Privileged Exec

Display Message

Fields	Definition
detail | summary	(Optional) Displays detailed or summarized information about all prefix lists.
listname	(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.

6.9.1.4. show route-map

To display a route map, use the show route-map command in Privileged EXEC mode.

Format show route-map [routemap]

Fields	Definition
routename	(Optional) Name of a specific route map.

Default None

Mode Privileged Exec

6.9.2. Configuration commands

6.9.2.1. ip policy route-map

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 route-map or match/set terms are added/removed from route-map statement, and also if route-map that is applied on an interface is removed, route-map needs to be removed from interface and added back again in order to have changed route-map configuration to be effective.

In order to disable policy based routing from an interface, use **no** form of this command.

Format ip policy route-map <routemap>

no ip policy route-map <routemap>

Fields	Definition
routename	(Optional) Name of a specific route map.

Default None

Mode Interface Config

6.9.2.2. 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 command "match ip address"

Up to 128 prefix lists may be configured. The maximum number of statements allowed in prefix list is 64.

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 ip prefix-list <list-name> {[seq <seq number>] {permit | deny} prefix/length [ge <length>] [le <length>] | renumber [<renumber-interval> [<first-statement-number>]]}

no ip prefix-list <list-name> [seq <seq number>] {permit | deny} prefix/length [ge <length>] [le <length>]

Fields	Definition
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.
prefix/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-interval> **<first-statement-number>**	(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.

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.

Mode Global Config

6.9.2.3. ip prefix-list description

To apply a text description to a prefix list, use the **ip prefix-list description** command in Global Configuration mode.

To remove the text description, use the **no** form of this command.

Format ip prefix-list <list-name> description <text>

no ip prefix-list <list-name> description

Fields	Definition
list-name	The text name of the prefix list. Up to 32 characters.
description text	Text description of the prefix list. Up to 80 characters.

Default No description is configured by default.

Mode Global Config

6.9.2.4. ipv6 prefix-list

To create a IPv6 prefix list or add a prefix list entry, use the **ipv6 prefix-list** command in Global Configuration mode. 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 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.

An IPv6 prefix list may be used within a route map to match a route's prefix using the command "match ipv6 address" A route map may contain both IPv4 and IPv6 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.

To delete a IPv6 prefix list or a statement in a prefix list, use the **no** form of this command. The command **no ipv6 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 ipv6 prefix-list <list-name> {[seq <seq number>] {permit | deny} ip6-prefix/prefix-length [ge <length>] [le <length>] | description <text> | renumber [<renumber-interval> [<first-statement-number>]]}

no ipv6 prefix-list <list-name> {[seq <seq number>] {permit | deny} ip6-prefix/prefix-length [ge <length>] [le <length>] | description}

Fields	Definition
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 IPv6 prefix where the address is specified in hexadecimal using 16-bit values between colons. The prefix-length is 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.
<renumber-interval> **<first-statement-number>**	(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. The valid range for renumber-interval is 1 - 100, and the valid range for first-statement-number is 1 - 1000

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.

Mode Global Config

6.9.2.5. 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. It accepts up to 64 route maps.

To delete a route map or one of its statements, use the **no** form of this command.

Format route-map <map-tag> [permit|deny] [sequence-number]

no route-map <map-tag> [sequence-number]

Fields	Definition
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. Not support in the **no** form.
deny	(Optional) Deny routes that match all of the match conditions in the route map. Not support in the **no** form.
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, three cases would happen: ● If there is no route map existed, a route map with sequence number 10 and permit action will be created. ● If there is already one route map in system, the existed route map will be edited.

	• If there is already more than one route map in system, need to specify the sequence number. . The range is 0 to 65,535.

Default No route maps are configured by default. If no permit or deny tag is given, permit is the default.

Mode Global Config

6.9.2.6. 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.

To delete the match as-path term that matches BGP autonomous system paths against an AS path access list, use the **no** form of this command.

Format match as-path <as-path-list-number>

no match as-path

Fields	Definition
as-path-list-number	An integer from 1 to 500 identifying the AS path access list to use as match criteria.

Default None

Mode Route Map Config

6.9.2.7. 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.

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 match community <community-list> [community-list...] [exact-match]

no match community <community-list> [community-list...] [exact-match]

Fields	Definition
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.

Default None

Mode Route Map Config

6.9.2.8. match ip address prefix-list

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.

To delete a match statement from a route map, use the **no** form of this command.

Format match ip address prefix-list <list-name> [list-name...]

no match ip address prefix-list <list-name> [list-name...]

Fields	Definition
list-name	The name of a prefix list used to identify the set of matching routes. Up to eight prefix lists may be specified.

Default No match criteria are defined by default

Mode Route Map Config

6.9.2.9. match ip address <acl-id | acl-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.

To delete a match statement from a route map, use the **no** form of this command.

Format match ip address <acl-id | acl-name> [...acl-id | acl-name]

no match ip address <acl-id | acl-name> [...acl-id | acl-name]

Fields	Definition
acl-id	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.
acl-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.

Default No match criteria are defined by default

Mode Route Map Config

6.9.2.10. match ipv6 address

To configure a route map to match based on a destination prefix, use the **match ip address** command in Route Map Configuration mode. prefix-list <prefix-list-name> identifies the name of an IPv6 prefix list used to identifythe set of matching routes. Up to eight prefix lists may be specified. 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 ipv6 address statement within a route map section that already has a match ipv6 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.

To delete a match statement from a route map, use the **no** form of this command.

Format match ipv6 address prefix-list <list-name> [list-name...]

no match ipv6 address prefix-list <list-name> [list-name...]

Fields	Definition
list-name	The name of a prefix list used to identify the set of matching routes. Up to eight prefix lists may be specified.

Default No match criteria are defined by default

Mode Route Map Config

6.9.2.11. 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. min specifies the packet's minimum Layer 3 length, inclusive, allowed for a match. max 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.

To delete a match statement from a route map, use the **no** form of this command.

Format match length <min> <max>

no match length

Default No match criteria are defined by default

Mode Route Map Config

6.9.2.12. 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.

To delete a match statement from a route map, use the **no** form of this command.

Format match mac-list <mac-list-name> [mac-list-name]

no match mac-list <mac-list-name> [mac-list-name]

Fields	Definition
mac-list-name	The mac-list name that identifies MAC ACLs. MAC Access-list name can be up to 31 characters in length.

Default No match criteria are defined by default

Mode Route Map Config

6.9.2.13. 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.

To remove a set command from a route map, use the **no** form of this command.

Format set as-path prepend <as-path-string>

no set as-path prepend

Fields	Definition
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.

Default None

Mode Route Map Config

6.9.2.14. 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).

To delete the set command from a route map, use the **no** form of this command.

Format set comm-list <community-list-name> delete

no set comm-list

Fields	Definition
community-list-name	A standard community list name.

Default None

Mode Route Map Config

6.9.2.15. 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 "**set comm-list delete**".

To remove a set term from a route map, use the **no** form of this command.

Format set community {<community-number> {[additive] | [no-advertise] | [no-export]} | no-advertise | no-export | none}

no set community

Fields	Definition
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.
no-advertise	Matching route not to be advertised to any BGP peer.
no-export	Matching route not to be advertised to external BGP peer
none	Removes all communities from matching routes

Default None

Mode Route Map Config

6.9.2.16. 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.

To remove a set term from a route map, use the **no** form of this command.

Format set interface null0

no set interface null0

Fields	Definition
null0	Specify the destination interface to be null interface .

Default None

Mode Route Map Config

6.9.2.17. 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 ECMP rule 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.

To remove a set command from a route map, use the **no** form of this command.

Format set ip next-hop <next-hop-address> [...next-hop-address]

no set ip next-hop <next-hop-address> [...next-hop-address]

Fields	Definition
next-hop-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.

Default None

Mode Route Map Config

6.9.2.18. 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 ECMP rule is used.

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.

To remove a set command from a route map, use the **no** form of this command.

Format set ip default next-hop <next-hop-address> [...next-hop-address]

no set ip default next-hop <next-hop-address> [...next-hop-address]

Fields	Definition
next-hop-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.

Default None

Mode Route Map Config

6.9.2.19. 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).

To reset the three IP precedence bits in the IP packet header to the default, use the **no** form of this command.

Format set ip precedence 0-7

no set ip precedence

Fields	Definition
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.

Default None

Mode Route Map Config

6.9.2.20. set ipv6 next-hop

Use this command to set the IPv6 next hop of a route. 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 UPDATE is received or sent. If the command specifies a global IPv6 address, the address is not required to be on a local subnet.

To remove a set command from a route map, use the **no** form of this command.

Format set ipv6 next-hop <next-hop-ipv6-address>

no set ipv6 next-hop

Fields	Definition
Next-hop-ipv6-address	The IPv6 address set as the Network Address of Next Hop field in the MP_NLRI attribute of an UPDATE message.

Default None

Mode Route Map Config

6.9.2.21. 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 'match as-path' or '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.

To remove a set command from a route map, use the **no** form of this command.

Format set local-preference <value>

no set local-preference

Fields	Definition
value	A local preference value, from 0 to 4,294,967,295 (any 32-bit integer).

Default None

Mode Route Map Config

6.9.2.22. set metric

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.

To remove a set command from a route map, use the **no** form of this command.

Format set metric <value>

no set metric

Fields	Definition
value	A metric value, from 0 to 4,294,967,295 (any 32-bit integer).

Default None

Mode Route Map Config

6.9.2.23. 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 [[list-name] [prefix/length]]

Fields	Definition
list-name	(Optional) Name of the prefix list from which the hit count is to be cleared.
prefix/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.

Default None

Mode Privileged Exec

6.9.2.24. clear ipv6 prefix-list

To reset IPv6 prefix-list counters, use the **clear ipv6 prefix-list** command in Privileged EXEC mode. This command is used to 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 [[list-name] [ipv6-prefix/prefix-length]]

Fields	Definition
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.

Default None

Mode Privileged Exec

6.10. Border Gateway Protocol (BGP) Commands

6.10.1. Show commands

6.10.1.1. show ip bgp

This command displays information relevant to the BGP router.

Format show ip bgp

Default None

Mode Privileged Exec

Display Message

Fields	Definition
BGP table version	The BGP Table Version is the main number used. This number is the same as the Generation ID of any BGP prefix for a specific address family and is used to track changes to the BGP route table. Each time phase 2 of the BGP decision process runs to select new BGP routes, this number is incremented.
Local Route ID	A 32-bit integer in dotted decimal format identifying the router, about which information is displayed. This is a configured value.
Status Codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s — The table entry is suppressed. • * — The table entry is valid. • > — The table entry is the best entry to use for that network. • i — The table entry was learned via an internal BGP (iBGP) session. • S — The table entry is stale route.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i — Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. • e — Entry originated from an Exterior Gateway Protocol (EGP). • ? — Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Destination prefix.
Next Hop	The route's BGP next hop.

Metric	Multi Exit Discriminator.
LocPref	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

6.10.1.2. show ip bgp <prefix/length>

This command displays the BGP routing table entries which are filtered the display output with a prefix/length.

Format show ip bgp [vrf <*vrf-name*>] <prefix/length> [longer-prefixes | shorter-prefixes [length]]

Fields	Definition
vrf-name	Display BGP route table whithin a VRF instance.
prefix/length	The destination IP prefix and prefix length entered to filter the output to display only a particular host or network in the BGP routing table.
longer-prefixes	Display the specified prefix and any longer prefixes within the same range.
shorter-prefixes [length]	Used with the *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.

Default None

Mode Privileged Exec
User Exec

Display Message

Fields	**Definition**
Prefix/Prefix Length	The destination IP prefix and prefix length entered to filter the output to display only a particular host or network in the BGP routing table.
Generation ID	Incremented each time phase 2 of the decision process runs and whenever an aggregate address changes. Used to track changes to the BGP route table.
Advertised to Update Groups	The outbound update groups that this route is advertised to.
Best Path	Shows best path information as following.
Non-Best Paths	Shows non-best path information as following.

Local Preference	Local preference value as set with the set local-preference route-map configuration command or received from the peer. The default value is 100.
AS Path	An Autnonomous System path is a list of all the autonomous systems that a specific route passes through to reach one destination.
Origin	Indicates the origin of the entry. It can be **IGP**, **EGP**, and **Incomplete**. Value of the ORIGIN attribute.
Metric	The value of the interautonomous system metric. Value of the MED attribute, if included.
Type	Type of peer (internal or external).
IGP Cost	The cost of Interior Gateway Protocol (IGP) to the BGP NEXT HOP.
Peer (Peer ID)	The IP Address of the Peer's BGP interface (The Router ID of the Peer's BGP).
BGP Next Hop	IP address of the next system that is used when forwarding a packet to the destination network.
Atomic Aggregate	Include atomic-aggregate routes or not.
Aggregator (AS, Router ID)	The information (AS number and router ID) of the speaker that aggregated the routes.
Communities	Valid value is a BGP community number in the range from 1 to 4294967200, or AA:NN (autonomous system-community number/2-byte number), **no-peer**, **no-export**, **no-export-subconfed**, or **no-advertise**.
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.

6.10.1.3. show ip bgp aggregate-address

This command displays information about the aggregate-address. If a VRF instance is specified, the aggregate addresses configured in that VRF instance are displayed.

Format show ip bgp [vrf *vrf-name*] aggregate-address

Default None

Mode Privileged Exec
User Exec

Display Message

Fields	Definition
Aggregation of routes with different MED values is allowed	The aggregate-different-meds is enabled.
Prefix/Len	Destination IP 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 address is currently begin advertised.

6.10.1.4. show ip bgp community

This command display routes that belong to specified BGP communities. If a VRF instance is specified, the routes belonging to the community within that VRF instance are displayed.

Format show ip bgp [vrf *vrf-name*] community [<community-number>] [exact-match] [no-advertise] [no-export]

Fields	Definition
vrf-name	Display routes belonging to communities whithin a VRF instance.
< community-number >	Valid value is a community number in the range from 1 to 4294967295, or AA:NN (autonomous system-community number/2-byte number).
exact-match	Destination IP prefix and prefix length.
no-advertise	Display only routes that are not advertised to any peer.
no-export	Display only routes that are not exported outside of the local AS.

Default None

Mode Privileged Exec

User Exec

Display Message

Fields	Definition
BGP table version	The BGP Table Version is the main number used. This number is the same as the Generation ID of any BGP prefix for a specific address family and is used to track changes to the BGP route table.

Local Route ID	A 32-bit integer in dotted decimal format identifying the router, about which information is displayed. This is a configured value.
Status Codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s — The table entry is suppressed. • * — The table entry is valid. • > — The table entry is the best entry to use for that network. • i — The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i — Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e — Entry originated from an Exterior Gateway Protocol (EGP). • ? — Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Destination IP address.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. Value of the MED attribute, if included.
LocPref	Local preference value as set with the **set local-preference** route-map configuration command or received from the peer. The default value is 100.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

6.10.1.5. show ip bgp community-list

This command display routes that are permitted by the Border Gateway Protocol (BGP) community list.

Format show ip bgp community-list <community-list-name> [exact-match]

Fields	Definition
community-list-name	Community list name. The community list name can be standard or expanded.

exact-match	Displays only routes that are an exact match for the set of communities in the matching community list statement.

Default None

Mode Privileged Exec

User Exec

Display Messages

Fields	Definition
BGP table version	The BGP Table Version is the main number used. This number is the same as the Generation ID of any BGP prefix for a specific address family and is used to track changes to the BGP route table.
Local Route ID	A 32-bit integer in dotted decimal format identifying the router, about which information is displayed. This is a configured value.
Status Codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s — The table entry is suppressed. • * — The table entry is valid. • > — The table entry is the best entry to use for that network. • i — The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i — Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e — Entry originated from an Exterior Gateway Protocol (EGP). • ? — Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Destination IP address.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. Value of the MED attribute, if included.
LocPref	Local preference value as set with the **set local-preference** route-map configuration command or received from the peer. The default value is 100.

Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

6.10.1.6. show ip bpg filter-list

Use this command to display routes that conform to a specified filter list.

Format show ip bgp filter-list as-path-list

Fields	Definition
as-path-list	Filter the output to the set of routes that match a given AS Path list. It can be a number from 1 to 500.

Default None

Mode Privileged Exec

User Exec

Display Messages

Fields	Definition
BGP table version	The BGP Table Version is the main number used. This number is the same as the Generation ID of any BGP prefix for a specific address family and is used to track changes to the BGP route table.
Local Route ID	A 32-bit integer in dotted decimal format identifying the router, about which information is displayed. This is a configured value.
Status Codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s — The table entry is suppressed. • * — The table entry is valid. • > — The table entry is the best entry to use for that network. • i — The table entry was learned via an internal BGP (iBGP) session. • S – The table entry stale route.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i — Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e — Entry originated from an Exterior Gateway Protocol (EGP). • ? — Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Destination IP address.

Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. Value of the MED attribute, if included.
LocPref	Local preference value as set with the **set local-preference** route-map configuration command or received from the peer. The default value is 100.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

6.10.1.7. show ip bgp neighbors

This command displays information about Border Gateway Protocol (BGP) and TCP connections to neighbors. If a VRF instance is specified, the routes information for the neighbors within that VRF instance are displayed.

Format show ip bgp [vrf *vrf-name*] neighbors [<ip-address> [advertised-routes | policy | received-routes | rejected-routes | routes] | policy]

Fields	Definition
vrf-name	Display routes whithin a VRF instance.
ip-address	Displays information about the IPv4 neighbor. If this argument is omitted, information about all neighbors is displayed.
Policy	Display inbound and outbound policies for all neighbors or the specified neighbor.
Advertised-routes	Display routes advertised to a neighbor.
Received-routes	Display routes received from a neighbor.
Rejected-routes	Display routes rejected by inbound policy.
Routes	Display routes accepted by inbound policy.

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	Definition
Remote Address	The IP Address of the Peer's BGP interface.

Remote AS	Autonomous system number of the neighbor.
BFD Enabled to Detect Fast Fallover	Specify if BFD has been enabled for BGP neighbors.
Peer ID	Router ID of the neighbor.
Peer Admin Status	States whether BGP is enabled or disabled of the neighbor.
Peer State	Finite state machine (FSM) stage of session negotiation.
Local Interface Address	The IPv4 address used as the source IP address in packets sent to this neighbor.
Local Port	The port number of the local port.
Remote Port	The port number of the remote port.
Connection Retry Interval	Time interval, in seconds, at which the device resend messages to this neighbor.
Neighbor Capabilities	BGP capabilities advertised and received from this neighbor.
IPv4 Unicast Support	Support IPv4 unicast packets or not. The valid value will be Both, Sent, Received or None.
VPNv4 Unicast Support	Support VPNv4 unicast packets or not. The valid value will be Both, Sent, Received or None.
IPv6 Unicast Support	Support IPv6 unicast packets or not. The valid value will be Both, Sent, Received or None.
BGP Graceful-Restart Mode	BGP Graceful-Restart mode. Enabled or Disabled.
BGP Graceful-Restart Restart-Time	BGP graceful restart helper restart timer.
Template Name	Name of a locally configured peer policy template.
Update Source	The configured value for the source IP address of packets sent to this neighbor. This field is only included in the output if the update source is configured.
Configured Hold Time	Configured time for this neighbor, in seconds, that BGP will maintain the session with this neighbor without receiving a messages.
Configured Keep Alive Time	Configured time interval for this neighbor, in seconds, at which keepalive messages are transmitted to this neighbor.
Negotiated Hold Time	Negotiated time with this neighbor, in seconds, that BGP will maintain the session with this neighbor without receiving a messages.
Negotiated Keep Alive Time	Negotiated time interval with this neighbor, in seconds, at which keepalive messages are transmitted to this neighbor.
MD5 Password	The TCP MD5 password, if one is configured, in plain text.
eBGP-MultiHop	Configured TTL value of the external BGP for this neighbor.
Last Error ()	Last error from received or sent for this neighbor.

Last SubError	Last sub error for this neighbor.
Time Since Last Error	The time stamps in which the last error occurred.
Established Transitions	The number of connections established.
Flap Count	Total number of times the neighbor flaps.
Established Time	The time from the last connection established.
Time Since Last Update	The time from the last Update message received.
IPv4 Outbound Update Group	The corresponding index number of the IPv4 update group.
IPv6 Outbound Update Group	The corresponding index number of the IPv6 update group.
BFD Enabled to Detect Fast Fallover	Indicate if the BFD is enabled for this BGP neighbor.
Msgs Sent	Total number of transmitted messages.
Msgs Rcvd	Total number of received messages.
Open	Number of open messages sent and received.
Update	Number of update messages sent and received.
Keepalive	Number of keepalive messages sent and received.
Notification	Number of notification (error) messages sent and received.
Refresh	Number of route refresh request messages sent and received.
Total	Total number of messages sent and received.
Received UPDATE Queue Size	The statistics of received UPDATE queue (Size, High, Limit, Drops).
IPv4 Prefix Statistics	The statistics of the IPv4 prefix.
VPNv4 Prefix Statistics	The statistics of the VPNv4 prefix.
IPv6 Prefix Statistics	The statistics of the IPv6 prefix.
Prefixes Advertised	Number of prefixes advertised.
Prefixes Withdrawn	Number of prefixes withdrawn.
Prefixes Current	Number of prefixes current kept.
Prefixes Accepted	Number of prefixes accepted.

Prefixes Rejected	Number of prefixes rejected.
Max NLRI per Update	Maximum number of network layer reachability attributes in UPDATEs.
Min NLRI per Update	Minimum number of network layer reachability attributes in UPDATEs.

6.10.1.8. show ip bgp prefix-list

This command displays information about a prefix list or prefix list entries.

Format show ip bgp prefix-list <prefix-list-name>

Fields	Definition
prefix-list-name	Filter the output to the set of routes that match a given prefix list..

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	Definition
BGP table version	The BGP Table Version is the main number used. This number is the same as the Generation ID of any BGP prefix for a specific address family and is used to track changes to the BGP route table.
Local Route ID	A 32-bit integer in dotted decimal format identifying the router, about which information is displayed. This is a configured value.
Status Codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s — The table entry is suppressed. • * — The table entry is valid. • > — The table entry is the best entry to use for that network. • i — The table entry was learned via an internal BGP (iBGP) session. • S — The table entry stale route.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i — Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e — Entry originated from an Exterior Gateway Protocol (EGP).

	• ? — Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Destination IP address.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. Value of the MED attribute, if included.
LocPref	Local preference value as set with the **set local-preference** route-map configuration command or received from the peer. The default value is 100.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

6.10.1.9. 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 within that VRF instance are displayed.

If a route reflector client is configured with an outbound route map, the output warns that the set statements in the route map are ignored when reflecting routes to this client.

Format show ip bgp [vrf *vrf-name*] route-reflection

Default None

Mode Privileged Exec

User Exec

Display Messages

Fields	Definition
Cluster ID	The cluster ID used by this router. The value configured with the *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	Display Enabled when this router reflectors routes received from it clients to its other clients; otherwise display Disabled.
Clients	A list of this router's internal peers that have been configured as router reflector clients.
Non-client Internal Peer	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.

6.10.1.10. show ip bgp summary

This command displays the status of all Border Gateway Protocol (BGP) connections. If a VRF instance is specified, the configuration and status for the routes within that VRF instance are displayed.

Format show ip bgp [vrf *vrf-name*] summary

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	Definition
IPv4 Routing	Whether IPv4 routing is globally enabled.
BGP Admin Mode	Shows whether the administrative mode of BGP in the router is enabled or disabled.
BGP Operational Mode	Shows whether the BGP is operated in enabled or disabled.
BGP Router ID	Router ID for the current BGP.
Local AS Number	Autonomous system number of the current BGP.
Number of Network Entries	Number of unique prefix entries in the BGP database.
Number of AS Paths	Number of path entries in the BGP database.
Dynamic Neighbors Current/High/Limit	The limit number of BGP dynamic neighbors
Neighbor	IP address of the neighbor.
ASN	Autonomous system number of the neighbor.
MsgRcvd	Number of messages received from the neighbor.
MsgSent	Number of messages sent to the neighbor.
State	The area ID of the OSPF area associated with the interface.
Up/Down Time	The length of time that the BGP session has been in the Established state, or the current status if not in the Established state.
Pfx Rcvd	The number of prefixes that have been received from a neighbor.

6.10.1.11. show ip bgp template

This command displays peer policy template configurations.

Format show ip bgp template [<template-name>]

Fields	Definition
template-name	Displays the configurations in a specific template.

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	Definition
template-name	Name of the peer template.
AF	Address Family (IPv4 or IPv6).
Configuration	The configuration information of the peer template.

6.10.1.12. show ip bgp traffic

This command displays global BGP message counters. If a VRF instance is specified, the counters within that VRF instance are displayed.

Format show ip bgp [vrf *vrf-name*] traffic

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	Definition
Time Since Counters Cleared	How long ago the SPF ran. The time is in the format hh:mm:ss, giving the hours, minutes, and seconds since the SPF run.
BGP Message Statistics	The statistics of BGP messages sent/received.
Recd	Total number of received messages.
Sent	Total number of transmitted messages.

Open	Number of open messages sent and received.
Update	Number of update messages sent and received.
Notification	Number of notification (error) messages sent and received.
Keepalive	Number of keepalive messages sent and received.
Refresh	Number of route refresh request messages sent and received.
Total	Total number of messages sent and received.
Max Received UPDATE rate	Maximum rate of received UPDATE messages.
Max Send UPDATE rate	Maximum rate of sent UPDATE messages.
BGP Queue Statistics	The queue statistics of BGP protocol thread.
Events	Holds configuration events, timer expiration events and TCP status reports.
Keepalive Tx	Keepalive timer event expirations.
Dec Proc	Holds events to trigger one of the 3 phases of the decision proces.
Rx Data	Incoming data.
RTO Notifications	RTO notifications. Redistributed routes and next hop resolution changes.
MIB Queries	BGP MIB path queries.
Current	Number of messages in queue currently.
Max	Maximum number of messages in queue.
Drops	Number of messages dropped.
Limit	Maximum size of queue.

6.10.1.13. show ip bgp update-group

This command displays information about the Border Gateway Protocol (BGP) update groups. 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 [index-group | peeripadd]

Fields	Definition
index-group	Update group type with its corresponding index number. The range of update-group index numbers is from 1 to 4294967295.

Peeripadd	IPv4 or IPv6 address of a single neighbor who is a member of an update group.

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	**Definition**
Update Group	Update-group number.
Peer Type	Update-group type (internal or external).
Minimum Advertisement Interval	Minimum time, in seconds, between update advertisements.
Send Community	If the BGP communities are included in route advertisements to members of the group.
Send Extended Community	If the BGP extended communites 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	Neighbor AS Path list out. All members of the group use the same.
Neighbor Prefix List Out	Neighbor prefix list out. All members of the group use the same.
Neighbor Route Map Out	Neighbor route map out. All members of the group use the same.
Members Added	Number of members added to the group.
Members Removed	Number of members removed from the group.
Update Version	Number of times phase 3 of the decision process has run for the group.
Number of UPDATES Sent	Number of UPDATE packets sent to this group.
Time Since Last UPDATE	Number of seconds since last UPDATE sent to group.
Current Prefixes	Number of prefixes currently advertised to the group.
Current Paths	Number of paths in update group's Adj-RIB-Out.

Prefixes Advertised	Number of prefixes advertised.
Prefixes Withdrawn	Number of prefixes withdrawn.
UPDATE Send Failures	Number of Tx of UPDATE message failed to one or more group members.
Current Members	The IPv4 address of all current members of the group.
Version	The number of times decision process phase 3 had run before this history table entry.
Delta T	When update send occured.
Duration	How long the update send process took.
UPD Built	Number of UPDATE messages constructed during this update send.
UPD Sent	Number of UPDATE messages transmitted during this update send. Generally each UPDATE built is sent once to each member of the update group.
Paths Sent	Number of prefixes advertised during this update send.
Pfxs Adv	Number of prefixes withdrawn during this update send.
Pfxs Wd	Number of paths advertised.

6.10.1.14. show bgp ipv6

This command displays IPv6 routes in the BGP routing table.

Format show bgp ipv6

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	Definition
BGP table version	The BGP Table Version is the main number used. This number is the same as the Generation ID of any BGP prefix for a specific address family and is used to track changes to the BGP route table. Each time phase 2 of the BGP decision process runs to select new BGP routes, this number is incremented.
Local Route ID	A 32-bit integer in dotted decimal format identifying the router, about which information is displayed. This is a configured value.
Status Codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values:

	• s — The table entry is suppressed. • * — The table entry is valid. • > — The table entry is the best entry to use for that network. • i — The table entry was learned via an internal BGP (iBGP) session. • S — The table entry is stale route
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i — Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e — Entry originated from an Exterior Gateway Protocol (EGP). • ? — Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 Destination prefix.
Next Hop	The IPv6 route's BGP next hop.
Metric	Multi Exit Discriminator.
LocPref	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

6.10.1.15. show bgp ipv6 <ipv6-prefix/prefix-length>

This command displays the BGP routing table entries which are filtered the display output with a ipv6-prefix/prefix-length.

Format show bgp ipv6 <ipv6-prefix/prefix-length> [longer-prefixes | shorter-prefixes [length]]

Fields	Definition
ipv6-prefix/length	The destination IPv6 prefix and prefix length entered to filter the output to display only a particular host or network in the BGP routing table.
longer-prefixes	Display the specified prefix and any longer prefixes within the same range.
shorter-prefixes [length]	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.

Default None

Mode Privileged Exec

User Exec

Display Messages

Fields	Definition
ipv6-prefix/length	The destination IPv6 prefix and prefix length entered to filter the output to display only a particular host or network in the BGP routing table.
Generation ID	Incremented each time phase 2 of the decision process runs and whenever an aggregate address changes. Used to track changes to the BGP route table.
Advertised to Update Groups	The outbound update groups that this route is advertised to.
Best Path	Shows best path information as following.
Non-Best Paths	Show non-best path information as following.
Local Preference	Local preference value as set with the set local-preference route-map configuration command or received from the peer. The default value is 100.
AS Path	An Autnonomous System path is a list of all the autonomous systems that a specific route passes through to reach one destination.
Origin	Indicates the origin of the entry. It can be **IGP**, **EGP**, and **Incomplete**. Value of the ORIGIN attribute.
Metric	The value of the interautonomous system metric. Value of the MED attribute, if included.
Type	Type of peer (internal or external).
IGP Cost	The cost of Interior Gateway Protocol (IGP) to the BGP NEXT HOP.
Peer (Peer ID)	The IP Address of the Peer's BGP interface (The Router ID of the Peer's BGP).
BGP Next Hop	IP address of the next system that is used when forwarding a packet to the destination network.
Atomic Aggregate	Include atomic-aggregate routes or not.
Aggregator (AS, Router ID)	The information (AS number and router ID) of the speaker that aggregated the routes.
Communities	Valid value is a BGP community number in the range from 1 to 4294967200, or AA:NN (autonomous system-community number/2-byte number), **no-peer**, **no-export**, **no-export-subconfed**, or **no-advertise**.
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.

6.10.1.16. show bgp ipv6 aggregate-address

This command displays information about the aggregate-address.

Format show bgp ipv6 aggregate-address

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	Definition
Aggregation of routes with different MED values is allowed	The aggregate-different-meds is enabled.
Prefix/Len	Destination IPv6 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 address is currently begin advertised.

6.10.1.17. show bgp ipv6 community

This command display routes that belong to specified BGP communities.

Format show bgp ipv6 community [<community-number>] [exact-match] [no-advertise] [no-export] [no-export-subconfed]

Fields	Definition
< community-number >	Valid value is a community number in the range from 1 to 4294967295, or AA:NN (autonomous system-community number/2-byte number).
exact-match	Display only routes that are members of those communities specified in the command.
no-advertise	Display only routes that are not advertised to any peer.
no-export	Display only routes that are not exported outside of the local AS.

no-export-subconfed	Display only routes that are not sent outside of the local AS or subconfeds.

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	Definition
BGP table version	The BGP Table Version is the main number used. This number is the same as the Generation ID of any BGP prefix for a specific address family and is used to track changes to the BGP route table.
Local Route ID	A 32-bit integer in dotted decimal format identifying the router, about which information is displayed. This is a configured value.
Status Codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s — The table entry is suppressed. • * — The table entry is valid. • > — The table entry is the best entry to use for that network. • i — The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i — Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e — Entry originated from an Exterior Gateway Protocol (EGP). • ? — Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Destination IP address.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network.
Metric	The value of the interautonomous system metric. Value of the MED attribute, if included.
LocPref	Local preference value as set with the **set local-preference** route-map configuration command or received from the peer. The default value is 100.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

6.10.1.18. show bgp ipv6 community-list

This command display IPv6 routes that are permitted by the Border Gateway Protocol (BGP) community list.

Format show bgp ipv6 community-list <community-list-name> [exact-match]

Fields	Definition
community-list-name	Community list name. The community list name can be standard or expanded.
exact-match	Displays only routes that are an exact match for the set of communities in the matching community list statement.

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	Definition
BGP table version	The BGP Table Version is the main number used. This number is the same as the Generation ID of any BGP prefix for a specific address family and is used to track changes to the BGP route table.
Local Route ID	A 32-bit integer in dotted decimal format identifying the router, about which information is displayed. This is a configured value.
Status Codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s — The table entry is suppressed. • * — The table entry is valid. • > — The table entry is the best entry to use for that network. • i — The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i — Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e — Entry originated from an Exterior Gateway Protocol (EGP). • ? — Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Destination IP address.

Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. Value of the MED attribute, if included.
LocPref	Local preference value as set with the **set local-preference** route-map configuration command or received from the peer. The default value is 100.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

6.10.1.19. show ip bgp vpnv4

This command displays BGP VPNv4 routes.

Format show ip bgp vpnv4 {<prefix/length> | all | rd <as-number>:<value> | <ip-address>:<value> [<prefix/length>] | vrf <vrfname> [<prefix/length>]}

Default None

Mode Privileged Exec

User Exec

Display Message

Fields	Definition
BGP table version	The BGP Table Version is the main number used. This number is the same as the Generation ID of any BGP prefix for a specific address family and is used to track changes to the BGP route table. Each time phase 2 of the BGP decision process runs to select new BGP routes, this number is incremented.
Local Route ID	A 32-bit integer in dotted decimal format identifying the router, about which information is displayed. This is a configured value.
Status Codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s — The table entry is suppressed. • * — The table entry is valid. • > — The table entry is the best entry to use for that network. • i — The table entry was learned via an internal BGP (iBGP) session. • S — The table entry is stale route

Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i — Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. • e — Entry originated from an Exterior Gateway Protocol (EGP). • ? — Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Destination prefix.
Next Hop	The route's BGP next hop.
Metric	Multi Exit Discriminator.
LocPref	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

6.10.1.20. show ip bgp listen range

This command displays IPv4 BGP listen ranges as well as peers discovered.

Format show ip bgp [vrf <vrf-name>] listen range [<prefix>/<prefix-length>]

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	Definition
Listen Range	The IP address range to listen BGP peers
Inherited Template	The peer template inherited
Member	The IP address of the BGP peer discovered
ASN	The AS number which the BGP peer belongs to
State	The neighboring state of the BGP peer discovered

6.10.1.21. show ip protocols bgp

This command displays setting of IPv4 BGP configuration. If the virtual router is specified, the summary of the configuration and status running in the specified virtual router is listed. If no virtual router is specified, the configuration and status for the default router are displayed.

Format show ip protocol [vrf vrf-name] bgp

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	Definition
Routing Protocol	Routing protocol of these setting. It's always BGP in this case.
BGP Router ID	Setting of BGP router ID
Local AS Number	AS Number of this device.
BGP Admin Mode	Whether BGP protocol is enabled. (Enabled or Disabled).
BGP GR-Enabled Mode	Whether BGP Graceful Restart Enabled Mode is enabled. (Enabled or Disabled)
BGP GR-Aware Mode	Whether BGP Graceful Restart Aware Mode is enabled. (Enabled or Disabled)
BGP GR restart-time	Setting of BGP Graceful Restart Timer.
BGP GR stalepath-time	Setting of BGP Graceful Stale Path Timer.
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 routers 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 an iBGP adjacency if the routing table manager reports that the peer address is no longer reachable.
Fast External Failover	Whether BGP immediately brings down a eBGP adjacency if the routing table manager reports that the peer address is no longer reachable..
Distance	The administrative distance for intra-area, inter-area, and external routes.
Prefix List In	The global prefix list used to filter inbound routers from all neighbors.

Prefix List Out	The global prefix list used to filter outbound routers from all neighbors.
Networks Originated	The set of networks originated through a network command. Those networks that are actually advertised to neighbors are marked “active”.

6.10.1.22. show bgp ipv6 filter-list

Use this command to display routes that conform to a specified filter list.

Format show bgp ipv6 filter-list <as-path-list>

Fields	Definition
as-path-list	Filter the output to the set of routes that match a given AS Path list. It can be a number from 1 to 500.

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	Definition
BGP table version	The BGP Table Version is the main number used. This number is the same as the Generation ID of any BGP prefix for a specific address family and is used to track changes to the BGP route table.
Local Route ID	A 32-bit integer in dotted decimal format identifying the router, about which information is displayed. This is a configured value.
Status Codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s — The table entry is suppressed. • * — The table entry is valid. • > — The table entry is the best entry to use for that network. • i — The table entry was learned via an internal BGP (iBGP) session. • S — The table entry stale route.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i — Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e — Entry originated from an Exterior Gateway Protocol (EGP).

	• ? — Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Destination IPv6 address.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network.
Metric	The value of the interautonomous system metric. Value of the MED attribute, if included.
LocPref	Local preference value as set with the **set local-preference** route-map configuration command or received from the peer. The default value is 100.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

6.10.1.23. show bgp ipv6 neighbors

This command displays information about Border Gateway Protocol (BGP) and TCP connections to neighbors.

Format show bgp ipv6 neighbors [<ip-address> [interface {<slot/port> | vlan <1-4093>}] [advertised-routes | policy | received-routes | rejected-routes | routes] | policy | autodetect interface <slot/port>[advertised-routes | policy | received-routes | rejected-routes | routes]]

Fields	Definition
ip-address	Displays information about the IPv6 neighbor. If this argument is omitted, information about all neighbors is displayed.
Policy	Display inbound and outbound policies for all neighbors or the specified neighbor.
advertised-routes	Display routes advertised to a neighbor.
received-routes	Display routes received from a neighbor.
rejected-routes	Display routes rejected by inbound policy.
Routes	Display routes accepted by inbound policy.
Autodetect	Display information about the autodetected IPv6 neighbor on the specified *interface-name*.

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	Definition
Remote Address	The IP Address of the Peer's BGP interface.
Autodetect Status	Display 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”.
Remote AS	Autonomous system number of the neighbor.
Allow my ASN occurences	The allowas-in count for a given peer.
Peer ID	Router ID of the neighbor.
Peer Admin Status	States whether BGP is enabled or disabled of the neighbor.
Peer State	Finite state machine (FSM) stage of session negotiation.
Local Interface Address	The IPv6 address used as the source IP address in packets sent to this neighbor.
Local Port	The port number of the local port.
Remote Port	The port number of the remote port.
Connection Retry Interval	Time interval, in seconds, at which the device resend messages to this neighbor.
Neighbor Capabilities	BGP capabilities advertised and received from this neighbor.
IPv4 Unicast Support	Support IPv4 unicast packets or not. The valid value will be Both, Sent, Received or None.
VPNv4 Unicast Support	Support VPNv4 unicast packets or not. The valid value will be Both, Sent, Received or None.
IPv6 Unicast Support	Support IPv6 unicast packets or not. The valid value will be Both, Sent, Received or None.
RFC 5549 Support	Support RFC5549 or not.
BGP Graceful-Restart Mode	BGP Graceful-Restart mode. Enabled or Disabled.
BGP Graceful-Restart Restart-Time	BGP graceful restart helper restart timer.
Template Name	Name of a locally configured peer policy template.
Update Source	The configured value for the source IP address of packets sent to this neighbor. This field is only included in the output if the update source is configured.
Configured Hold Time	Configured time for this neighbor, in seconds, that BGP will maintain the session with this neighbor without receiving a messages.
Configured Keep Alive Time	Configured time interval for this neighbor, in seconds, at which keepalive messages are transmitted to this neighbor.

Negotiated Hold Time	Negotiated time with this neighbor, in seconds, that BGP will maintain the session with this neighbor without receiving a messages.
Negotiated Keep Alive Time	Negotiated time interval with this neighbor, in seconds, at which keepalive messages are transmitted to this neighbor.
MD5 Password	The TCP MD5 password, if one is configured, in plain text.
eBGP-MultiHop	Configured TTL value of the external BGP for this neighbor.
Last Error ()	Last error from received or sent for this neighbor.
Last SubError	Last sub error for this neighbor.
Time Since Last Error	The time stamps in which the last error occurred.
Established Transitions	The number of connections established.
Flap Count	Total number of times the neighbor flaps.
Established Time	The time from the last connection established.
Time Since Last Update	The time from the last Update message received.
IPv4 Outbound Update Group	The corresponding index number of the IPv4 update group.
IPv6 Outbound Update Group	The corresponding index number of the IPv6 update group.
BFD Enabled to Detect Fast Fallover	Indicate if the BFD is enabled for this BGP neighbor.
Msgs Sent	Total number of transmitted messages.
Msgs Rcvd	Total number of received messages.
Open	Number of open messages sent and received.
Update	Number of update messages sent and received.
Keepalive	Number of keepalive messages sent and received.
Notification	Number of notification (error) messages sent and received.
Refresh	Number of route refresh request messages sent and received.
Total	Total number of messages sent and received.
Received UPDATE Queue Size	The statistics of received UPDATE queue (Size, High, Limit, Drops).
IPv4 Prefix Statistics	The statistics of the IPv4 prefix.
IPv6 Prefix Statistics	The statistics of the IPv6 prefix.

Prefixes Advertised	Number of prefixes advertised.
Prefixes Withdrawn	Number of prefixes withdrawn.
Prefixes Current	Number of prefixes current kept.
Prefixes Accepted	Number of prefixes accepted.
Prefixes Rejected	Number of prefixes rejected.
Max NLRI per Update	Maximum number of network layer reachability attributes in UPDATEs.
Min NLRI per Update	Minimum number of network layer reachability attributes in UPDATEs.

6.10.1.24. show bgp ipv6 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 route reflector client is configured with an outbound route map, the output warns that the set statements in the route map are ignored when reflecting routes to this client.

Format show bgp ipv6 route-reflection

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	Definition
Cluster ID	The cluster ID used by this router. The value configured with the *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	Display Enabled when this router reflectors routes received from it clients to its other clients; otherwise display Disabled.
Clients	A list of this router's internal peers that have been configured as router reflector clients.
Non-client Internal Peer	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.

6.10.1.25. show bgp ipv6 statistics

This command displays the recent decision process history.

Format show bgp ipv6 statistics

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	Definition
Delta T	The time values since decision process ran. Hours:minutes:seconds if the elapsed time is less than 24 hours. Otherwise, days:hours.
Phase	In which decision process phase that ran.
Upd Grp	Outbound update group ID. Only set when decProcPhase is 3.
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	Why decision process was triggered.
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 phase took, in milliseoncds.
Adds	Number of routes added during decision process phase.
Mods	Number of routes modified during decision process phase. Always 0 in phase 1.
Dels	Number of routes deleted during decision process phase. Always 0 in phase 1.

6.10.1.26. show bgp ipv6 summary

This command displays the status of all Border Gateway Protocol (BGP) connections.

Format show bgp ipv6 summary

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	Definition
IPv6 Routing	Whether IPv6 routing is globally enabled.
BGP Admin Mode	Shows whether the administrative mode of BGP in the router is enabled or disabled.
BGP Operational Mode	Shows whether the BGP is operated in enabled or disabled.
BGP Router ID	Router ID for the current BGP.
Local AS Number	Autonomous system number of the current BGP.
Number of Network Entries	Number of unique IPv6 prefix entries in the BGP database.
Number of AS Paths	Number of path entries in the BGP database.
Neighbor	IPv6 address of the neighbor.
ASN	Autonomous system number of the neighbor.
MsgRcvd	Number of messages received from the neighbor.
MsgSent	Number of messages sent to the neighbor.
State	The area ID of the OSPF area associated with the interface.
Up/Down Time	The length of time that the BGP session has been in the Established state, or the current status if not in the Established state.
Pfx Rcvd	The number of IPv6 prefixes that have been received from a neighbor.

6.10.1.27. show bgp ipv6 update-group

This command displays information about the Border Gateway Protocol (BGP) update groups and their numbers.

Format show bgp ipv6 update-group [index-group | peeripadd | autodetect interface <interface-name>]

Fields	Definition
index-group	Update group type with its corresponding index number. The range of update-group index numbers is from 1 to 4294967295.
Peeripadd	IPv4 or IPv6 address of a single neighbor who is a member of an update group.
Autodetect	The routing interface on which the neighbor's link local IPv6 address is auto detected.

Default None

Mode Privileged Exec

User Exec

Display Messages

Fields	Definition
Update Group	Update-group number.
Peer Type	Update-group type (internal or external).
Minimum Advertisement Interval	Minimum time, in seconds, between update advertisements.
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. Otherwsie No.
Route Reflector Client	If peers in this update group are route reflector clients.
Neighbor AS Path Access List Out	Neighbor AS Path list out. All members of the group use the same.
Neighbor Prefix List Out	Neighbor prefix list out. All members of the group use the same.
Neighbor Route Map Out	Neighbor route map out. All members of the group use the same.
Members Added	Number of members added to the group.
Members Removed	Number of members removed from the group.
Update Version	Number of times phase 3 of the decision process has run for the group.
Number of UPDATES Sent	Number of UPDATE packets sent to this group.
Time Since Last UPDATE	Number of seconds since last UPDATE sent to group.
Current Prefixes	Number of prefixes currently advertised to the group.
Current Paths	Number of paths in update group's Adj-RIB-Out.
Prefixes Advertised	Number of prefixes advertised.
Prefixes Withdrawn	Number of prefixes withdrawn.
UPDATE Send Failures	Number of Tx of UPDATE message failed to one or more group members.
Current Members	The IPv4 address of all current members of the group.

Version	The number of times decision process phase 3 had run before this history table entry.
Delta T	When update send occured.
Duration	How long the update send process took.
UPD Built	Number of UPDATE messages constructed during this update send.
UPD Sent	Number of UPDATE messages transmitted during this update send. Generally each UPDATE built is sent once to each member of the update group.
Paths Sent	Number of prefixes advertised during this update send.
Pfxs Adv	Number of prefixes withdrawn during this update send.
Pfxs Wd	Number of paths advertised.

6.10.1.28. show ipv6 protocols bgp

This command displays setting of IPv6 BGP configuration.

Format show ipv6 protocol bgp

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	Definition
Routing Protocol	Routing protocol of these setting. It's always BGP in this case.
BGP Router ID	Setting of BGP router ID
Local AS Number	AS Number of this device.
BGP Admin Mode	Whether BGP protocol is enabled. (Enabled or Disabled).
BGP GR-Enabled Mode	Whether BGP Graceful Restart Enabled Mode is enabled. (Enabled or Disabled)
BGP GR-Aware Mode	Whether BGP Graceful Restart Aware Mode is enabled. (Enabled or Disabled)
BGP GR restart-time	Setting of BGP Graceful Restart Timer.
BGP GR stalepath-time	Setting of BGP Graceful Stale Path Timer.
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 routers 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 a eBGP adjacency if the routing table manager reports that the peer address is no longer reachable..
Distance	The administrative distance for intra-area, inter-area, and external routes.
Prefix List In	The global prefix list used to filter inbound routers from all neighbors.
Prefix List Out	The global prefix list used to filter outbound routers from all neighbors.
Networks Originated	The set of networks originated through a network command. Those networks that are actually advertised to neighbors are marked “active”.

6.10.1.29. show bgp ipv6 listen range

This command displays IPv6 BGP listen ranges as well as peers discovered.

Format show bgp ipv6 listen range [<ipv6-prefix>/<prefix-length>]

Fields	Definition
listen range	Display all listen subnet ranges that have been created.
<ipv6-prefix>/<prefix-length>	Display information about specified listen range.

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	Definition
Listen Range	The IP address range to listen BGP peers.
Inherited Template	The peer template inherited.
Member	The IP address of the BGP peer discovered .
ASN	The AS number which the BGP peer belongs to.

State	The neighboring state of the BGP peer discovered.

6.10.2. Configuration commands

6.10.2.1. router bgp

Use this command to enable BGP, enter the Border Gateway Protocol (BGP) router mode, and identify the AS number of the router. Only a single instance of BGP can be run and the router can only belong to a single AS. **no router bgp** command disables BGP and resets all BGP configuration to default values. Alternatively, you can use *no enable* command in BGP router configuration mode to disable BGP globally without clearing the BGP configuration.

Format router bgp <autonomous-system-number>

no router bgp <autonomous-system-number>

Fields	Definition
autonomous-system-number	Number of an autonomous system that identifies the router to other BGP routers and tags the routing information that is passed along. Number in the range from 1 to 4294967295.

Default BGP inactive

Mode Global Config

6.10.2.2. enable

Use **enable** command resets the default administrative mode of BGP in the router (active). **no enable** command sets the administrative mode of BGP in the router to inactive. When you disable BGP, BGP retains its configuration.

Format enable

no enable

Default Enabled

Mode Router BGP Config Mode

6.10.2.3. aggregate-address

Use **aggregate-address** command to create an aggregate entry in a Border Gateway Protocol (BGP) database. Use **no aggregate-address** command to disable an aggregate entry in a Border Gateway Protocol (BGP) database.

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 lengh equals the length of the aggregate address is not considered a match.
BGP accepts up to 128 summary addresses for each address family.

Format aggregate-address {<address> <mask> | <ipv6-prefix> <prefix-length>} [as-set] [summary-only]

no aggregate-address {<address> <mask> | <ipv6-prefix> <prefix-length>} [as-set] [summary-only]

Fields	Definition
Address	Summary IPv4 address. The default route cannot be configured as an aggregate address.
Mask	Summary IPv4 mask. The mask cannot be a 32-bit mask (255.255.255.255). The combination of address and mask must be a valid unicast destination prefix.
ipv6-prefix	Summary IPv6 prefix. Not support under IPv4 VRF address family mode.
prefix-length	Summary IPv6 prefix length. The range is from 1 to 127. Not support under IPv4 VRF address family mode.
as-set	if this option is set, the aggregate is advertised with a non-empty AS_PATH. If the AS_PATH of all contained routes is the same, the AS_PATH of the aggregate is the AS_PATH of the contained route. 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 aggregate routes.
summary-only	Filters all more-specific routes within the aggregate address and not being advertised to neighbors.

Default None

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.

Mode Router BGP Config Mode

IPv4 VRF Address Family

6.10.2.4. bgp aggregate-different-meds

Use **bgp aggregate-different-meds** command to allow aggregation of routes with different MED values. Use **no bgp aggregate-different-meds** command to disable this function.
When this command is issued, the path for an active aggregate address is advertised without a MED attribute. When this command is not issued, 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.

Format bgp aggregate-different-meds

no bgp aggregate-different-meds

Default Disable

All the routes aggregated by a given aggrerate address must have the same MED value.

Mode Router BGP Config Mode

IPv6 Address Family Config Mode

IPv4 VRF Address Family

6.10.2.5. bgp always-compare-med

Use **bgp always-compare-med** command to compare MED values in paths received from peers in different ASs. Use **no bgp always-compare-med** command to disable this function.

Format bgp always-compare-med

no bgp always-compare-med

Default Disable

MED values are only compared for paths received from peers in the same AS.

Mode Router BGP Config Mode

IPv6 Address Family Config Mode

IPv4 VRF Address Family

6.10.2.6. bgp bestpath as-path ignore

This command ignores the AS PATH length in the best path calculation during the decision process. For IPv6 routes, configure this command under the IPv6 Address Family Config mode.

To revert to the default behavior, where AS PATH length is not ignored in the BGP best path calculation, use the no form of this command.

Format bgp bestpath as-path ignore

no bgp bestpath as-path ignore

Default Disable

AS PATH length is not ignored in the BGP best path calculation.

Mode Router BGP Config Mode

IPv6 Address Family Config Mode

IPv4 VRF Address Family

6.10.2.7. bgp client-to-client reflection

Use this command to reflect routes received from its client ot its other clients. To disable client-to-client reflection, use the no form of this command.

Format bgp client-to-client reflection

no bgp client-to-client reflection

Default Enabled when a router is configured as a route reflector.

Mode Router BGP Config Mode

IPv6 Address Family Config Mode

IPv4 VRF Address Family

6.10.2.8. bgp cluster-id

Use this command to specify the cluster ID of a route reflector. The same cluster ID is used for both IPv4 and IPv6 route reflection. To revert the cluster ID to its default, use the no form of this command.

Format bgp cluster-id <cluster-id>

no bgp cluster-id

Fields	Definition
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 IPv4 address or as an integer. The range is from 1 to 4294967295.

Default Use BGP router ID as the cluster ID if a route reflector does not configure cluster ID.

Mode Router BGP Config Mode

IPv4 VRF Address Family

6.10.2.9. bgp default local-preference

This command changes the default local preference value. To return the local preference value to the default setting, use the no form of this command.

Format bgp default local-preference <number>

no bgp default local-preference

Fields	Definition
Number	Local preference value from 0 to 4294967295.

Default 100

Mode Router BGP Config Mode
IPv4 VRF Address Family

6.10.2.10. bgp fast-external-failover

This command configures Border Gateway Protocol (BGP) routing process to immediately reset external BGP peering sessions if the link used to reach these peers goes down. **no bgp fast-external-failover** command disables this function.

Format bgp fast-external-failover
no bgp fast-external-failover

Default Enabled

Mode Router BGP Config Mode
IPv4 VRF Address Family

6.10.2.11. bgp fast-internal-failover

This command configures Border Gateway Protocol (BGP) routing process to immediately reset internal BGP peering sessions if the link used to reach these peers goes down. **no bgp fast-internal-failover** command disables fast failover for internal peers.

Format bgp fast-internal-failover
no bgp fast-internal-failover

Default Enabled

Mode Router BGP Config Mode
IPv4 VRF Address Family

6.10.2.12. bgp log-neighbor-changes

This command enables logging of BGP neighbor resets . To disable the logging of changes in BGP neighbor adjacencies, use the **no** form of this command.

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 Establish state are logged at the Notice serverity level.

Format bgp log-neighbor-changes

no bgp log-neighbor-changes

Default Disabled

Mode Router BGP Config Mode

IPv4 VRF Address Family

6.10.2.13. bgp router-id

This command configures a valid IPv4 unicast address uniquely identifying the router bgp id. The <router-id> is a configured value. There is no default BGP router ID. The system does not select a router ID automatically and must configure one manually.

Format bgp <router-id>

no bgp <router-id>

Fields	Definition
router-id	An IPv4 address for BGP to use as its router ID. Not required to be an address assigned to the router. Setting the router ID to 0.0.0.0 disables BGP. Changing the router ID disables and re-enables BGP, which causes all adjacencies to be reestablished.

Default None

Mode Router BGP Config Mode

6.10.2.14. bgp maxas-limit

This command specifies Border Gateway Protocol (BGP) a limit on the length of AS PATHs that BGP accepts from its neighbors. If BGP receives a path whose AS PATH attribute is longer than the configured limit, BGP sends a NOTIFICATION and resets the adjacency. To return the router to default operation, use the no form of this command.

Format bgp maxas-limit <number>

no bgp maxas-limit

Fields	Definition
Number	Maximum number of autonomous system numbers in the AS PATH attribute of the BGP Update message, ranging from 1 to 100.

Default 75

Mode Router BGP Config Mode

IPv4 VRF Address Family

6.10.2.15. bgp graceful-restart

The user is able to enable BGP graceful restart enabled mode by command bgp graceful-restart in BGP router configuration mode. To disable the BGP graceful restart enabled mode, use no form of this command.

Format bgp graceful-restart

no bgp graceful-restart

Default Disable

Mode Router BGP Config Mode

6.10.2.16. bgp graceful-restart-helper

The user is able enable BGP graceful restart helper mode by command bgp graceful-restart-helper in BGP router configuration mode. To disable the BGP graceful restart helper mode, use no form of this command.

Format bgp graceful-restart-helper

no bgp graceful-restart-helper

Default Disable

Mode Router BGP Config Mode

6.10.2.17. bgp graceful-restart restart-time <restart-time>

The user is able configure BGP graceful restart helper restart timer by command bgp graceful-restart restart-time in BGP router configuration mode. To reset BGP graceful restart helper restart timer to default value, use no form of this command..

Format bgp graceful-restart restart-time <restart-time>

no bgp graceful-restart restart-time <restart-time>

Fields	Definition
Restart-time	The setting of the restart timer ranged from 1 to 3600. The timer is used by BGP GR aware node to decide whether restart operation of neighbor BGP GR enabled node is successful. The restart operation is considered failed if the BGP Aware node does not received BGP OPEN message from BGP enabled node after the timer expires.

Default 180 seconds

Mode Router BGP Config Mode

6.10.2.18. bgp graceful-restart stalepath-time <stalepath-time>

The user is able configure BGP graceful restart helper stale path timer by command bgp graceful-restart stalepath-time in BGP router configuration mode. To reset BGP graceful restart helper restart timer to default value, use no form of this command.

Format bgp graceful-restart stalepath-time <stalepath-time>

no bgp graceful-restart stalepath-time <stalepath-time>

Fields	Definition
Stalepath-time	The setting of the stale path timer ranged from 1 to 3600. The timer is used by BGP GR aware node to remove state routes learned from neighboring BGP GR enabled node after the timer expires.

Default 300 seconds

Mode Router BGP Config Mode

6.10.2.19. bgp listen

The user is able to activate dynamic neighbors feature and specify the maximum number of IPv4/IPv6 neighbors that can be created, IPv4/IPv6 prefix for listening range, as well as the peer template inherited by command bgp listen in BGP router configuration mode. To de-activate dynamic neighbors feature, use no form of this command.

Format bgp listen {limit <max-num>| range <prefix>/<prefix-length> [inherit peer <peer-template-name>] }

no bgp listen {limit <max-num>| range <prefix>/<prefix-length> [inherit peer <peer-template-name>] }

Fields	Definition
Maximum Peers	Maximum number of dynamic members in this VRF with specific address family. Number from 1 to 100. Default is 20.
Prefix/Length	Specify the listen range IP prefix and prefix length to be created.
Template	Specify the name of a BGP peer template 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.

Default No subnets are associated with a BGP listen subnet range, and the BGP dynamic neighbor feature is not activated.

Mode Router BGP Config Mode

IPv6 Address Family Mode

6.10.2.20. exit

This command is used to exit bgp configuration mode.

Format exit

Default None

Mode Router BGP Config Mode

6.10.2.21. timers bgp

This command is used to set the keepalive and holdtime timers. To return the router to default operation, use the no form of this command.

Format timers bgp <keepalive> <holdtime>

no timers bgp

Fields	Definition
Keepalive	The number of seconds this BGP speaker waits for a keepalive message before deciding that the connection is down. We recommend you configure the *keepalive* parameter as 1/3 of the *holdtime* parameter. The range is from 0 to 65535.
Holdtime	The number of seconds this BGP speaker waits for a keepalive, update, or notification message before deciding that the connection is down. We recommend you configure the holdtime parameter as 3 times the keepalive parameter. The range is from 0 to 65535.

Default The default value of **keepalive** is 60 seconds.

The default value of **holdtime** is 180 seconds.

Mode Router BGP Config Mode

IPv4 VRF Address Family

6.10.2.22. neighbor default-originate route-map

This command is used to originate a default route to a specific neighbor. Use the option *if-default-present* to originate the default route only if the default route exists in the routing table. The global default-originate command is overridden by the default-originate setting for a neighbor if enabled.

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.

To prevent BGP from originating a default route to a specific neighbor, use the no form of this command.

Format neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} default-originate [if-default-present] [route-map <route-map-name>]

no neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} default-originate [if-default-present] [route-map]

Fields	Definition
ipv4-address	IPv4 address of the neighboring router.
ipv6-address	IPv6 address of the neighboring router.
Interface	If the neighbor's IPv6 address is a link local address, the local interface must be specified as well.
autodetect interface	The routing interface on which the neighbor's IPv6 link local address is auto detected.
route-map-name	A route map may be configured to set attributes on the default route advertised to the neighbor.

Default No default route is originated by default.

Mode Router BGP Config Mode

IPv6 Address Family Config Mode

IPv4 VRF Address Family

6.10.2.23. neighbor inherit peer

This command is used to inherit neighbor configuration parameters from a peer template. 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. A neighbor can inherit directly from only one peer template.
To remove the inheritance, use the no form of this command.

Format neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} inherit peer <templatename>

no neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} inherit peer

Fields	Definition
ipv4-address	IPv4 address of the neighboring router.
ipv6-address	IPv6 address of the neighboring router. Not support under IPv4 VRF address family mode.
Interface	If the neighbor's IPv6 address is a link local address, the local interface must be specified as well. Not support under IPv4 VRF address family mode.
autodetect interface	The routing interface on which the neighbor's IPv6 link local address is auto detected.
Templatename	Name of the peer template whose peer configuration parameters are to be inherited by this neighbor.

Default None

Mode Router BGP Config Mode

IPv4 VRF Address Family

6.10.2.24. neighbor local-as

This command is used to advertise the configured local AS number instead of the router's own AS in the routes advertised to the neighbor. This command is only allowed on the external BGP neighbors.
To remove the local AS, use the no form of this command.

Format neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} local-as <as-number> no-prepend replace-as

no neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} local-as

Fields	Definition
ipv4-address	IPv4 address of the neighboring router.
ipv6-address	IPv6 address of the neighboring router. Not support under IPv4 VRF address family mode.
Interface	If the neighbor's IPv6 address is a link local address, the local interface must be specified as well. Not support under IPv4 VRF address family mode.
autodetect interface	The routing interface on which the neighbor's IPv6 link local address is auto detected.
As-number	The AS number to advertise as the local AS in the AS PATH sent to the neighbor.
no-prepend	Do not prepend the local-AS in the AS PATH received in the updates from this neighbor.
replace-as	Replace the router's own AS with the local-AS in the AS PATH sent to the neighbor.

Default None

Mode Router BGP Config Mode

IPv4 VRF Address Family

6.10.2.25. neighbor update-source

This command is used to configure BGP to use the IP address on the specific routing interface as the source address for the TCP connection with a neighbor.
To use the primary IP address on the outgoing interface to the neighbor for the TCP connection, use the no form of this command.

Format neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} update-source {<slot/port> | loop <loop interface number> | vlan <vlan id>} [encrypted]

no neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} update-source

Fields	Definition
ipv4-address	IPv4 address of the neighboring router.
ipv6-address	IPv6 address of the neighboring router. Not support under IPv4 VRF address family mode.
Interface	If the neighbor's IPv6 address is a link local address, the local interface must be specified as well. Not support under IPv4 VRF address family mode.
autodetect interface	The routing interface on which the neighbor's IPv6 link local address is auto detected.
slot/port	Valid slot and port number separated by forward slashes.
loop interface number	The valid value is from 0 to 63.
vlan id	The valid value is from 1 to 4093.

Default Disable

Use the primary IP address on the outgoing interface to the neighbor.

Mode Router BGP Config Mode

IPv4 VRF Address Family

6.10.2.26. neighbor description

This command is used to record a text description for a neighbor. This description is informational and has no functional impact.
To remove the description, use the no form of this command.

Format neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} description <description>

no neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} description

Fields	Definition
ipv4-address	IPv4 address of the neighboring router.
ipv6-address	IPv6 address of the neighboring router. Not support under IPv4 VRF address family mode.
Interface	If the neighbor's IPv6 address is a link local address, the local interface must be specified as well. Not support under IPv4 VRF address family mode.
autodetect interface	The routing interface on which the neighbor's IPv6 link local address is auto detected.
Description	Text (up to 80 characters) that describes the neighbor.

Default None

Mode Router BGP Config Mode

IPv4 VRF Address Family

6.10.2.27. neighbor ebgp-multihop

This command is used to form neighborship with non-directly-connected external neighbor with configured maximum hop-count allowed to reach it. For internal BGP neighbors, the TTL value remains 64 and cannot be modified. To make the *update-source* config work for external BGP neighbors, *ebgp-multihop* should be configured to increase the TTL value instead of the default TTL of 1.
To remove the neighborship, use the no form of this command.

Format neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} ebgp-multihop <hop-count>

no neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} ebgp-multihop

Fields	Definition
ipv4-address	IPv4 address of the neighboring router.
ipv6-address	IPv6 address of the neighboring router. Not support IPv4 VRF address family mode.
Interface	If the neighbor's IPv6 address is a link local address, the local interface must be specified as well. Not support IPv4 VRF address family mode.
autodetect interface	The routing interface on which the neighbor's IPv6 link local address is auto detected.

hop-count	The maximum hop-count allowed to reach the neighbor. The allowed range is from 1 to 255.

Default 1

Mode Router BGP Config Mode

IPv4 VRF Address Family

6.10.2.28. neighbor password

This command is used to enable Message Digest 5 (MD5) authentication on a TCP connection between two BGP peers and configures an authentication key. MD5 must either be enabled or disabled on both peers. The same password must be configured on both peers.

To disable this function, use the no form of this command.

Format neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} password [<string> encrypted]

no neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} password

Fields	Definition
ipv4-address	IPv4 address of the neighboring router.
ipv6-address	IPv6 address of the neighboring router. Not supported in the IPv4 VRF address family mode.
interface	If the neighbor's IPv6 address is a link local address, the local interface must be specified as well. Not supported in the IPv4 VRF address family mode.
autodetect interface	The routing interface on which the neighbor's IPv6 link local address is defined is auto-detected.
password	Use this option directly to set plain-text passwords with a maximum length of 25 characters. Use this option with the '<string> encrypted' parameter to set passwords in encrypted form with a length of 128 hexadecimal digits.

Default None

Mode Router BGP Config Mode

IPv4 VRF Address Family

6.10.2.29. neighbor connect-retry-interval

This command is used to configure the initial connection retry time for a specific neighbor. If a neighbor does not response to an initial TCP connection attempt, BGP retries three times. The first retry is after the retry interval configured with *neighbor connect-retry-interval*. Each subsequence 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 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.
To return the router to default initial connection retry time for a specific neighbor, use the no form of this command.

Format neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} connect-retry-interval <connection-retry-interval>

no neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} connect-retry-interval

Fields	Definition
ipv4-address	IPv4 address of the neighboring router.
ipv6-address	IPv6 address of the neighboring router.
Interface	If the neighbor's IPv6 address is a link local address, the local interface must be specified as well.
autodetect interface	The routing interface on which the neighbor's IPv6 link local address is auto detected.
connection-retry-interval	The valid range is 1 to 65535 seconds.

Default 2 seconds

Mode Router BGP Config Mode

IPv4 VRF Address Family

6.10.2.30. neighbor maximum-prefix

This command is used to limit how many prefixes can be received from a neighbor. The prefix limit is compared against the number of prefixes received from neighbor, including prefixes that are rejected by inbound policy. A neighbor that exceeds the limit is shutdown unless the *warning-log* option is configured.

To revert to the default value for the maximum number of prefixes that BGP will accept from a specific neighbor, use the no form of this command.

Format neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} maximum-prefix {<maximum> [<threshold>] [warning-only] | unlimited}

no neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} maximum-prefix

Fields	Definition
ipv4-address	IPv4 address of the neighboring router.
ipv6-address	IPv6 address of the neighboring router. Not support under IPv4 VRF address family mode.

Interface	If the neighbor's IPv6 address is a link local address, the local interface must be specified as well. Not support under IPv4 VRF address family mode.
autodetect interface	The routing interface on which the neighbor's IPv6 link local address is auto detected.
Maximum	Maximum number of prefixes BGP will accept from this neighbor. Range is from 0 to 4294967295.
Unlimited	Don't restric the number of prefixes from this neighbor.
Threshold	Integer specifying at what percentage of the maximum BGP starts to write log messages. The range is from 1 to 100.
warning-only	BGP only discards excess prefixes and writes a log message rather than shutting down the adjacency if BGP receives more than the maximum number of prefixes.

Default **Threshold**: default is 75

Mode Router BGP Config Mode

IPv6 Address Family Config Mode

IPv4 VRF Address Family

6.10.2.31. neighbor next-hop-self

This command is used to configure BGP to set the next hop attribute to a local IP address when advertising a route to an internal peer.

Normally BGP retains the next hop attribute received from the external peer. When the next hop attribute in routes from external peers is retained, internal peer must have a route to the external peer's IP address. This is commonly done by configuring the IGP on the boarder router to advertise the external subnet.

To disable this feature, use the no form of this command.

Format neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} next-hop-self

no neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} next-hop-self

Fields	Definition
ipv4-address	IPv4 address of the neighboring router.
ipv6-address	IPv6 address of the neighboring router. Not support under IPv4 VRF address family mode.
Interface	If the neighbor's IPv6 address is a link local address, the local interface must be specified as well. Not support under IPv4 VRF address family mode.
autodetect interface	The routing interface on which the neighbor's IPv6 link local address is auto detected.

Default None

Mode Router BGP Config Mode

IPv6 Address Family Config Mode

IPv4 VRF Address Family

6.10.2.32. neighbor filter-list

This command is used to filter 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 nonexisted AS path access list, all routes are filtered.

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.

To unconfigure neighbor filter lists, use the no form of this command.

Format neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} filter-list <listnum> {in | out}

no neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} filter-list <listnum> {in | out}

Fields	Definition
ipv4-address	IPv4 address of the neighboring router.
ipv6-address	IPv6 address of the neighboring router.
Interface	If the neighbor's IPv6 address is a link local address, the local interface must be specified as well.
autodetect interface	The routing interface on which the neighbor's IPv6 link local address is auto detected.
Listnum	Number to identify an AS path list. The range is from 1 to 500.
In	Access list is applied to advertisements received from the neighbor.
Out	Access list is applied to advertisements to be sent to the neighbor.

Default None

Mode Router BGP Config Mode

IPv6 Address Family Config Mode

IPv4 VRF Address Family

6.10.2.33. neighbor prefix-list

This command is used to filter advertisements sent to or receive from 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.

To remove an IP filter list, use the no form of this command.

Format neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} prefix-list <listname> {in | out}

no neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} prefix-list <listname> {in | out}

Fields	Definition
ipv4-address	IPv4 address of the neighboring router.
ipv6-address	IPv6 address of the neighboring router.
Interface	If the neighbor's IPv6 address is a link local address, the local interface must be specified as well.
autodetect interface	The routing interface on which the neighbor's IPv6 link local address is auto detected.
Listname	Name of a prefix list. The list defines which networks are to be received and which are to be suppressed in routing updates, based upon matching destination prefixes in the prefix list.
In	Access list is applied to advertisements received from the neighbor.
Out	Access list is applied to advertisements to be sent to the neighbor.

Default None

Mode Router BGP Config Mode

IPv6 Address Family Config Mode

6.10.2.34. neighbor remote-as

This command is used to configure a neighbor and identify 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.

To remove a neighbor, use the no form of this command.

Format neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} remote-as <as-number>

no neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} remote-as

Fields	Definition
ipv4-address	IPv4 address of the neighboring router.
ipv6-address	IPv6 address of the neighboring router.
Interface	If the neighbor's IPv6 address is a link local address, the local interface must be specified as well.
autodetect interface	The routing interface on which the neighbor's IPv6 link local address is auto detected.
As-number	Number of an autonomous system to which the neighbor belongs in the range from 1 to 4294967295.

Default None

Mode Router BGP Config Mode

6.10.2.35. neighbor remove-private-as

This command is used to remove private AS numbers when advertising routes to an external peer. 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 AS when removing or replacing private ASNs.

To stop removing private AS numbers, use the no form of this command.

Format neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} remove-private-as [all replace-as]

no neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} remove-private-as

Fields	Definition
ipv4-address	IPv4 address of the neighboring router.
ipv6-address	IPv6 address of the neighboring router. Not support under IPv4 VRF address family mode.
Interface	If the neighbor's IPv6 address is a link local address, the local interface must be specified as well. Not support under IPv4 VRF address family mode.
autodetect interface	The routing interface on which the neighbor's IPv6 link local address is auto detected.

all replace-as	To retain the original AS path length, replace each private AS number with the local AS number.

Default Private AS numbers are not removed by default

Mode Router BGP Config Mode

IPv6 Address Family Config Mode

IPv4 VRF Address Family

6.10.2.36. neighbor route-map

This command is used to apply a route map to incoming or outgoing routes for a specific neighbor. A route map can be used to change the local preference, MED, or AS path of a route.

To remove a route map, use the no form of this command.

Format neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} route-map <route-map-name> { in | out }

no neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} route-map <route-map-name> { in | out }

Fields	Definition
ipv4-address	IPv4 address of the neighboring router.
ipv6-address	IPv6 address of the neighboring router. Not support IPv4 VRF address family mode.
Interface	If the neighbor's IPv6 address is a link local address, the local interface must be specified as well. Not support IPv4 VRF address family mode.
autodetect interface	The routing interface on which the neighbor's IPv6 link local address is auto detected.
route-map-name	Identifier of a configured route map. The route map should be examined to filter the networks to be advertised/received.
In	Applies route map to incoming routes.
out	Applies route map to outgoing routes.

Default None

Mode Router BGP Config Mode

IPv6 Address Family Config Mode

IPv4 VRF Address Family

6.10.2.37. neighbor route-reflector-client

This command is used to configure an internal peer as an IPv4 route reflector client. Configuring the first route reflector client automatically makes this 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 *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 not inconsistent with other routers in the AS.

To remove a route map, use the no form of this command.

Format neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} route-reflector-client

no neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} route-reflector-client

Fields	Definition
ipv4-address	IPv4 address of the neighboring router.
ipv6-address	IPv6 address of the neighboring router. Not support under IPv4 VRF address family mode.
Interface	If the neighbor's IPv6 address is a link local address, the local interface must be specified as well. Not support under IPv4 VRF address family mode.
autodetect interface	The routing interface on which the neighbor's IPv6 link local address is auto detected.

Default Peers are not route reflector clients

Mode Router BGP Config Mode

IPv6 Address Family Config Mode

IPv4 VRF Address Family

6.10.2.38. neighbor shutdown

This command is used 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 learnt from that peer is purged. When an adjacency is administratively shutdown, the adjacency stays down until administratively re-enabled by using *no neighbor shutdown* command.

To administratively reenable the neighbor, use the no form of this command.

Format neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} shutdown

no neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} shutdown

Fields	Definition
ipv4-address	IPv4 address of the neighboring router.
ipv6-address	IPv6 address of the neighboring router. Not support IPv4 VRF address family mode.
Interface	If the neighbor's IPv6 address is a link local address, the local interface must be specified as well. Not support IPv4 VRF address family mode.
autodetect interface	The routing interface on which the neighbor's IPv6 link local address is auto detected.

Default Neighbors are not shutdown

Mode Router BGP Config Mode

IPv4 VRF Address Family

6.10.2.39. neighbor timers

This command is used to override the global timer values and set the keepalive and hold timers for a specific BGP peer. 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.

To revert the keep alive and hold time for a specific peer, use the no form of this command. After executing this command, the BGP peer must be reset before the changes take effect.

Format neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} timers <keepalive> <holdtime>

no neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} timers

Fields	Definition
ipv4-address	IPv4 address of the neighboring router.
ipv6-address	IPv6 address of the neighboring router. Not support under IPv4 VRF address family mode.
Interface	If the neighbor's IPv6 address is a link local address, the local interface must be specified as well. Not support under IPv4 VRF address family mode.
autodetect interface	The routing interface on which the neighbor's IPv6 link local address is auto detected.
Keepalive	Frequency (in seconds) with which the router sends keepalive messages to its peer. The range is from 0 to 65535.
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 this value, BGP drops the adjacency. If the hold time is set to 0, BGP does not enforce a hold time and does not send periodic KEEPALIVE messages. The range is from 0 to 65535.

Default The default value of <keepalive> is 60 seconds.

The default value of <holdtime> is 180 seconds.

Mode Router BGP Config Mode

IPv4 VRF Address Family

6.10.2.40. neighbor advertisement-interval

This command is used to configure the minimum time that must elapse between advertisement of the same route to a give neighbor. This value does not limit the rate of route selection but 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. The interval applies to withdrawals as well as advertisements.

To revert to the default minimum time that must elapse between advertisements of the same route to a given neighbor, use the no form of this command.

Format neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} advertisement-interval <seconds>

no neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} advertisement-interval

Fields	Definition
ipv4-address	IPv4 address of the neighboring router.
ipv6-address	IPv6 address of the neighboring router. Not support IPv4 VRF address family mode.
Interface	If the neighbor's IPv6 address is a link local address, the local interface must be specified as well. Not support IPv4 VRF address family mode.
autodetect interface	The routing interface on which the neighbor's IPv6 link local address is auto detected.
Seconds	The minimum time between route advertisement, in seconds. Range is from 0 to 600.

Default 30 seconds for external peers and 5 seconds for internal peers

Mode Router BGP Config Mode

IPv6 Address Family Config Mode

IPv4 VRF Address Family

6.10.2.41. neighbor send-community

This command is used to configure the router to send the BGP community attributes in Update messages to a specific neighbor.

To revert to default configuration, use the no form of this command.

Format neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} send-community

no neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} send-community

Fields	Definition
ipv4-address	IPv4 address of the neighboring router.
ipv6-address	IPv6 address of the neighboring router. Not support IPv4 VRF addres family mode.
Interface	If the neighbor's IPv6 address is a link local address, the local interface must be specified as well. Not support IPv4 VRF address family mode.
autodetect interface	The routing interface on which the neighbor's IPv6 link local address is auto detected.

Default The communities attribute is not sent to neighbors

Mode Router BGP Config Mode

IPv6 Address Family Config Mode

IPv4 VRF Address Family

6.10.2.42. neighbor send-community extended

This command is used to configure the router to send the BGP community attributes in Update messages to a specific neighbor. The BGP community attributes can be configurable.

To disable the exchange of VPNv4 prefixes with the neighbor, use the no form of this command.

Format neighbor <ipv4-address> send-community <extended | both>

no neighbor <ipv4-address> send-community <extended | both>

Fields	Definition
ipv4-address	IPv4 address of the neighboring router.
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.

Default The communities attribute is not sent to neighbors

Mode VPNv4 Address Family Config Mode

6.10.2.43. neighbor active

This command is used to enable exchange of IPv6 routes with a neighbor. The neighbor address must be the same IP address used in the neighbor remote-as command to create 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.

To disable exchange of IPv6 routes, use the no form of this command.

Format neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} activate

no neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} activate

Fields	Definition
ipv4-address	IPv4 address of the neighboring router.
ipv6-address	IPv6 address of the neighboring router. Not support under IPv4 VRF address family mode.
Interface	If the neighbor's IPv6 address is a link local address, the local interface must be specified as well. Not support under IPv4 VRF address family mode.
autodetect interface	The routing interface on which the neighbor's IPv6 link local address is auto detected.

Default None

Mode IPv6 Address Family Config Mode

IPv4 VRF Address Family

6.10.2.44. neighbor rfc5549-support

The enable advertisement of IPv4 routes over IPv6 next hops selectively to an external BGP IPv6 peer, use the command **neighbor rfc5549-support** in BGP Router Configuration mode. This command may only be applied to external BGP peers via single hop.

To disable advertisement/process of RFC 5549 routes for BGP neighbors, use the **no** form of the command.

Format neighbor {<ipv6-address> | autodetect interface <slot/port>} rfc5549-support

no neighbor {<ipv6-address> | autodetect interface <slot/port>} rfc5549-support

Fields	Definition
ipv6-address	IPv6 address of the neighboring router.
Autodetect interface <slot/port>	The routing interface on which the neighbor's link local IPv6 address is auto detected.

Default Enabled

Mode BGP Router Configuration Mode

6.10.2.45. distance

This command is used to set the preference (also known as administrative distance) of BGP routes to specific destinations. Up to 128 instances of this commands are allowed. 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 wildcard 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 change to the 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 routing table and relearned, either by resetting the peers from which the routes are learnt or by disabling and re-enabling BGP.

To return to the default values, use the no form of this command.

Format distance <1-255> [<peer-range> <wildcard-mask>] [prefix-list]

no distance <1-255> [<peer-range> <wildcard-mask>] [prefix-list]

Fields	Definition
1-255	The preference value for matching routes. The range is from 1 to 255.
peer-range, wildcard-mask	Routes learned from BGP peers whose address falls within this prefix are assigned the configured preference value. The wildcard-mask is an inverted network mask whose 1 bits indicate the don't care portion of the prefix.
prefix-list	A prefix list can optionally be specified to limit the preference value to a specific set of destination prefixes learned from matching neighbors.

Default BGP assigns preference values according to the *distance bgp* command, unless overridden for specific neighbors or prefixes by this command

Mode Router BGP Config Mode

6.10.2.46. distance bgp

This command is used to set the preference (also known as administrative distance) of BGP routes. Different distance values can be configured for routes learnt from external peers, routes learnt 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 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 routing table and relearned, either by resetting the peers from which the routes are learnt or by disabling and re-enabling BGP.

To return to the default values, use the no form of this command.

Format distance bgp <external-distance> <internal-distance> <local-distance>

no distance bgp

Fields	Definition
external-distance	The preference value for routes learnt from external peers. The range is from 1 to 255.
internal-distance	The preference value for routes learnt from internal peers. The range is from 1 to 255.
local-distance	The preference value for locally-originated routes. The range is from 1 to 255.

Default external-distance: 20

internal-distance: 200

local-distance: 200

Mode Router BGP Config Mode

IPv6 Address Family Config Mode

IPv4 VRF Address Family

6.10.2.47. default-information originate

This command is used to allow BGP to originate a default route. By default, BGP does not originate a defatul route. If a default route is redistributed into BGP, BGP does not advertise the default route unless this command is issued. To disable this function, use the no form of this command.

Format default-information originate <always>

no default-information originate

Fields	Definition
<always>	Originate a default route even if routing table doesn't have one. Disable by default.

Default Disable

Mode Router BGP Config Mode
IPv6 Address Family Config Mode
IPv4 VRF Address Family

6.10.2.48. maximum-paths

This command is used to configure the maximum number of next hops BGP may include in an Equal Cost Multipath (ECMP) route derived from paths received from neighbors within or outside the local AS.

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.

To restore the default value, use the no form of this command.

Format maximum-paths [ibgp] <number>
no maximum-paths [ibgp] <number>

Fields	Definition
Ibgp	Specifies the maximum number of next hops in a BGP route derived from paths received from neighbors withint the local AS.
Number	Specifies the maximum number of next hops in a BGP route. The range is from 1 to 32.

Default Single next hop

Mode Router BGP Config Mode
IPv6 Address Family Config Mode
IPv4 VRF Address Family

6.10.2.49. default-metric

This command is used to configure the value of the Multi Exit Discriminator (MED) attribute for routes redistributed into Border Gateway Protocol (BGP) when no metric has been specified in the command *redistribute* for BGP. To delete the default for the metric of redistributed routes, use the no form of this command.

Format default-metric <number>

no default-metric

Fields	Definition
<number>	Default metric value applied to the redistributed route. The range of values for this argument is from 1 to 4294967295.

Default No default metric is set and no MED is included in redistributed routes

Mode Router BGP Config Mode

IPv6 Address Family Config Mode

IPv4 VRF Address Family

6.10.2.50. redistribute

This command is used to redistribute routes from outside into BGP routing domain. BGP can redistribute local (connected), static, and OSPF routes.

A default route cannot be redistributed unless the *default-information originate* command is issued.

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.

To disable redistribution, use the no form of this command.

Format redistribute <protocol> [metric <0-4294967295>] [match {internal | external 1 | external 2 | nssa-external 1 | nssa-external 2}] [route-map <route-map-name>]

no redistribute <protocol> [metric] [match {internal | external 1 | external 2 | nssa-external 1 | nssa-external 2}] [route-map <route-map-name>]

Fields	Definition
Protocol	Source protocol from which routes are being redistributed. It can be one of the following keywords: connected, ospf, static, connected.
metric <0-4294967295>	When this option is specified, BGP advertises the prefix with the MED path attribute set to the configured value. If this option is not specified but a default metric is configured by *default-information originate* command, the MED is set to the default metric. If a default metric is not configured, the prefix is advertised without a MED attribute.
Match	Use this option to redistribute specific types of OSPF routes.
route-map-name	Identifier of a configured route map. The route map should be examined to filter the networks to be redistributed. A route map can be used to set attributes on redistribution routes.

Default BGP redistributes no route

Mode Router BGP Config Mode
IPv6 Address Family Config Mode
IPv4 VRF Address Family

6.10.2.51. distribute-list in

This command is used to filter routes received in incoming Border Gateway Protocol (BGP) updates 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 which does not exist, the command is accepted and all routes are permitted.

To disable the filter, use the no form of this command.

Format distribute-list prefix <list-name> in
no distribute-list prefix <list-name> in

Fields	Definition
list-name	Name of a prefix list. The list defines which networks are to be received and which are to be suppressed in routing updates, based upon matching destination prefixes in the prefix list.

Default None

Mode Router BGP Config Mode
IPv4 VRF Address Family

6.10.2.52. distribute-list out

This command is used 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 (connected, OSPF, or static). One instance of this command may also be configured as a global filter for outbound prefixes. If the command refers to a prefix list which 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.

To disable the filter, use the no form of this command.

Format distribute-list prefix <list-name> out [connected | ospf | static]
no distribute-list prefix <list-name> out [connected | ospf | static]

Fields	Definition
list-name	Name of a prefix list. The list defines which networks are to be received and which are to be suppressed in routing updates, based upon matching destination prefixes in the prefix list.

connected | ospf | static	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.

Default None

Mode Router BGP Config Mode
IPv4 VRF Address Family

6.10.2.53. ip bgp fast-external-failover {deny|permit}

This command configures fast external failover behavior for a specific routing interface. This command overrides the global configured fast external failover behavior. If permit is specified, the feature is enabled on the interface, regardless of the global configuration. If the deny is specified, the feature is disabled on the interface, regardless of the global configuration.

To disable the filter, use the no form of this command.

Format ip bgp fast-external-failover {deny | permit}
no ip bgp fast-external-failover

Fields	Definition
Permit	Enable fast external failover on the interface, regardless of the global configuration of the fearture.
Deny	Disable fast external failover on the interface, regardless of the global configuration of the fearture.

Default None

Mode Interface Config

6.10.2.54. network

This command is used 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.

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. If there is no route map with the name given, the network is not advertised.

To disable BGP from advertising an address prefix, use the no form of this command.

Format network <ipaddress> mask <mask> [route-map <route-map-name>]

no network <ipaddress> mask <mask> [route-map <route-map-name>]

Fields	Definition
Ipaddress	An address prefix that BGP will advertise.
Mask	Network mask for the prefix.
route-map-name	Identifier of a configured route map. The route map should be examined to filter the networks to be advertised.

Default No networks are advertised

Mode Router BGP Config Mode

IPv4 VRF Address Family

6.10.2.55. network <ipv6-prefix>/<prefix-length>

This command is used to advertise an IPv6 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.

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. If there is no route map with the name given, the network is not advertised.

To disable BGP from advertising an IPv6 prefix, use the no form of this command.

Format network <ipv6-prefix>/<prefix-length> [route-map <route-map-name>]

no network <ipv6-prefix>/<prefix-length>

Fields	Definition
ipv6-prefix	An IPv6 prefix that BGP will advertise.
prefix-length	The prefix length of the IPv6 prefix.
route-map-name	Identifier of a configured route map. The route map should be examined to filter the networks to be advertised.

Default No networks are advertised

Mode IPv6 Address Family Config Mode

6.10.2.56. template peer

This command is used to create a BGP peer template and enter BGP peer template mode for the specified template. Peer template is a configuration feature that allows you to share policies between neighbors. 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.

To delete a peer template, use the no form of this command.

Format template peer <template name>

no template peer <template name>

Fields	Definition
template name	Name of the peer template. The name may be no more than 32 characters.

Default None

Mode Router BGP Config Mode

6.10.2.57. clear ip bgp

This command is used to 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.

Format clear ip bgp { [vrf <vrf-name>] {* [soft [in | out]] | <1-4294967295> | <neighbor-address> [[interface {<slot/port> | vlan <1-4093>}] soft [in | out]] | counters } } | interface {<slot/port> | vlan <1-4093>} [soft [in | out]] | listen range <prefix>/<prefix-length> [soft [in | out]]

***** Resets adjacency with every BGP peer.

Fields	Definition
vrf-name	Display the BGP route table whithin a VRF instance.
1-4294967295	Specify the BGP peer's AS number for which the adjacency will be reset.
neighbor-address	Sepcify the IPv4 and IPv6 address of the peer for which the adjacency will be reset.
Interface	Specify the interface for IPv6 link local peer address for which the adjacency will be reset.
listen range	The IP address range to listen BGP peers.
prefix/prefix-length	Specify the listen range IP prefix and prefix length to be created.

Soft	By default, adjacencies are torn down and re-established. If this option is specified, RGP resends all updates to neighbors and reprocesses updates from the neighbors.
in/out	If the **in** option is given, updates from the neighbors are reprocessed. If the **out** option is given, updates are resent to the neighbors. If neither keywords is given, updates are reprocessed in both directions.

Default None

Mode Privileged EXEC
User EXEC

6.10.2.58. clear ip bgp counters

This command is used to resets all BGP counters to 0. These counters include send and receive packet and prefix counters for all neighbors.

Format Clear ip bgp counters

Default None

Mode Privileged EXEC
User EXEC

6.10.2.59. ip as-path access-list

This command is used to create an AS path access list. An AS path access list filters BGP routes on the AS PATH attribute of a BGP route. 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 as 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 statement 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.

128 AS path access lists are allowed to be configured 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.

To delete an AS path access list, use the no form of this command.

Format ip as-path access-list <1-500> <deny | permit> <regexp>

no ip as-path access-list <1-500>

Fields	Definition
1-500	A number uniquely identifying the list. All AS path access list commands with the same this number are considered part of the same list.
Permit	Permit the routes whose AS PATH attribute matches the regular expression.
Deny	Deny the routes whose AS PATH attribute matches the regular expression.
Regexp	A regular expression used to match the AS PATH attribute of a BGP route where the AS path is treated as an ASCII string. **AS path regular expression syntax:** **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. **period(.):** Matches any single character, including white space. **question mark(?):** Matches 1 or more 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.

Default None

Mode Global Config

6.10.2.60. ip bgp-community new-format

This command is used to display BGP standard communities in the new format AA:NN. The new format displays a community number as the ASN followed by a 16-bit AS-specific number.

To display BGP standard communities as 32-bit integers, use the no form of this command.

Format ip bgp-community new-format

no ip bgp-community new-format

Default None

Mode Global Config

6.10.2.61. ip community-list

This command is used to create or configure a BGP community list. 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 standard testlist 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 *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.

To delete a community list, use the no form of this command.

Format ip community-list standard <list-name> {permit | deny} [community] [no-advertise] [no-export] [no-export-subconfed] [no-peer]

no ip community-list standard <list-name>

Fields	Definition
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	Specify a community number formatted as a 32-bit integers or in AA:NN format, where AA is a 2-byte AS number and NN is a 16 bit integer. The range is from 1 to 4294967295 (any 32-bit integer other than 0). Communities are separated by spaces.
no-advertise	Specify the routes that are not advertised to any peer.
no-export	Specify the routes that are not exported outside of the local AS.
no-export-subconfed	Specify the routes that are not exported to other external peers.
no-peer	Specify the routes that are not exported to other peers.

Default None

Mode Global Config

6.10.2.62. show ip as-path-access-list

This command is used to display the contents of AS path access lists.

Format show ip as-path-access-list [<0-500>]

Fields	Definition
0-500	When an AS path list number is specified, the output is limited to the single AS path list specified.

Default None

Mode Privileged EXEC
User EXEC

6.10.2.63. show ip community-list

This command is used to display community lists. The format of community values is dictated by the command *ip bgp-community new-format*.

Format show ip community-list [detail] [<listname>]

Fields	Definition
listname	A standard community list name. This option limits the output to a single list.
detail	Specify to show statistics about community lists.

Default None

Mode Privileged EXEC
User EXEC

6.10.2.64. clear ip community-list

This command is used to clear community lists.

Format clear ip community-list [<list-name>]

Fields	Definition
listname	Specify a community list name to be cleared.

Default None

Mode Privileged EXEC
User EXEC

6.10.2.65. rd

This command is used to specify the route distinquisher (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 distinquisher for a VPN. The RD is added to the beginning of the IPv4 prefixes to change them into globally unique VPNv4 prefixes.

Format rd {route-distinquisher}

Fields	Definition
route-distinquisher	A route distinquisher can be specified in either of the following formats: ● 2-byte ASN-related: Composed of an automonous system number and an arbitraty number: <as-number>:<value> ● 4-byte ASN-related: Composed of an 4-byte automonous system number and an arbitraty number: <as-number>:<value> ● IP address-related: Composed of an IP address and an arbitrary number: <ip-address>:<value>

Default A VRF does not associate with any RD

Mode Virtual Router Config

i This command is effective only if BGP is running on the router. The RD for a VRF cannot be removed or changed once configured. 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.

6.10.2.66. route-target

This command is used 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.

Use no form to remove the route target specified for a VRF instance.

Format route-target {export | import | both} {route-target}

no route-target {export | import | both} {route-target}

Fields	Definition
export	Exports routing information to the target VPN extended community.

Import	Imports routing information from the target VPN extended community.
Both	Exports/imports routing information to/from the target VPN extended community.
route-target	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 distinquisher, the route-target extended community can be specified in one of the following formats: ● 2-byte ASN-related: Composed of an automonous system number and an arbitraty number: <as-number>:<value> ● 4-byte ASN-related: Composed of an 4-byte automonous system number and an arbitraty number: <as-number>:<value> ● IP address-related: Composed of an IP address and an arbitrary number: <ip-address>:<value>

Default A VRF does not associate with any RT

Mode Virtual Router Config

i This command is effective only if BGP is running on the router.

6.10.2.67. address-family ipv4

This command is used to enter IPv4 VRF Address Family Configuration mode to configure BGR VRF parameters. 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.

To return to the default values, use the no form of this command.

Format address-family ipv4 vrf <vrf-name>

no address-family ipv4 vrf <vrf-name>

Fields	Definition
vrf-name	Specify the name of the VRF instance.

Default VRF configuration is disabled

Mode Router BGP Config Mode

6.10.2.68. address-family ipv6

This command is used to enter IPv6 Address Family Configuration mode in order to specify IPv6-specific configuration parameters. 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.

To return to the default values, use the no form of this command.

Format address-family ipv6

no address-family ipv6

Default Exchange of IPv6 routes is disabled

Mode Router BGP Config Mode

6.10.2.69. address-family vpnv4

This command is used to 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 both
• neighbor ip-address send-community extended

To return to the default values, use the no form of this command.

Format address-family vpnv4 unicast

no address-family vpnv4 unicast

Default The VPNv4 address family is disabled

Mode Router BGP Config Mode

6.10.2.70. neighbor allowas-in

This command is used 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.

To return to the default values, use the no form of this command.

Format neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} allowas-in <count>

no neighbor {<ipv4-address> | <ipv6-address> [interface {<slot/port> | vlan {1-4093}}] | autodetect interface <slot/port>} allowas-in

Fields	Definition
Count	The maximum number of occurrences of the local ASN allowed in the AS_PATH attribute received in the prefix updates. The range is 1 to 10.

Default Disabled

Mode Router BGP Config Mode

6.11. VRRPv3 Commands

VRRPv3 provides address redundancy for both IPv4 and IPv6 router addresses. VRRPv3 support on the switch 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-localIPv6 address too
The interval time used for sending VRRP Advertisement packets is in seconds	The interval time is in the order of milliseconds
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}

i VRRPv2 configuration cannot be modified under VRRPv3 enabled mode.

6.11.1. Show commands

6.11.1.1. 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>]]

Default None

Mode Privileged Exec

Display Message

Fields	Definition
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 Virutal router belongs.
vlan-id	(Optional) indicates the VLAN number to which the Virtual router belongs.
vrid	(Optional) Virtual router group number. The range is from 1 to 255.

Example:

```
(IX2) (config-if-vrrp)#show vrrp

vlan 2 - VRID 2 - Address-Family IPv4

Virtual IP address.............................. 192.168.2.254
Secondary IP Address(es).......................
Virtual MAC Address............................. 00:00:5e:00:01:02
Priority........................................ 100
Configured Priority............................. 100
Advertisement Interval.......................... 100 millisecs
Pre-empt Mode................................... Enable
Accept Mode..................................... Disable
Administrative Mode............................. Enable
State........................................... Master
Master Router IP / Priority..................... 192.168.2.250 / 100
Master Advertisement interval................... 100 millisecs
Master Down interval............................ 300 millisecs

Track Interface State DecrementPriority
--------------- ----- ------------------

Track Route(pfx/len)   Reachable  DecrementPriority
---------------------  ---------  ------------------

(IX2) (config-if-vrrp)#
```

6.11.1.2. show vrrp brief

This command displays brief information for all active VRRPv3 groups.

Format show vrrp brief

Default None

Mode Privileged Exec

Display Message

Fields	Definition
Interface	Interface on which VRRP is configured.
VRID	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:

```
(IX8D) (Config)#show vrrp brief
Interface   VRID A-F  Pri AdvIntvl Pre Acc State  VR IP Address
----------- ---- ---- --- -------- --- --- ------ -------------
0/1         1    IPv4 100 1        N   N   Backup 10.255.255.123
```

6.11.1.3. 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>} <vr-id>]

Default None

Mode Privileged Exec

Display Message

Fields	Definition
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:

```
(IX8D) (Config)#show vrrp statistics ipv4 0/1 1

Master Transitions.............................. 0
New Master Reason............................... notMaster(0)
Advertisements Received......................... 153317
Advertisements Sent............................. 0
Advertisement Interval Errors................... 0
IP TTL Errors................................... 0
Last Protocol Error Reason...................... noError(0)
Zero Priority Packets Received.................. 0
Zero Priority Packets Sent...................... 0
Invalid Type Packets Received................... 0
Address List Errors............................. 0
Packet Length Errors............................ 0
Row Discontinuity Time.......................... 0 days 0 hrs 0 mins 0 secs
Refresh Rate (in milliseconds).................. 0
```

6.11.2. Configuration commands

6.11.2.1. 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.

To disable the VRRPv3 and enable VRRPv2 in the router, use the **no** form of this command.

Format fhrp version vrrp v3
no fhrp version vrrp v3

Default Disabled

Mode Global Config

6.11.2.2. vrrp

This command creates a VRRPv3 group and enters VRRPv3 group configuration mode.
To remove the specified VRRPv3 group, use the **no** form of this command. Before you can use this command, you must disable Virtual Router using the shutdown command in the appropriate VRRP Config mode

Format vrrp <group-id> address-family {ipv4 | ipv6}
no vrrp <group-id> address-family {ipv4 | ipv6}

Fields	Definition
<group-id>	The virutal router group number. The range is from 1 to 255.
address-family	Specifies the address family for the VRRP.
ipv4	(Optional) Specifies IPv4 address.
ipv6	(Optional) Specifies IPv6 address.

Default None

Mode Interface Config

6.11.2.3. preempt

This command configures the device to take over as master virtual router for a VRRP group if it has higher priority than the current master virtual route.
To prevent the device from taking over as master virtual router for a VRRP group if it has higher priority than the current master virtual route, use the **no** form of this command.

Format preempt [delay minimum <centiseconds>]
no preempt

Fields	Definition
<centiseconds>	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.

Default Enabled with default delay value of 0

Mode VRRPv3 Config

6.11.2.4. accept-mode

This command controls 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.
To reset the accept mode to the default value, use the no form of this command.

Format accept-mode
no accept-mode

Default Disabled

Mode VRRPv3 Config

6.11.2.5. priority

This command sets the priority level of the device within a VRRPv3 group. The priority level controls which device becomes the master virtual router.
To reset the priority level of the device to the default value, use the no form of this command.

Format priority <level>

no priority

Fields	Definition
level	Priority of the device within the VRRP group. The range is from 1 to 254.

Default 100

Mode VRRPv3 Config

6.11.2.6. timers advertise

This command configures the interval between successive advertisements by the master virtual router in a VRRP group.
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.
To restore the default value, use the no form of this command.

Format timers advertise <milliseconds>

no timers advertise

Fields	Definition
milliseconds	Time interval between successive advertisements by the master virtual router. The unit of the interval is in 100 milliseconds. The valid range is 100 to 40000 milliseconds

Default 1 (100 milliseconds)

Mode VRRPv3 Config

6.11.2.7. shutdown

This command disables the VRRP group configuration.
To enable and update the virtual router state after completing configuration.restore the default value, use the no form of this command.

Format shutdown

no shutdown

Default shutdown

Mode VRRPv3 Config

6.11.2.8. address

This command set the primary or secondary IP address of the device within a VRRPv3 group.
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.
To remove the secondary address, use the no form of this command.

Format address <ip-address> [primary | secondary]

no address <ip-address> secondary

Fields	Definition
ip-address	IPv4 or IPv6 address You can specify an IPv4 address in the following format: *ipv4-address* You can specify an IPv6 address in the following format: *ipv6-link-local-address*
primary	(Optional) Set primary IP address of the VRRPv3 group.
secondary	(Optional) Set additional IP address of the VRRPv3 group.

Default None

Mode VRRPv3 Config

6.11.2.9. track interface

This command configures tracking of the interface for the device within a VRRPv3 group. Once interface tracking is configured, the VRRPv3 feature receives notifications when the interface 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 interface goes down.
To disable tracking of the interface for the device within a VRRPv3 group, use the no form of this command.

Format track interface {<slot/port> | vlan <vlan-id>} [decrement number]

no track interface {<slot/port> | vlan <vlan-id>} [decrement number]

Fields	Definition
slot/port	The interface to track.
vlan-id	The VLAN to track.
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.

Default Disabled (the default of the decrement number is 10)

Mode VRRPv3 Config

6.11.2.10. track ip route

This command configures 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.
To disable tracking of IP route for the device within a VRRPv3 group, use the no form of this command.

Format track ip route <ip-address/prefix-len> [decrement number]

no track ip route <ip-address/prefix-len> [decrement number]

Fields	Definition
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.

Default None (the default of the decrement number is 10)

Mode VRRPv3 Config

6.11.2.11. clear vrrp statistics

This command clears 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>} <vr-id>]

Fields	Definition
ipv4	(Optional) The Virtual router group belongs to IPv4 address family.

ipv6	(Optional) The Virtual router group belongs to IPv6 address family.
slot/port	(Optional) The interface number to which the Virtual router belongs.
vlan-id	(Optional) The VLAN number to which the virtual router belongs. The range is from 1 to 4093.
vr-id	(Optional) The virtual router group number. The range is from 1 to 255.

Mode Privileged Exec

6.12. Virtual Router Commands

6.12.1. Show commands

6.12.1.1. show ip vrf

This command shows the information about the virtual router instances.

Format show ip vrf [{<vrf-name> | detail <vrf-name> | interfaces | memory [<vrf-name>]}]

Default None

Mode Privileged Exec

Display Message

Fields	Definition
vrf-name	Name of the virtual router instance
detail	Displays the configuration and status of the specified 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

6.12.2. Configuration commands

6.12.2.1. ip vrf

Use this command to create a virtual router with a specified name and enters VRF configuration mode. Alternatively, you can use *no ip vrf* command to delete the virtual router with the specified name.

Format ip vrf <vrf-name>

no ip vrf <vrf-name>

Fields	Definition
vrf-name	The name of the virtual router. The name is a string of up to 64 characters from an ASCII set.

Default No VRs are defined

Mode Global Config

6.12.2.2. maximum routes

Use this command to reserve 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.
Alternatively, you can use *no maximum routes* command to remove any reservation for the number of routes allowed in the virtual router instance and clears the warning threshold value.

Format maximum routes {<limit> | warn <threshold>}

no maximum routes [warn]

Fields	Definition
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.
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.

Default Limited by the number of free routes available

Mode Virtual Router Config

6.12.2.3. description

Use this command to configure a descriptive text for a virtual router.
Alternatively, you can use *no description* command to remove the descriptive text configuration for a virtual router.

Format description text

no description

Fields	Definition
text	The descriptive text for the virtual router. A set of ASCII characters up to 512 characters in length.

Default None

Mode Virtual Router Config

6.12.2.4. ip vrf forwarding

Use this command to associate a routing interface with a virtual router.
Alternatively, you can use *no ip vrf* command to disassociate a routing interface from the configured virtual router and associates it back to the default virtual router.

Format ip vrf forwarding <vrf-name>

no ip vrf forwarding

Fields	Definition
vrf-name	The name of the virtual router.

Default Default virtual router

Mode Interface Config

6.13. Black Hole Detection (BHD) Commands

In networking terms, *black holes* refer to the 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.

6.13.1. Show commands

6.13.1.1. show bhd status

This command shows the global configuration of black hole detection feature along with the list of ports enabled for BHD.

Format show bhd status

Default None

Mode Privileged Exec

Display Message

Fields	Definition
Spine port	The ports enabled for BHD
BHD Count	Displays the BHD packet counts

6.13.2. Configuration commands

6.13.2.1. bhd spine-port enable

Use this command to enable the port to be monitored for black hole detection. Only port-based routing interface can be enabled as BHD spine ports. Alternatively, you can use *no bhd spine-port enable* command to disable the port to be monitored for black hole detection.

Format bhd spine-port enable

no bhd spine-port enable

Default Disabled

Mode Interface Config

6.13.2.2. bhd enable

Use this command to enable the BHD feature globally on the system.
Alternatively, you can use *no bhd enable* command to disable the BHD feature globally on the system.

Format bhd enable

no bhd enable

Default Disabled

Mode Global Config

6.13.2.3. clear counter bhd

Use this command to clear the counters of BHD.

Format clear counters bhd

Default None

Mode Privileged Exec

6.14. IP Event Dampening Commands

6.14.1.1. 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]]

no dampening

Mode Interface Config

Parameter	Definition
Half-life period	The numbe 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 1-20000. 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 1-20000. Default value is 2000.

6.14.1.2. 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 examples of the command.

```
(Router)# show dampening interface

2 interfaces are configured with dampening.

1 interface is being suppressed.
```

7. IP Multicast Commands

7.1. Internet Group Management Protocol (IGMP) Commands

This section provides a detailed explanation of the IGMP commands. The commands are divided into the following different groups:

Show commands are used to display device settings, statistics and other information.

Configuration commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.

7.1.1. Show commands

7.1.1.1. show ip igmp

This command displays the system-wide IGMP information.

Format show ip igmp

Default None

Mode Privileged EXEC
User EXEC

Display Message

Fields	Definition
IGMP Admin Mode	This field displays the administrative status of IGMP. This is a configured value.
IGMP Router-Alert check	This field displays the administrative status of Router-Alert validation for IGMP packets.
Interface	Valid slot and port number separated by forward slashes.
Interface Mode	This field indicates whether IGMP is enabled or disabled on the interface. This is a configured value.
Operational-Status	This field indicates the current state of IGMP on this interface. Possible values are Operational or Non-Operational.

7.1.1.2. show ip igmp groups

This command displays the registered multicast groups on the interface. If “detail” is specified this command displays the registered multicast groups on the interface in detail.

Format show ip igmp groups {<slot/port> | vlan <vlan-id> | loopback <0-63>} [detail]

Fields	Definition
<slot/port>	Valid slot and port number separated by forward slashes.
<vlan-id>	VLAN ID. The range of VLAN ID is from 1 to 4093.
<loopback>	Loopback interface number. The range of Loopback interface is from 0-63.
[detail]	Display details of subscribed multicast groups.

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
IP Address	This displays the IP address of the interface participating in the multicast group.
Subnet Mask	This displays 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:*
Querier Status	This displays whether the interface has IGMP in Querier mode or Non-Querier mode.
Groups	This displays the list of multicast groups that are registered on this interface. *If detail is specified, the following fields are displayed:*
Multicast IP Address	This displays the IP Address of the registered multicast group on this interface.
Last Reporter	This displays the IP Address of the source of the last membership report received for the specified multicast group address on this interface.
Up Time	This displays the time elapsed since the entry was created for the specified multicast group address on this interface.
Expiry Time	This displays the amount of time remaining to remove this entry before it is aged out.
Version1 Host Timer	This displays 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	This displays 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 Compatibilty Mode	The group compatibility mode (v1, v2 or v3) for this group on the specified interface.

7.1.1.3. show ip igmp interface

This command displays the IGMP information for the interface.

Format show ip igmp interface {<slot/port> | vlan <vlan-id> | loopback <0-63>}

Fields	Definition
<slot/port>	Valid slot and port number separated by forward slashes.
<vlan-id>	VLAN ID. The range of VLAN ID is from 1 to 4093.
<loopback>	Loopback interface number. The range of Loopback interface is from 0-63.
<multicast-group>	The IP address of the multicast group.

Default None

Mode Privileged EXEC
User EXEC

Display Message

Fields	Definition
Interface	Valid slot and port number separated by forward slashes.
IP Address	This displays the IP address of the interface participating in the multicast group.
Subnet Mask	This displays the subnet mask of the interface participating in the multicast group.
IGMP Admin Mode	This field displays the administrative status of IGMP. This is a configured value
Interface Mode	This field indicates whether IGMP is enabled or disabled on the interface. This is a configured value.
IGMP Version	This field indicates 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 (secs)	This field indicates the frequency at which IGMP Host-Query packets are transmitted on this interface. This is a configured value.
Query Max Response Time (secs)	This field indicates the maximum query response time advertised in IGMPv2 queries on this interface. This is a configured value.
Robustness	This field displays 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. This is a configured v. alue.
Startup Query Interval (secs)	This value indicates the interval between General Queries sent by a Querier on startup. This is a configured value.
Startup Query Count	This value is the number of Queries sent out on startup, separated by the Startup Query Interval. This is a configured value.
Last Member Query Interval (secs)	This value indicates the Maximum Response Time inserted into Group-Specific Queries sent in response to Leave Group messages. This is a configured value
Last Member Query Count	This value is the number of Group-Specific Queries sent before the router assumes that there are no local members. This is a configured value.

7.1.1.4. 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]

Fields	Definition
<multiipaddr>	A multicast IP address.
[detail]	Display details of subscribed multicast groups.

Default None

Mode Privileged EXEC

User EXEC

Display Message

Fields	Definition
Interface	Valid slot and port number separated by forward slashes.
Interface IP	This displays the IP address of the interface participating in the multicast group.

State	This displays whether the interface 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 detail is specified, the following fields are displayed:

Fields	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.
Source Hosts	This displays 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	This displays the amount of time remaining to remove this entry before it is aged out. This is "- ----" for IGMPv1 and IGMPv2 Membership Reports.

7.1.1.5. show ip igmp interface stats

This command displays the IGMP statistical information for the given interface. The statistics are only displayed when the interface is enabled for IGMP.

Format show ip igmp interface stats {<slot/port> | vlan <vlan-id> | loopback<0-63>}

Fields	Definition
<slot/port>	Valid slot and port number separated by forward slashes.
<vlan-id>	VLAN ID. The range of VLAN ID is from 1 to 4093.
<loopback>	Loopback interface number. The range of Loopback interface is from 0-63.

Default None

Mode Privileged EXEC

User EXEC

Display Message

Fields	Definition
Querier Status	This field indicates the status of the IGMP router, whether it is running in Querier mode or Non-Querier mode.
Querier IP Address	This field displays the IP Address of the IGMP Querier on the IP subnet to which this interface is attached.
Querier Up Time	This field indicates the time since the interface Querier was last changed.
Querier Expiry Time	This field displays 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	This field indicates the number of queries received whose IGMP version does not match the IGMP version of the interface.
Number of Joins Received	This field displays the number of times a group membership has been added on this interface.
Number of Groups	This field indicates the current number of membership entries for this interface.

7.1.2. Configuration commands

7.1.2.1. ip igmp

This command sets the administrative mode of IGMP in the router to active. To set the administrative mode of IGMP in the router to inactive, use the no form of this command.

Format ip igmp
no ip igmp

Default Disable

Mode Global Config
Interface Config

7.1.2.2. ip igmp router-alert-check

This command is used to enables Router-Alert validation for IGMP packets.

To disables Router-Alert validation for IGMP packets, use the no form of this command.

Format ip igmp router-alert-check

no ip igmp router-alert-check

Default Disable

Mode Global Config

7.1.2.3. ip igmp version

This command configures the version of IGMP for an interface.

To reset the version of IGMP for this interface to the default value, use the no form of this command.

Format ip igmp version {1 | 2 | 3}

no ip igmp version

Fields	Definition
<1- 3>	The IGMP version number.

Default 3

Mode Interface Config

7.1.2.4. ip igmp last-member-query-count

This command sets the number of Group-Specific Queries sent by the interface before the router assumes that there are no local members on the interface.

To reset the number of Group-Specific Queries to the default value, use the no form of this command.

Format ip igmp last-member-query-count <1-20>

no ip igmp last-member-query-count

Fields	Definition
<1-20>	The range for last-member-query-count is from 1 to 20.

Default 2

Mode Interface Config

7.1.2.5. ip igmp last-member-query-interval

This command configures the Maximum Response Time being inserted into Group-Specific Queries sent in response to Leave Group messages on the interface.

To reset the Maximum Response Time being inserted into Group-Specific Queries sent in response to Leave Group messages on the interface to the default value, use the no form of this command.

Format ip igmp last-member-query-interval <0-255>

no ip igmp last-member-query-interval

Fields	Definition
<1-25>	The range for last-member-query-interval is from 1 to 25 seconds.

Default 1 second

Mode Interface Config

7.1.2.6. ip igmp query-interval

This command configures the query interval for the specified interface. This is the frequency at which IGMP Host-Query packets are transmitted on this interface.

To reset the query interval for the specified interface to the default value, use the no form of this command.

Format ip igmp query-interval <1-31744>

no ip igmp query-interval

Fields	Definition
<1-31744>	The range for query-interval is from 1 to 31744 seconds.
IGMP version 3	range 1-31744, version 2: range 1-3600, version 1: range 1-3600

Default 125 seconds

Mode Interface Config

7.1.2.7. ip igmp query-max-response-time

This command configures the maximum response time interval for the specified interface, which is the maximum query response time advertised in IGMPv2 queries on this interface.The time interval is specified in tenths of a second.

To reset the maximum response time interval for the specified interface to the default value, use the no form of this command.

Format ip igmp query-max-response-time <0-3174>

no ip igmp query-max-response-time

Fields	Definition
<1-3174>	The range for query-max-response-time is from 0 to 3174 seconds.
IGMP version 3	range 1-3174, version 2: range 1-25, version 1: range 1-25

Default 10 seconds

Mode Interface Config

7.1.2.8. ip igmp robustness

This command configures the robustness that allows tuning of the interface. 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.

To reset the robustness value to the default value, use the no form of this command.

Format ip igmp robustness <1-255>

no ip igmp robustness

Fields	Definition
<1-255>	The range for robustness is from 1 to 255.

Default 2

Mode Interface Config

7.1.2.9. 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.

To reset the number of Queries sent out on startup to the default value, use the no form of this command.

Format ip igmp startup-query-count <1-20>

no ip igmp startup-query-count

Fields	Definition
<1-20>	The range for startup-query-count is from 1 to 20.

Default 2

Mode Interface Config

7.1.2.10. ip igmp startup-query-interval

This command sets the interval between General Queries sent by a Querier on startup on the interface. The time interval value is in seconds.

To reset the interval between General Queries sent by a Querier on startup on the interface to the default value, use the no form of this command.

Format ip igmp startup-query-interval <1-300>

no ip igmp startup-query-interval

Fields	Definition
<1-300>	The range for startup-query-interval is from 1 to 300 seconds.

Default 31

Mode Interface Config

7.2. MLD Commands

This section provides a detailed explanation of the MLD commands. The commands are divided into the following different groups:

Show commands are used to display device settings, statistics and other information.

Configuration commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.

7.2.1. Show commands

7.2.1.1. 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.

Format show ipv6 mld groups {<slot/port> | vlan <vlan-id> | <group-address>}

Fields	Definition
<slot/port>	Valid slot and port number separated by forward slashes.
<vlan-id>	VLAN ID. The range of VLAN ID is from 1 to 4093.
<group-address>	The address of the multicast group.

Default None

Mode Privileged Exec

Display Message

The following fields are displayed as a table when <slot/port> is specified.

Fields	Definition
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.

Fields	Definition
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.

Fields	Definition
Source Address	The IP address of the source.
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.

7.2.1.2. show ipv6 mld interface

Use this command to display MLD-related information for the specific interface.

Format show ipv6 mld interface [{<slot/port> | vlan <vlan-id>}]

Fields	Definition
<slot/port>	Valid slot and port number separated by forward slashes.
<vlan-id>	VLAN ID. The range of VLAN ID is from 1 to 4093.

Default None

Mode Privileged Exec

Display Message

The following information is displayed for each of the interfaces or for only the specified interface.

Fields	Definition
Interface	The interface number in slot/port format.
MLD Global Admin Mode	Displays the configured administrative status of MLD.
MLD Interface Admin Mode	Displays the configured administrative status of MLD on the interface.
MLD Operational Mode	The operational status of MLD on the interface.
MLD Version	Indicates the version of MLD configured on the interface.
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.

Fields	Definition
Querier Status	This value indicates whether the interface is an MLD querier or non-querier on the subnet it is associated with.
Querier IP 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 Received	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.

7.2.1.3. show ipv6 mld traffic

Use this command to display MLD statistical information for the router.

Format show ipv6 mld traffic

Default None

Mode Privileged Exec

Display Message

Fields	Definition
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.
Malformed MLD Packets	The number of malformed MLD packets received by the router.

7.2.2. Configuration commands

7.2.2.1. ipv6 mld query-interval

Use this command to set the MLD router's query interval for the interface. The query-interval is the amount of time between the general queries sent when the router is the querier on that interface.

To reset the query interval for the specified interface to the default value, use the no form of this command.

Format ipv6 mld query-interval <1-31744>

no ipv6 mld query-interval

Fields	Definition
<1-31744>	The range for query-interval is 1 to 31744 seconds.
MLD version 2	range 1-31744, version 1: range 1-3600

Default 125

Mode Interface Config

7.2.2.2. ipv6 mld query-max-response-time

Use this command to set the MLD querier's maximum response time for the interface and this value is used in assigning the maximum response time in the query messages that are sent on that interface.

To reset the maximum response time interval for the specified interface to the default value, use the no form of this command.

Format ipv6 mld query-max-response-time <1-8387>

no ipv6 mld query-max-response-time

Fields	Definition
<0-8387>	The range for query-max-response-time is 0 to 8387 seconds.
MLD version 2	range 1-8387, version 1: range 1-65

Default 10 seconds

Mode Interface Config

7.2.2.3. ipv6 mld last-member-query-interval

Use this command to set the last member query interval for the MLD interface, which is the value of the maximum response time parameter in the group specific queries sent out of this interface.

To reset the Maximum Response Time being inserted into Group-Specific Queries sent in response to Leave Group messages on the interface to the default value, use the no form of this command.

Format ipv6 mld last-member-query-interval <1-65>

no ipv6 mld last-member-query-interval

Fields	Definition
<1-65>	The range for last-member-query-interval is from 1 to 65 seconds.

Default 1 second

Mode Interface Config

7.2.2.4. 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 the interface.

To reset the number of Group-Specific Queries to the default value, use the no form of this command.

Format ipv6 mld last-member-query-count <1-20>

no ipv6 mld last-member-query-count

Fields	Definition
<1-20>	The range for last-member-query-count is from 1 to 20.

Default 2

Mode Interface Config

7.2.2.5. ipv6 mld router

Use this command, in the administrative mode of the router, to enable MLD in the router.

To set the administrative mode of MLD in the router to inactive, use the no form of this command.

Format ipv6 mld router

no ipv6 mld router

Default Disable

Mode Global Config

Interface Config

7.2.2.6. clear ipv6 mld counters

The user can go to the CLI Privilege Configuration Mode to clear MLD counters on the system.

Format clear ipv6 mld counters [{<slot/port> | vlan <vlan-id>}]

Fields	Definition
<slot/port>	Specify the interface.
<vlan-id>	Specifies the VLAN interface. The range of the VLAN ID is 1 to 4093.

Default None

Mode Privileged Exec

7.2.2.7. clear ipv6 mld traffic

The user can go to the CLI Privilege Configuration Mode to clear MLD traffec on the system.

Format clear ipv6 mld traffic

Default None

Mode Privileged Exec

7.2.2.8. ipv6 mld version

This command configures the version of MLD for an interface.

To reset the version of MLD for this interface to the default value, use the no form of this command.

Format ipv6 mld version {1 | 2}

no ipv6 mld version

Fields	Definition
<1- 2>	The mld version number.

Default 2

Mode Interface Config

7.2.2.9. ipv6 mld reset-status

Use this command to reset the MLD proxy's host interface status parameters for the interface.

Format ipv6 mld reset-status

Mode Interface Config

7.2.2.10. ipv6 mld startup-query-count

Use this command to set the MLD router’s startup query count for the interface.

Format ipv6 mld startup-query-count <1-20>

Default 2

Mode Interface Config

7.2.2.11. ipv6 mld startup-query-interval

Use this command to set the MLD router’s startup query interval for the interface.

Format ipv6 mld startup-query-interval <1-300>

Default 31

Mode Interface Config

7.2.2.12. ipv6 mld unsolicit-rprt-interval

Use this command to set the MLD proxy unsolicited report interval for the interface.

Format ipv6 mld unsolicit-rprt-interval <1-260>

Default 1

Mode Interface Config

7.3. Multicast Commands

7.3.1. Show commands

7.3.1.1. show ip mcast

This command displays the system-wide multicast information

Format show ip mcast

Default None

Mode Privileged Exec
User Exec

Display Message

Fields	Definition
Admin Mode	This field displays the administrative status of multicast. This is a configured value.
IPv4 Protocol State	This field indicates the current state of the IPv4 multicast protocol. Possible values are Operational or Non-Operational.
IPv6 Protocol State	This field indicates the current state of the IPv6 multicast protocol. Possible values are Operational or Non-Operational.
IPv4 Table Max Size	The max number of the IPv4 entries allowed in the multicast table.
IPv6 Table Max Size	The max number of the IPv6 entries allowed in the multicast table.
IPv4 Protocol	This field displays the multicast IPv4 protocol running on the router.
IPv6 Protocol	This field displays the multicast IPv6 protocol running on the router.
IPv4 Multicast Forwarding Cache Entry Count	This field displays the number of entries in the IPv4 multicast table.
IPv6 Multicast Forwarding Cache Entry Count	This field displays the number of entries in the IPv6 multicast table.

7.3.1.2. show ip mcast boundary

This command displays all the configured administrative scoped multicast boundaries.

Format show ip mcast boundary {<slot/port> | all | vlan <vlan-id>}

Fields	Definition
<slot/port >	Interface number.
<vlan-id>	VLAN ID. The range of VLAN ID is 1 to 4093.
<all>	All interface.

Default None

Mode Privileged Exec
User Exec

Display Message

Fields	Definition
Interface	Valid slot and port number separated by forward slashes.
Group IP	The group IP address.
Mask	The group IP mask.

7.3.1.3. show ip mcast interface

This command displays the multicast information for the specified interface.

Format show ip mcast interface {<slot/port> | vlan <vlan-id>}

Fields	Definition
<slot/port >	Interface number.
<vlan-id>	VLAN ID. The range of VLAN ID is 1 to 4093.

Default None

Mode Privileged Exec
User Exec

Display Message

Fields	Definition
Interface	Valid slot and port number separated by forward slashes.
TTL	This field displays the time-to-live value for this interface.

7.3.1.4. show ip mcast mroute

This command displays a summary or all the details of the multicast table.

Format show ip mcast mroute {detail | summary}

Fields	Definition
Detail	displays the multicast routing table details.
Summary	displays the multicast routing table summary.

Default None

Mode Privileged Exec
User Exec

Display Message

If the "**detail**" parameter is specified, the following fields are displayed:

Fields	Definition
Source IP	This field displays the IP address of the multicast data source.
Group IP	This field displays the IP address of the destination of the multicast packet.
Expiry Time (secs)	This field displays the time of expiry of this entry in seconds.
Up Time (secs)	This field displays the time elapsed since the entry was created in seconds.
RPF Neighbor	This field displays the IP address of the RPF neighbor.
Flags	This field displays the flags associated with this entry.

If the "**summary**" parameter is specified, the following fields are displayed:

Fields	Definition
Source IP	This field displays the IP address of the multicast data source.
Group IP	This field displays the IP address of the destination of the multicast packet.
Protocol	This field displays the multicast routing protocol by which this entry was created.
Incoming Interface	This field displays the interface on which the packet for this source/group arrives.
Outgoing Interface List	This field displays the list of outgoing interfaces on which this packet is forwarded.

7.3.1.5. 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}

Fields	*Definition*
< groupipaddr >	the IP Address of the destination of the multicast packet.
Detail	Display the multicast routing table details.
Summary	Display the multicast routing table summary.

Default None

Mode Privileged Exec
User Exec

Display Message

If the **detail** parameter is specified the follow fields are displayed:

Fields	**Definition**
Source IP	This field displays the IP address of the multicast data source.
Group IP	This field displays the IP address of the destination of the multicast packet.

Expiry Time (secs)	This field displays the time of expiry of this entry in seconds.
Up Time (secs)	This field displays the time elapsed since the entry was created in seconds.
RPF Neighbor	This field displays the IP address of the RPF neighbor.
Flags	This field displays the flags associated with this entry.

If the **summary** parameter is specified the follow fields are displayed:

Fields	Definition
Source IP	This field displays the IP address of the multicast data source.
Group IP	This field displays the IP address of the destination of the multicast packet.
Protocol	This field displays the multicast routing protocol by which this entry was created.
Incoming Interface	This field displays the interface on which the packet for this group arrives.
Outgoing Interface List	This field displays the list of outgoing interfaces on which this packet is forwarded.

7.3.1.6. 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 <sourceipaddr>.

Format show ip mcast mroute source <sourceipaddr> {summary | detail}

Fields	**Definition**
< sourceipaddr >	the IP Address of the multicast data source.
summary	display the multicast routing table summary
Detail	Display the multicast routing table details.

Default None

Mode Privileged Exec
User Exec

Display Message

If the **detail** parameter is specified the follow fields are displayed:

Fields	Definition
Source IP	This field displays the IP address of the multicast data source.
Group IP	This field displays the IP address of the destination of the multicast packet.
Expiry Time (secs)	This field displays the time of expiry of this entry in seconds.
Up Time (secs)	This field displays the time elapsed since the entry was created in seconds.
RPF Neighbor	This field displays the IP address of the RPF neighbor.
Flags	This field displays the flags associated with this entry.

If the **summary** parameter is specified the follow fields are displayed:

Fields	Definition
Source IP	This field displays the IP address of the multicast data source.
Group IP	This field displays the IP address of the destination of the multicast packet.
Protocol	This field displays the multicast routing protocol by which this entry was created.
Incoming Interface	This field displays the interface on which the packet for this source arrives.
Outgoing Interface List	This field displays the list of outgoing interfaces on which this packet is forwarded.

7.3.1.7. show ip mcast mroute static

This command displays all the static routes configured in the static mcast table, if it is specified, or display the static route associated with the given <sourceipaddr>.

Format show ip mcast mroute static [<sourceipaddr>]

Fields	*Definition*
< sourceipaddr >	the IP Address of the multicast data source.

Default None

Mode Privileged Exec
User Exec

Display Message

Fields	Definition
Source IP	This field displays the IP address of the multicast data source.
Source Mask	This field displays the IP address Mask of the multicast data source.
RPF Address	This field displays the IP address of the RPF next-hop toward the source.
Preference	This field displays the administrative distance for this static mroute.

7.3.1.8. show ipv6 mroute

Use this command to display IPv6 multicast routing table information.

Format show ipv6 mroute {detail | summary}

Mode Privileged Exec
User Exec

Display Message

If you use the **summary** parameter, the command displays the following information:

Fields	Definition
Source IP	The IP address of the multicast data source.
Group IP	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.

Example:

```
(M4500-48XF8C) # show ipv6 mroute summary

                  Multicast route table summary

                                          Incoming  Outgoing

Source IP       Group IP        Protocol   Interface Interface List

--------------- --------------- ---------- --------- ---------------

       *        ff1e::1         PIMSM                0/1

2002::6         ff1e::1         PIMSM      0/2       0/1


(M4500-48XF8C) (Interface 0/2)#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


( *,ff1e::1)

00:08:14/000    RP: 2002::1

Joins/Prunes: 0/0

Incoming interface:           RPF nbr: ::

Outgoing interface list:

0/1        00:08:14/250    Joins:          0    Flags:   C


(2002::6,ff1e::1)

00:00:14/195    Flags:   T

Joins/Prunes: 0/0    Reg/Reg-stop: 0/0

Incoming interface: 0/2        RPF nbr: 2002::6

Outgoing interface list:

0/1        00:00:14/000    Joins:          0
```

7.3.1.9. show ipv6 mroute group

Use this command to display IPv6 multicast routing table information specific to the given group IPv6 address.

Format show ipv6 mroute group <group-address> {detail | summary}

Mode Privileged Exec
User Exec

Display Message

If you use the **detail** parameter, the command displays the following information:

Fields	Definition
Source IP	The IP address of the multicast data source.
Group IP	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 the outgoing interfaces on which the packet is forwarded.

If you use the **summary** parameter, the command displays the following information:

Fields	Definition
Source IP	The IP address of the multicast data source.
Group IP	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.

7.3.1.10. show ipv6 mroute source

Use this command to display IPv6 multicast routing table information specific to the given source IPv6 address.

Format show ipv6 mroute source <source-address> {detail | summary}

Mode Privileged Exec

User Exec

Display Message

If you use the **detail** parameter, the command displays the following information:

Fields	Definition
Source IP	The IP address of the multicast data source.
Group IP	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 the outgoing interfaces on which the packet is forwarded.

If you use the **summary** parameter, the command displays the following information:

Fields	Definition
Source IP	The IP address of the multicast data source.
Group IP	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.

7.3.1.11. show ipv6 mroute static

Use this command to display all configured IPv6 multicast static routes.

Format show ipv6 mroute static <source-address>

Mode Privileged Exec
User Exec

Display Message

Fields	Definition
Source Address	The IP address of the multicast source network.

Source Mask	The subnet mask pertaining to the source IP.
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 link-local address.
Preference	The administrative distance for this Static MRoute.

7.3.1.12. clear ip mroute

This command clears IPv4 multicast route entries.

Format clear ip mroute {* | <groupipaddr> [<sourceipaddr>]}

Default None

Mode Privileged Exec

7.3.1.13. clear ipv6 mroute

Use this command to delete all or the specified IPv6 multicast route entries. This command clears dynamic mroute entries only. It does not clear static mroutes.

Format clear ipv6 mroute { * | group-address [source-address]}

Mode Privileged Exec

7.3.2. Configuration commands

7.3.2.1. ip multicast

This command sets the administrative mode of the IP multicast forwarder in the router to active. For multicast routing to become operational, IGMP must be currently enabled. An error message will be displayed on the CLI if multicast routing is enabled while IGMP is disabled. However, the IP multicast mode configuration is stored in the multicast configuration file and is automatically enabled once IGMP is enabled.

To set the administrative mode of the IP multicast forwarder in the router to inactive, use the no form of this command.

Format ip multicast

no ip multicast

Default None

Mode Global Config

7.3.2.2. 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.

To remove an administrative scope multicast boundary specified by <groupipaddr> and <mask> for which this multicast administrative boundary is applicable, use the no form of this command.

Format ip mcast boundary <groupipaddr> <mask>

no ip mcast boundary <groupipaddr> <mask>

Fields	Definition
<groupipaddr>	The multicast group address for the start of the range of addresses to be excluded. The address must be in the range of 239.0.0.0 through 239.255.255.255.
<mask>	The mask to be applied to the multicast group address.

Default None

Mode Interface Config

7.3.2.3. ip multicast ttl-threshold

This command applies the given <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.

To reset the <ttl-threshold> for the routing interface to the default value, use the no form of this command.

Format ip multicast ttl-threshold <0 - 255>

no ip multicast ttl-threshold

Fields	Definition
<0 - 255>	the TTL threshold. The range is from 0 to 255.

Default 1

Mode Interface Config

7.4. IPv4 Protocol Independent Multicast (PIM) Commands

7.4.1. Show commands

7.4.1.1. show ip pim

This command displays the system-wide information for PIM-SM.

Format show ip pim

Default None

Mode Privileged Exec
User Exec

Display Message

Fields	Definition
PIM Mode	Indicates the PIM mode is sparse (PIM-SM)
Data Threshold Rate (Kbps)	Rate (in kbps) of SPT Threshold
Interface	slot/port, or VLAN ID
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.

7.4.1.2. show ip pim bsr-router

This command displays the bootstrap router (BSR) information.

Format show ip pim bsr-router {candidate | elected}

Default None

Mode Privileged Exec
User Exec

Display Message

Fields	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 bsrcandidate command
C-BSR Advertisement Interval(secs)	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(hh:mm:ss)	Time (in hours, minutes, and seconds) in which the next bootstrap message is due from this BSR

7.4.1.3. show ip pim interface

This command displays the interface information for PIM on the specified interface. If no interface is specified, the command displays the status parameters for all PIM-enabled interfaces.

Format show ip pim interface [{<slot/port> | loopback <loopback-id> | vlan <vlan-id>}]

Fields	Definition
<slot/port>	Interface number.
<loopback-id>	The loopback interface. The range is 0 to 63.
<vlan-id>	VLAN ID. The range of VLAN ID is 1 to 4093.

Default None

Mode Privileged Exec
User Exec

Display Message

Fields	Definition
Interface	slot/port, loopback ID, or VLAN ID
Mode	Indicates the PIM mode enabled on the interface is 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.
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.

7.4.1.4. show ip pim neighbor

This command displays PIM neighbors discovered by PIMv2 Hello messages. If the interface number is not specified, this command displays the neighbors discovered on all the PIM enabled interfaces.

Format show ip pim neighbor [{<slot/port> | vlan <vlan-id>}]

Fields	Definition
<slot/port>	Interface number.
<vlan-id>	VLAN ID. The range of VLAN ID is 1 to 4093.

Default None

Mode Privileged Exec
User Exec

Display Message

Fields	Definition
Neighbor Address	The IP address of the neighbor on an interface
Interface	slot/port or VLAN ID
Up Time	The time since this neighbor has become active on this interface
Expiry Time	The expiry time of the neighbor on this interface
DR Priority	The DR Priority configured on this Interface (PIM-SM only)
BSR Border	Identifies whether this interface is configured as a bootstrap router border interface

DR Priority is applicable only when sparse-mode configured routers are neighbors. Otherwise, NA is displayed in this field.

7.4.1.5. show ip pim rp mapping

Use this command to display all active group-to-RP mappings 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}]

Default None

Mode Privileged Exec
User Exec

Display Message

Fields	Definition
RP Address	The IP address of the RP for the group specified
Group Address	The IP address and prefix length 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
Expiry Time	The expiry time of the RP mapping
C-RP Advertisement Interval(secs)	Indicates the configured C-RP Advertisement interval with which the router, acting as a C-RP, will periodically send the C-RP advertisement messages.
Next Candidate RP Advertisement (hh:mm:ss)	Time (in hours, minutes, and seconds) in which the next C-RP Advertisement is due from this Router

7.4.1.6. show ip pim rp-hash

This command displays which rendezvous point (RP) is being used for a specified group.

Format show ip pim rp-hash <group-address>

Fields	Definition
<group-address>	the multicast group address for the start of the range of addresses to be excluded. The address must be in the range of 239.0.0.0 through 239.255.255.255.

Default None

Mode Privileged Exec
User Exec

Display Message

Fields	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

7.4.1.7. 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

Default None

Mode Privileged Exec
User Exec

Display Message

Fields	Definition
Group Address	The IP multicast address of the SSM group
Prefix Length	The network prefix length

7.4.1.8. show ip pim statistic

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 [{<slot/port> | vlan <vlan-id>}]

Fields	Definition
<slot/port >	Interface number.
<vlan-id>	VLAN ID. The range of VLAN ID is 1 to 4093.

Default None

Mode Privileged Exec
User Exec

Display Message

Fields	Definition
Intf	The PIM-enabled routing interface.
Stat	Rx: Packets received, Tx: Packets transmitted.
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.

7.4.1.9. show ip mfc

This command displays mroute entries in the multicast forwarding (MFC) database.

Format show ip mfc

Default None

Mode Privileged Exec
User Exec

Display Message

Fields	Definition
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.
Current multicast IPv4 protocol	The current operating IPv4 multicast routing protocol.
Current multicast IPv6 protocol	The current operating IPv6 multicast 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.
IPv4 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.

7.4.1.10. clear ip pim statistics

This command clears IP PIM statistics.

Format clear ip pim statistics

Default None

Mode Privileged Exec

7.4.2. Configuration commands

7.4.2.1. ip pim bsr-candidate

This command is used to configure the router to announce its candidacy as a bootstrap router (BSR).

To remove a configured candidate bootstrap router (C-BSR), use the no form of this command.

Format ip pim bsr-candidate interface {<slot/port> | loopback <loopback-id> | vlan <vlan-id>} <hash-mask-length> [<priority>] [interval <1-16383>]

no ip pim bsr-candidate interface {<slot/port> | loopback <loopback-id> | vlan <vlan-id>}

Fields	Definition
<slot/port>	Valid slot and port number separated by forward slashes.
<vlan-id>	VLAN ID. The range of VLAN ID is 1 to 4093.
<loopback-id>	The loopback interface. The range is 0 to 63.
<hash-mask-length>	BSR hash-mask length. The range of the mask is 0 to 32.
<priority>	BSR priority. The range of the priority is 0 to 255.
<interval>	BSR candidate advertisement interval. The range of the priority is 1 to 16383.

Default Disable

Mode Global Config

This command takes effect only when PIM-SM is configured as the PIM mode.

7.4.2.2. ip pim rp-address

This command is used to statically configure the RP address for one or more multicast groups. The parameter rp-address is the IP address of the RP. The parameter groupaddress is the group address supported by the RP. The parameter groupmask is the group mask for the group address. The optional keyword override indicates that if there is a conflict, the RP configured with this command prevails over the RP learned by BSR.

To remove a configured RP address for one or more multicast groups, use the no form of this command.

Format ip pim rp-address <rp-address> <group-address> <group-mask> [override]

no ip pim rp-address <rp-address> <group-address> <group-mask>

Fields	Definition
<rp-address>	Specifies the rp address.
<group-address>	Specifies the group address.
<group-mask>	Specifies the group mask.
[overide]	Indicates that if there is a conflict, the RP configured with this command prevails over the RP learned by BSR.

Default 0

Mode Global Config

This command takes effect only when PIM-SM is configured as the PIM mode.

7.4.2.3. ip 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).

To disable the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR), use the no form of this command.

Format ip pim rp-candidate interface {<slot/port> | loopback <loopback-id> | vlan <vlan-id>} <group-address> <group-mask> [interval <1-16383>]

no ip pim rp-candidate interface {<slot/port> | loopback <loopback-id> | vlan <vlan-id>} <group-address> <group-mask>

Fields	Definition
<slot/port>	Valid slot and port number separated by forward slashes.
<vlan-id>	VLAN ID. The range of VLAN ID is 1 to 4093.
<loopback-id>	The loopback interface. The range is 0 to 63.
<group-address>	Specifies the group address.
<group-mask>	Specifies the group mask.
[interval]	Indicates the RP candidate advertisement interval. The range is from 1 to 16383. The default value is 60 seconds.

Default None

Mode Global Config

This command takes effect only when PIM-SM is configured as the PIM mode.

7.4.2.4. ip pim sparse

This command enables the administrative mode of PIM-SM in the router.

To set the administrative mode of IPv4 PIM-SM in the router to inactive, use the no form of this command.

Format ip pim sparse

no ip pim sparse

Default Disable

Mode Global Config

7.4.2.5. ip pim-spt-threshold

Use this command to configure the Data Threshold rate for the last-hop router to switch to the shortest path. The possible values are 0 or Infinity.

To reset the Data Threshold rate for the last-hop router to switch to the shortest path to the default value, use the no form of this command.

Format ip pim spt-threshold {0 | Infinity}

no ip pim spt-threshold

Fields	Definition
<0>	This is 0 kilobits per seconds.
<Infinity>	This command will disable the function.

Default 0

Mode Global Config

This command takes effect only when PIM-SM is configured as the PIM mode.

7.4.2.6. ip pim ssm

Use this command to define the Source Specific Multicast (SSM) range of IP multicast addresses.

To disable the specified Source Specific Multicast (SSM) range, use the no form of this command.

Format ip pim ssm {default | <group-address> <group-mask>}
no ip pim ssm {default | <group-address> <group-mask>}

Fields	Definition
Default	Defines the SSM range access list 232/8.
<group-address>	Specifies the group address.
<group-mask>	Specifies the group-mask.

Default Disable

Mode Global Config

7.4.2.7. ip pim

This command administratively enables PIM on an interface or range of interfaces.

To set the administrative mode of PIM on an interface to disabled, use the no form of this command.

Format ip pim
no ip pim

Default Disable

Mode Interface Config

7.4.2.8. ip pim bsr-border

Use this command to prevent bootstrap router (BSR) messages from being sent or received through an interface or range of interfaces.

To disable the interface from being the BSR border, use the no form of this command.

Format ip pim bsr-border
no ip pim bsr-border

Default Disable

Mode Interface Config

This command takes effect only when PIM-SM is configured as the PIM mode.

7.4.2.9. ip pim dr-priority

Use this command to set the priority value for which a router is elected as the designated router (DR). This command can be configured on a single interface or a range of interfaces.

To reset the priority value to the default value for which a router is elected as the designated router (DR), use the no form of this command.

Format ip pim dr-priority <0-4294967294>

no ip pim dr-priority

Fields	Definition
<0-4294967294>	The range for dr-priority is from 0 to 4294967294.

Default 1

Mode Interface Config

This command takes effect only when PIM-SM is configured as the PIM mode.

7.4.2.10. ip pim hello-interval

Use this command to configure the PIM hello interval for the specified router interface or range of interfaces.

To reset the PIM hello interval to the default value, use the no form of this command.

Format ip pim hello-interval <0–18000>

no ip pim hello-interval

Fields	Definition
<0-18000>	The range for hello-interval is from 0 to 18000 seconds.

Default 30

Mode Interface Config

7.4.2.11. ip 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.

To reset the PIM join/prune interval to the default value, use the no form of this command.

Format ip pim join-prune-interval <0-18000>

no ip pim join-prune-interval

Fields	Definition
<0-18000>	The range for the join/prune interval is from 0 to 18000 seconds.

Default 60

Mode Interface Config

This command takes effect only when PIM-SM is configured as the PIM mode.

7.5. IPv6 Protocol Independent Mulitcast (PIM) Commands

7.5.1. Show commands

7.5.1.1. show ipv6 pim

Use this command to display the system-wide information for PIM-SM.

Format show ipv6 pim

Default None

Mode Privileged Exec
User Exec

Display Message

Fields	Definition
PIM Mode	Indicates the PIM mode is sparse (PIM-SM)
Data Threshold Rate	Indicates the data threshold rate for PIM.
Interface	slot/port, loopback ID or VLAN ID.
Interface Mode	Indicates whether PIM is enabled or disabled on this interface.
Operational Status	The current state of PIM on this interface. Possible values are Operational or Non-Operational.

7.5.1.2. show ipv6 pim ssm

Use this command to 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

Default None

Mode Privileged Exec
User Exec

Display Message

Fields	Definition
Group Address	The IPv6 multicast address of the SSM group.
Prefix Length	The network prefix length.

7.5.1.3. show ipv6 pim interface

Use this command to displays the interface information for PIM on the specified interface. If no interface is specified, the command displays the status parameters for all PIM-enabled interfaces.

Format show ipv6 pim interface [{<slot/port> | loopback <loopback-id> | vlan <vlan-id>}]

Fields	Definition
<slot/port>	Valid slot and port number separated by forward slashes.
<loopback-id>	The loopback interface. The range is 0 to 63.
<vlan-id>	VLAN ID. The range of VLAN ID is 1 to 4093.

Default None

Mode Privileged Exec
User Exec

Display Message

Fields	Definition
Interface	slot/port, loopback ID, or VLAN ID.
Mode	Indicate the PIM mode enabled on the interface is 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. By default, the value is 60 seconds.
DR Priority	The priority of the Designated Router configured on the interface.
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.

7.5.1.4. show ipv6 pim neighbor

Use this command to display PIM neighbors discovered by PIMv2 Hello messages. 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 <vlan-id>}]

Fields	Definition
<slot/port>	Valid slot and port number separated by forward slashes.
<vlan-id>	VLAN ID. The range of VLAN ID is 1 to 4093.

Default None

Mode Privileged Exec
User Exec

Display Message

Fields	Definition
Interface	Slot, and port number separated by forward slashes, or VLAN ID.
Neighbor Address	The IP address of the neighbor on an interface.
Up Time	The time since this neighbor has become active on this interface.
Expiry Time	The expiry time of the neighbor on this interface.
DR Priority	The DR Priority configured on this interface (PIM-SM only).

7.5.1.5. show ipv6 pim bsr-router

This command displays the bootstrap router (BSR) information.

Format show ipv6 pim bsr-router {candidate | elected}

Default None

Mode Privileged Exec

User Exec

Display Message

Fields	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.
Next Bootstrap Message	Time (in hours, minutes, and seconds) in which the next bootstrap message is due from this BSR.
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.

7.5.1.6. 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>

Fields	Definition
<group-address>	The IPv6 address of the specified group.

Default None

Mode Privileged Exec

User Exec

Display Message

Fields	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.

7.5.1.7. show ipv6 pim rp-mapping

This command displays themapping for the PIM group to the active Rendezvous points(RP) of which the router is 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}]

Default None

Mode Privileged Exec

User Exec

Display Message

Fields	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.
Expiry Time	The expiry time of the RP mapping.
Next Candidate RP Advertisement (hh:mm:ss)	Time (in hours, minutes, and seconds) in which the next C-RP Advertisement is due from this Router

If candidate is specified, the following fields are displayed:

Fields	Definition
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.

7.5.1.8. show ipv6 pim statistic

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 ipv6 pim statistics [{<slot/port> | vlan <vlan-id>}]

Fields	Definition
<slot/port >	Interface number.
<vlan-id>	VLAN ID. The range of VLAN ID is 1 to 4093.

Default None

Mode Privileged Exec
User Exec

Display Message

Fields	Definition
Intf	The PIM-enabled routing interface.
Stat	Rx: Packets received, Tx: Packets transmitted.
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.

7.5.1.9. clear ipv6 pim statistics

This command clears IPv6 PIM Statistics.

Format clear ipv6 pim statistics

Default None

Mode Privileged Exec

7.5.2. Configuration commands

7.5.2.1. ipv6 pim sparse

This command enables the administrative mode of PIM-SM in the router.

To set the administrative mode of IPv6 PIM-SM in the router to inactive, use the no form of this command.

Format ipv6 pim sparse
no ipv6 pim sparse

Default Disable

Mode Global Config

7.5.2.2. ipv6 pim

This command administratively enables PIM on an interface or range of interfaces.

To set the administrative mode of IPv6 PIM on an interface to disabled, use the no form of this command.

Format ipv6 pim
no ipv6 pim

Default Disable

Mode Interface Config

7.5.2.3. ipv6 pim hello-interval

Use this command to configure the PIM hello interval for the specified router interface or range of interfaces.

To reset the PIM hello interval to the default value, use the no form of this command.

Format ipv6 pim hello-interval <0–18000>
no ipv6 pim hello-interval

Fields	Definition
<0-18000>	The range for hello-interval is from 0 to 18000 seconds.

Default 30

Mode Interface Config

7.5.2.4. ipv6 pim bsr-border

Use this command to prevent bootstrap router (BSR) messages from being sent or received through an interface or range of interfaces. Note that this command takes effect only when PIM-SM is enabled in the Global mode.

To disable the interface from being the BSR border, use the no form of this command.

Format ipv6 pim bsr-border

no ipv6 pim bsr-border

Default Disable

Mode Interface Config

7.5.2.5. ipv6 pim bsr-candiate

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.

To remove a configured PIM candidate bootstrap router (C-BSR), use the no form of this command.

Format ipv6 pim bsr-candidate interface {<slot/port> | loopback <loopback-id> | vlan <vlan-id>} <hash-mask-length> [<priority>] [interval <1-16383>]

no ipv6 pim bsr-candidate interface {<slot/port> | loopback <loopback-id> | vlan <vlan-id>}

Fields	Definition
<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..
<loopback-id>	The loopback interface. The range is 0 to 63.
<vlan-id>	VLAN ID. The range of VLAN ID is 1 to 4093.
<hash-mask-length>	BSR hash-mask length. The range of the mask is 0 to 128. The length of a mask that is to be ANDed with the group address before the hash function is called. All groups with the saem 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.
<priority>	Priority of the candidate BSR. The range of the priority is 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>	BSR candidate advertisement interval. The range of the priority is 1 to 16383.

Default None

Mode Global Config

7.5.2.6. ipv6 pim dr-priority

Use this command to set the priority value for which a router is elected as the designated router (DR). This command can be configured on a single interface or a range of interfaces.

To reset the priority value to the default value for which a router is elected as the designated router (DR), use the no form of this command.

Format ipv6 pim dr-priority <0-4294967294>

no ipv6 pim dr-priority

Fields	Definition
<0-4294967294>	The range for dr-priority is from 0 to 4294967294.

Default 1

Mode Interface Config

7.5.2.7. ipv6 pim join-prune-interval

This command is used to configure the interface join/prune interval for the PIM-SM router on an interface or range of interfaces. The join/prune interval is specified in seconds.

To reset the join/prune interval to the default value, use the no form of this command.

Format ipv6 pim join-prune-interval <0-18000>

no ipv6 pim join-prune-interval

Fields	Definition
<0-18000>	The range for join-prune-interval is from 0 to 18000 seconds.

Default 60

Mode Interface Config

7.5.2.8. ipv6 pim rp-address

This command is used to define the address of a PIM Rendezvous point (RP) for a specific multicast group range. The parameter <*rp-address*> is the IPv6 address of the RP. The parameter <*group-address*> is the group address supported by the RP. The parameter <*prefix-length*> is the group mask for the group address. The optional

keyword **override** indicates that if there is a conflict, the RP configured with this command prevails over the RP learned by BSR.

To remove a configured RP address for one or more multicast groups, use the no form of this command.

Format ipv6 pim rp-address *<rp-address> <group-address/prefix-length>* [override]

no ipv6 pim rp-address *<rp-address> <group-address/prefix-length>*

Fields	Definition
<rp-address>	The IPv6 address of the RP.
<group-address>	The group address supported by the RP.
<prefix-length>	The group mask for the group address.
Override	Indicates that if there is a conflict, the RP configured with this command prevails over the RP learned by BSR.

Default None

Mode Global Config

7.5.2.9. ipv6 pim rp-candiate

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.

To disable the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR), use the no form of this command.

Format ipv6 pim rp-candidate interface {<slot/port> | loopback <loopback-id> / vlan <vlan-id>} *<group-address/prefix-length> [interval <interval>*]

no ipv6 pim rp-candidate interface {<slot/port> | loopback <loopback-id> | vlan <vlan-id>} *<group-address/prefix-length>*

Fields	Definition
<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.
<loopback-id>	The loopback interface. The range is 0 to 63.
<vlan-id>	VLAN ID. The range of VLAN ID is 1 to 4093.
<group-address>	The multicast group address that is advertised in association with the RP address.

<prefix-length>	The multicast group prefix that is advertised in association with the RP address.
<interval>	Configure the C-RP advertisement interval. The range of interval is 1 to 16383, and the default value is 60.

Default None

Mode Global Config

7.5.2.10. ipv6 pim spt-threshold

This command is used to configure the Data Threshold rate for the last-hop router to switch to the shortest path. Now support to enable (0) or disable(Infinity).

To reset the Data Threshold rate for the last-hop router to switch to the shortest path to the default value, use the no form of this command.

Format ipv6 pim spt-threshold {0 | Infinity}

no ipv6 pim spt-threshold

Fields	Definition
<0>	This is 0 kilobits per seconds.
<Infinity>	This command will disable the function.

Default 0

Mode Global Config

7.5.2.11. ipv6 pim ssm

Use this command to define the Source Specific Multicast (SSM) range of IPv6 multicast addresses on the router. Note that this command takes effect only when PIM-SM is configured as the PIM mode.

To disable the specified Source Specific Multicast (SSM) range, use the no form of this command.

Format ipv6 pim ssm {*default* | *<group-address>*/*<prefix-length>*}

no ipv6 pim ssm {*default* | *<group-address>*/*<prefix-length>*}

Fields	Definition
Default	Defines the SSM range access list FF3x::/32.

<group-address>	Specifies the group address.
<group-mask>	Specifies the group-mask.

Default Disable

Mode Global Config

8. IPv6 Commands

8.1. 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, please refer to “ip address” command. To assign an IPv6 address to the tunnel interface, please refer to “ipv6 address” command.

8.1.1. Show commands

8.1.1.1. 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 [<0-7>]

Fields	Definition
<0-7>	Specify the tunnel interface number you would like to show**.**

Default None

Mode Privileged Exec

Display Message

If you do not specify a tunnel ID, the command shows the following information for each configured tunnel:

Fields	Definition
tunnel ID	Shows the tunnel identification number.
interface	Shows the name of the tunnel interface.
tunnel Mode	Shows the tunnel mode.
source Address	Shows the source transport address of the tunnel.
destination Address	Shows the destination transport address of the tunnel.

If you specify a tunnel ID, the command shows the following information for the tunnel:

Fields	Definition
interface Link Status	Shows whether the link is up or down.
MTU Size	Shows 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.

Example: If you specify a tunnel ID, the command shows the following information for the tunnel in the example.

```
(M4500-48XF8C)(Interface tunnel 0)#show interface tunnel 0


Routing Mode..................................... Disabled

Administrative Mode.............................. Enabled

IPv6 Implicit Mode............................... Disabled

IPv6 Operational Mode............................ Disabled

Interface Maximum Transmit Unit.................. 1480

Router Duplicate Address Detection Transmits... 1

Router Advertisement NS Interval................. 0

Router Advertisement Lifetime.................... 1800

Router Advertisement Reachable Time.............. 0

Router Advertisement Interval(max)............... 600

Router Advertisement Interval(min)............... 200

Router Advertisement Managed Config Flag....... Disabled

Router Advertisement Other Config Flag......... Disabled

Router Advertisement Suppress Flag.............. Disabled

IPv6 Destination Unreachables.................... Disabled
```

8.1.2. Configuration commands

8.1.2.1. interface tunnel

This command uses to enter the Interface Config mode for a tunnel interface. The tunnel id range is from 0 to 7.

To remove the tunnel interface and associated configuration parameters for the specified tunnel interface, use the no form of this command.

Format interface tunnel <0-7>

no interface tunnel <0-7>

Default None

Mode Global Config

8.1.2.2. tunnel source

This command specifies the source transport address of the tunnel, either explicitly or by reference to an interface.

To remove the tunnel source, use the no form of this command.

Format tunnel source {<ipv4-address> | <ethernet> {<slot/port> | vlan <vlan-id>}}>

no tunnel source

Fields	Definition
<slot/port>	The Interface number.
<vlan-id>	VLAN ID. The range of VLAN ID is 1 to 4093.
<ipv4-address>	A valid IP Address.

Default None

Mode Interface Tunnel Mode

8.1.2.3. tunnel destination

This command specifies the destination transport address of the tunnel.

To remove the tunnel destination, use the no form of this command.

Format tunnel destination {<ipv4-address>}

no tunnel destination

Fields	Definition
<ipv4-address>	A valid IP Address.

Default None

Mode Interface Tunnel Mode

8.1.2.4. tunnel mode

This command specifies the mode of the tunnel.

To restore the tunnel mode, use the no form of this command.

Format tunnel mode ipv6ip [6to4]]

no tunnel mode

Fields	Definition
[6to4]	With the optional 6to4 argument, the tunnel mode is set to 6to4 automatic. Without the optional 6to4 argument, the tunnel mode is configured.

Default None

Mode Interface Tunnel Mode

8.2. 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, please refer to “ip address” command. To assign an IPv6 address to the loopback interface, please refer to “ipv6 address” command.

8.2.1. Show commands

8.2.1.1. show interface loopback

This command displays information about configured loopback interfaces.

Format show interface loopback [{<0-63> | vrf <vrf-name>}]

Fields	Definition
<0-63>	Specify the ID of the loopback interface. The range is from 0 to 63.
<vrf-name>	Specify the name of the VRF

Default None

Mode Privileged Exec

Display Message

If you do not specify a loopback ID, the following information appears for each loopbackinterface on the system:

Fields	Definition
Loopback ID	Shows the loopback ID associated with the rest of the information in the row.
Interface	Shows the interface name.
IP Address	Shows the IP address of the interface

If you specify a loopback ID, the following information appears:

Fields	Definition
Interface Link Status	Shows whether the link is up or down.
IP Address	Shows the IPv4 address of the interface.

IPv6 is enabled (disabled)	Shows whether IPv6 is enabled on the interface
IPv6 Prefix is	Shows the IPv6 address of the interface.
MTU size	Shows the maximum transmission size for packets on this interface, in bytes.

8.2.2. Configuration commands

8.2.2.1. interface loopback

This command is used to enter the Interface Config mode for a loopback interface. The range of

the loopback ID is 0 to 63.

To remove the loopback interface and associated configuration parameters for the specified loopback interface, use the **no** form of this command.

Format interface loopback <0-63>

no interface loopback <0-63>

Fields	Definition
<0-63>	Specify the ID of the loopback interface.

Default None

Mode Global Config

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.

8.3.1. Show commands

8.3.1.1. show ipv6 brief

This command displays the IPv6 status and IPv6 unicast routing mode.

Format show ipv6 brief

Default None

Mode Privileged Exec
User Exec

Display Message

Fields	Definition
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 “ipv6 hot-limit”.
ICMPv6 Rate Limit Error Interval	Shows how often the token bucket is initialized with burst-size tokens. For more information, see “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 “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.
IPv6 NUD Maximum Unicast Solicits	Shows the maximum number of unicast Neighbor Solicitations sent during NUD (neighbor unreachability detection) before switching to multicast Neighbor Solicitations.
IPv6 NUD Maximum Multicast Solicits	Shows the maximum number of multicast Neighbor Solicitations sent during NUD (neighbor unreachability detection) when in UNREACHABLE state.

IPv6 NUD Maximum Unicast SolicitsExponential Backoff Multiple	Shows the exponential backoff multiple to be used in the calculation of the next timeout value for Neighbor Solicitations transmission during NUD (neighbor unreachability detection) following the exponential backoff algorithm.

8.3.1.2. show ipv6 interface

This command displays the usability status of IPv6 interfaces and whether ICMPv6 Destination Unreachable messages may be sent.

Format show ipv6 interface [{brief | {port <slot/port> | vlan <vlan-id>} [prefix] | tunnel <0-7> | loopback <0-63>}]

Fields	Definition
<slot/port>	Valid slot and port number separated by forward slashes.
<vlan-id>	VLAN ID. The range of VLAN ID is 1 to 4093.
<0-7>	Specify the tunnel ID.
<0-63>	Specify the loopback ID.

Default None

Mode Privileged Exec

User Exec

Display Message

If you use the brief parameter, the following information displays for all configured IPv6 interfaces:

Fields	Definition
Interface	Shows the interface in slot/port, vlan, lb (loopback), or tunnel format.
Oper. Mode	Shows whether the mode is enabled or disabled.
IPv6 Address/Length	Shows the IPv6 address and length on interfaces with IPv6 enabled.

If you specify an interface, the following information also appears.

Fields	Definition
IPv6 Prefix	Shows the IPv6 prefix for the specified interface.

Routing Mode	Shows whether IPv6 routing is enabled or disabled.
IPv6 Enable Mode	Shows whether IPv6 is enabled on the interface.
IPv6 Routing Operational Mode	Shows whether the operational state of an interface is enabled or disabled.
IPv6 Link-local Scope ID	Shows the scope ID of the link local address.
Bandwidth	Shows the bandwidth of the interface.
Interface Maximum Transmission Unit	Shows the MTU size, in bytes.
Router Duplicate Address Detection Transmits	Shows 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	Indicate 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	Shows the interval, in milliseconds, between router advertisements for advertised neighbor solicitations.
Router Advertisement MTU	Shows the MTU value of the interface in router advertisements.
Router Advertisement Lifetime	Shows the router lifetime value of the interface in router advertisements.
Router Advertisement Reachable Time	Shows the amount of time, in milliseconds, to consider a neighbor reachable after neighbor discovery confirmation.
Max/Min Router Advertisement Interval	Shows 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 router preference value in IPv6 router advertisements.

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).
ICMPv6 Redirects	Specify 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.

Fields	Definition
IPv6 Prefix	Shows the IPv6 prefix for the specified interface.
Preferred Lifetime	Shows the amount of time the advertised prefix is a preferred prefix.
Valid Lifetime	Shows 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.

8.3.1.3. show ipv6 interface neighbors

This command displays information about the IPv6 neighbors.

Format show ipv6 interface neighbors [<ipv6-address> | interface {<slot>/port> | {tunnel <0-7>} | {vlan <1-4093>}}]

Fields	Definition
<ipv6-address>	Specif the IPv6 address of the neighbor.
<slot/port>	Valid slot and port number separated by forward slashes.
<0-7>	Specify the tunnel ID.
<1-4093>	Specify the VLAN ID.

Default None

Mode Privileged Exec

Display Message

Count of Learned Neighbors the number of neighbor mac address be learned.

Fields	Definition
Interface	Shows the interface in slot/port format.
Type	The type of the IPv6 address. It can be Dynamic, Static, Local or Other.
IPv6 Address	IPV6 address of neighbor or interface.
MAC Address	Link-layer Address.
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 not mean Note 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.
Age(Seconds)	The time in seconds that has elapsed since an entry was added to the cache.

8.3.1.4. show ipv6 protocols

This command lists a summary of the configuration and status of 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]

Fields	Definition
bgp	Option to specify only display BGP summary.
Ospf	Option to specify only display OSPF summary.

Default None

Mode Privileged Exec

Display Message

BGP section:

Fields	Definition
Routing Protocol	BGP.

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.
BGP GR-Enabled Mode	Whether BGP Graceful Restart Enabled Mode is enabled. (Enabled or Disabled)
BGP GR-Aware Mode	Whether BGP Graceful Restart Aware Mode is enabled. (Enabled or Disabled)
BGP GR restart-time	Setting of BGP Graceful Restart Timer.
BGP GR stalepath-time	Setting of BGP Graceful Stale Path Timer.
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	Whether BGP is configured to compare the MEDs for routes received from peers in different ASs.
Fast Interval Failover	Whether BGP immediately brings down a iBGP adjacency if the routing table manager reports that the peer address is no longer reachable.
Fast Exteral 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.
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.
Network Originated	The set of networks originated through a network command.
Neighbors	A list of configured neighbors.

OSPFv3 section:

Fields	**Definition**
Routing Protocol	OSPFv3.
Router ID	The router ID configured for OSPFv3.

OSPF Admin Mode	Whether OSPFv3 is globally enabled or disabled.
Maximum Paths	The maximum number of next hops in an OSPF route.
Default Route Advertise	Whether OSPF is configured to orginiate a default route.
Distance	The default administrative distance (or route preference) for intra-as, inter-as, and external OSPF routes.
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.

8.3.1.5. 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 **<slot/port>** corresponds to a physical routing interface. The keyword *vlan* is used to specify the VLAN ID of the routing VLAN directly. The **<protocol>** specifies the protocol that installed the routes. The **<protocol>** is one of the following keywords: **connected, bgp, ospf, static, 6to4.** The *all* specifies that all routes including best and non-best routes are displayed. Otherwise, only the best routes are displayed.

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 <vlan-id>} [<protocol>] | <protocol> | summary} [all] | all}]

Fields	Definition
vlan-id	The range is from 1 to 4093.

Default None

Mode Privileged Exec

User Exec

Display Message

The **show ipv6 route** command displays the routing tables in the following format:

```
Codes: C - connected, S – static, 6To4 – 6to4 Route , B - BGP Derived, D - Database 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, K - Kernel
```

The columns for the routing table display the following information:

Fields	Definition
Code	The code for the routing protocol that created this routing entry.
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	Displays 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
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 destnation. 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 beacause 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.

8.3.1.6. 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

Default None

Mode Privileged Exec

8.3.1.7. show ipv6 route hw-failure

This command displays 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

Default None

Mode Privileged Exec

8.3.1.8. show ipv6 route preferences

This command displays 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

Default None

Mode Privileged Exec

Display Message

Fields	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 eBGP routes.
BGP Internal	Preference of iBGP routes.
BGP Local	Preference of BGP local routes.

8.3.1.9. show ipv6 route summary

This command displays the summary of the routing table. Use *all* to display the count summary for all routes, including best and non-best routes. Use the command without parameters to display the count summary for only the best routes.

Format show ipv6 route summary [all]

Default None

Mode Privileged Exec

Display Message

Fields	Definition
Connected Routes	Total number of connected routes in the routing table.
Static Routes	Total number of static routes in the routing table.
Kernel Routes	Total number of kernel routes in the routing table.
6to4 Routes	Total number of 6to4 routes in the routing table.
BGP Routes	Total number of routes installed by BGP protocol. The routes include external routes, internal routes and local routes.
OSPF Routes	Total number of routes installed by OSPFv3 protocol. The routes include intra-area routes, inter-area routes, external type-1 routes, and external type-2 routes.
Reject Routes	Total number of reject routes installed by all protocols.
Total Routes	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 Rotue Adds	The number of routes 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.
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.
Kernel Failed Route Adds	The number of routes that failed to be added to the routing table by kernel 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.
Unique Next Hops (High)	The number of distinct next hops used among all routes currently in the routing table. The *(High)* means the highest count of uniqe next hops since counters were last cleared. These include local interfaces for local routes and neighbors for indirect routes.
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 *(High)* means 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 *(High)* means the highest count of next hop groups with multiple next hops since counters were last cleared.
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 a 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 Hop	The current number of routes with each number of next hops.
Number of Prefixes	Summarizes the number of routes with prefixes of different lengths.

8.3.1.10. show ipv6 traffic

This command displays traffic and statistics for IPv6 and ICMPv6. Specify a logical, loopback, or tunnel interface to view information about traffic on a specific interface. If you do not specify an interface, the command displays information about traffic on all interfaces.

Format show ipv6 traffic [{<slot/port> | loopback <loopback-id> | tunnel <tunnel-id> | vlan <vlan-id>}]

Fields	Definition
loopback-id	The range is from 0 to 63.
tunnel-id	The range is from 0 to 7.
vlan-id	The range is from 1 to 4093.

Default None

Mode Privileged Exec

Display Message

IPv6 STATISTICS

Fields	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 re-assembly.
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.
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. 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 **Datagrams Forwarded**.
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 **Datagrams Forwarded** if any such packets met this (discretionary) discard criterion.
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.
Fragments Created	Number of output datagram fragments that have been generated as a result of fragmentation at this output interface.
Multicast Datagrams Received	Number of multicast packets received by the interface.
Multicast Datagrams Transmitted	Number of multicast packets transmitted by the interface.

ICMPv6 STATISTICS

Fields	Definition
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 Received	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 Received	Number of ICMP Destination Unreachable messages received by the interface.
ICMPv6 Messages Prohibited Administratively Received	Number of ICMP destination unreachable/communication administratively prohibited messages received by the interface.
ICMPv6 Time Exceeded Messages Received	Number of ICMP Time Exceeded messages received by the interface.
ICMPv6 Parameter Problem Messages Received	Number of ICMP Parameter Problem messages received by the interface.
ICMPv6 Packet Too Big Messages Received	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.
ICMPv6 Group Membership Query Messages Received	Number of ICMPv6 Group Membership Query messages received by the interface.
ICMPv6 Group Membership Response Messages Received	Number of ICMPv6 Group Membership Response messages received by the interface.
ICMPv6 Group Membership Reduction Messages Received	Number of ICMPv6 Group Membership Reduction 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.
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 Transmitted	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 Transmitted	Number of ICMPv6 Group Membership Query messages sent.
ICMPv6 Group Membership Response Messages Transmitted	Number of ICMPv6 Group Membership Response messages sent.
ICMPv6 Group Membership Reduction Messages Transmitted	Number of ICMPv6 Group Membership Reduction messages sent.
ICMPv6 Duplicate Address Detects	Number of duplicate addresses detected by interface.

8.3.2. Configuration commands

This section describes the IPv6 commands you use to configure IPv6 on the system and on the interface.

8.3.2.1. 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. 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.

To return the unicast hop count to the default, use the no form of this command.

Format ipv6 hop-limit <hops>

no ipv6 hop-limit

Fields	Definition
<hops>	The range is from 1 to 255.

Default Not configured

Mode Global Config

8.3.2.2. ipv6 unicast-routing

Use this command to enable the forwarding of IPv6 unicast packets.

To disable the forwarding of IPv6 unicast packets, use the no form of this command.

Format ipv6 unicast-routing

no ipv6 unicast-routing

Default Disabled

Mode Global Config

8.3.2.3. ipv6 enable

Use this command to enable IPv6 routing on an interface, 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.

To disable IPv6 routing on an interface, use the no form of this command.

Format ipv6 enable

no ipv6 enable

Default Disabled

Mode Interface Config

Interface VLAN

8.3.2.4. ipv6 address

Use this command to configure an IPv6 address on an interface, 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 linklocal 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.

To remove all IPv6 addresses or specified IPv6 address on an interface, use the no form of this command. If you do not specify any parameter, the command deletes all the IPv6 addresses on an interface.

Format ipv6 address <prefix> / <prefix_length> [{eui64 | link-local}]

no ipv6 address [<prefix> / <prefix_length>] [{eui64 | link-local}]

Fields	Definition
<prefix>	The parameter consists of the bits of the address to be configured.
<prefix_length>	This option designates how many of the high-order contiguous bits of the address comprise the prefix.
[eui-64]	This 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.
link-local	The IPv6 link-local address to be configured.

Default None

Mode Interface Config
Interface VLAN

8.3.2.5. ipv6 address autoconfig

Use this command to allow an in-band interface to acquire an IPv6 address through IPv6 Neighbor Discovery Prococol (NDP) and through the use of Router Advertisement messages.

To revert the IPv6 autoconfiguration status on an interface to the default value, use the no form of this command.

Format ipv6 address autoconfig
no ipv6 address autoconfig

Default Disable

Mode Interface Config
Interface VLAN

8.3.2.6. 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.

To release a leased address and disable DHCPv6 on an interface, use the no form of this command.

Format ipv6 address dhcp [restart]
no ipv6 address dhcp

Fields	Definition
<dhcp>	Obtains IPv6 address from DHCPv6.
<restart>	To restart the DHCPv6 process.

Default Disable

Mode Interface-Vlan Config

Interface Config

8.3.2.7. 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. 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 interface <slot/port> identifies direct static routes from point-to-point and broadcast interfaces, and 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.

To delet an IPv6 static route, use the no form of this command. Use the command without the optional parameters to delete all static routes to the specified destination. Use the <preference> parameter to revert preference of a route to default preference.

Format ipv6 route <ipv6-prefix>/<prefix_length> {<next-hop-address> | Null0 | interface {<slot/port> | tunnel <tunnel-id> | vlan <vlan-id>} <next-hop-address>} [<preference>]

no ipv6 route <ipv6-prefix>/<prefix_length> [{<next-hopaddress> | Null0 | interface {<slot/port> | tunnel <tunnel-id> | vlan <vlan-id>} <next-hop-address> | <preference>}]

Fields	Definition
<tunnel-id>	The range is from 0 to 7.
<vlan-id>	The range is from 1 to 4093.

Default Disable

Mode Global Config

8.3.2.8. 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.

To reset the default static route preference value in the router to the original default preference, use the no form of this command.

Format ipv6 route distance <1-255>

no ipv6 route distance

Default 1

Mode Global Config

8.3.2.9. ipv6 mtu

This command sets the maximum transmission unit (MTU) size, in bytes, of IPv6 packets on an interface. This command replaces the default or link MTU with a new MTU value. The default MTU value for a tunnel interface is 1480. You cannot change this value.

To reset maximum transmission unit value to default value, use the no form of this command.

Format ipv6 mtu <1280-9394>

no ipv6 mtu

Default 0 or link speed (MTU value is 1500)

Mode Interface Config

8.3.2.10. ipv6 nd dad attemps

This command sets the number of duplicate address detection probes transmitted on an interface. Duplicate address detection verifies that an IPv6 address on an interface is unique.

To reset to number of duplicate address detection value to default value, use the no form of this command.

Format ipv6 nd dad attempts <0 – 255>

no ipv6 nd dad attempts

Default 1

Mode Interface Config

8.3.2.11. ipv6 nd managed-config-flag

This command sets the “managed address configuration” flag in router advertisements on the interface. When the value is true, end nodes use DHCPv6. When the value is false, end nodes automatically configure addresses.

To reset the “managed address configuration” flag in router advertisements to the default value, use the no form of this command.

Format ipv6 nd managed-config-flag

no ipv6 nd managed-config-flag

Default False

Mode Interface Config

8.3.2.12. ipv6 nd ns-interval

This command sets the interval between router advertisements for advertised neighbor solicitations, in milliseconds, for an interface. An advertised value of 0 means the interval is unspecified.

To reset the neighbor solicit retransmission interval of the specified interface to the default value, use the no form of this command.

Format ipv6 nd ns-interval { <1000 – 4294967295> | 0 }

no ipv6 nd ns-interval

Default 0

Mode Interface Config

8.3.2.13. ipv6 nd other-config-flag

This command sets the “other stateful configuration” flag in router advertisements sent from the interface.

To reset the “other stateful configuration” flag back to its default value in router advertisements sent from the interface, use the no form of this command.

Format ipv6 nd other-config-flag

no ipv6 nd other-config-flag

Default False

Mode Interface Config

8.3.2.14. ipv6 nd ra-interval

This command sets the transmission interval between router advertisements on the interface.

To set router advertisement interval to the default, use the no form of this command.

Format ipv6 nd ra-interval <4 – 1800> [<Min Router Advertisement Interval>]

no ipv6 nd ra-interval

Fields	Definition
Min Router Advertisement Interval	This command sets the minimal transmission interval between router advertisements on the interface.

Default 600

Mode Interface Config

8.3.2.15. 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. 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.

To reset router lifetime to the default value, use the no form of this command.

Format ipv6 nd ra-lifetime <lifetime>

no ipv6 nd ra-lifetime

Default 1800

Mode Interface Config

8.3.2.16. 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.

To reset reachable time to the default value, use the no form of this command.

Format ipv6 nd reachable-time <0 - 3600000>

no ipv6 nd reachable-time

Default 0

Mode Interface Config

8.3.2.17. ipv6 nd router-preference

This command sets the default router preference that the interface advertises in router advertisement messages.

To reset router preference to default, use the no form of this command.

Format ipv6 nd router-preference <high | low | medium>

no ipv6 nd router-preference

Default Medium

Mode Interface Config

8.3.2.18. ipv6 nd suppress-ra

This command suppresses router advertisement transmission on an interface.

To enables router transmission on an interface, use the no form of this command.

Format ipv6 nd suppress-ra

no ipv6 nd suppress-ra

Default Disabled

Mode Interface Config

8.3.2.19. ipv6 nd prefix

This command is used 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.

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.

To set prefix configuration to default values, use the no form of this command.

Format ipv6 nd prefix <prefix/prefix_length> [{<0-4294967295> | infinite}{<0-4294967295> | infinite}] [no-autoconfig][off-link]

no ipv6 nd prefix <prefix/prefix_length>

Default Valid-lifetime: 2592000

Preferred-lifetime: 604800

Autoconfig: enabled

On-link: enabled

Mode Interface Config

8.3.2.20. ipv6 neighbor

Use this command to configure a static IPv6 neighbor with the given IPv6 address and MAC address on a routing interface.

To remove a static IPv6 neighbor with the given IPv6 address on a routing interface, use the no form of this command.

Format ipv6 neighbor <ipv6address> {<slot/port> | vlan <1-4093>} <macaddr>

no ipv6 neighbor <ipv6address> {<slot/port> | vlan <1-4093>}

Fields	Definition
ipv6address	The IPv6 address of the neighbor.
Macaddr	The MAC address for the neighbor.

Default None

Mode Global Config

8.3.2.21. ipv6 neighbor dynamicrenew

Use this command to automatically renew the IPv6 neighbor entries.

To disable automatic renewing of IPv6 neighbor entries, use the no form of this command.

Format ipv6 neighbors dynamicrenew

no ipv6 neighbors dynamicrenew

Default Disable

Mode Global Config

8.3.2.22. ipv6 nud

Use this command to configure Neighbor Unreachability Detection (NUD). NUD verifies that communication with a neighbor exists.

To reset to the default value, use the no form of this command.

Format ipv6 nud {backoff-multiple <1-5> | max-multicast-solicits <3-255> | max-unicast-solicits <3-10>}

no ipv6 {backoff-multiple | max-multicast-solicits | max-unicast-solicits}

Fields	Definition
backoff-multiple	Set the exponential backoff multiple to calculate time outs in NS transmissions during NUD. The value ranges from 1 to 5. 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	Set the maximal number of multicast solicits sent during NUD. The value ranges from 3 to 255.
max-unicast-solicits	Set the maximal number of unicast solicits sent during NUD. The value ranges from 3 to 10.

Default backoff-multiple: 1

max-multicast-solicits: 3

max-unicast-solicits: 3

Mode Global Config

8.3.2.23. ipv6 unreachables

Use this command to enable the generation of ICMPv6 Destination Unreachable messages. By default, the generation of ICMPv6 Destination Unreachable messages is enabled.

To prevent the generation of ICMPv6 Destination Unreachable messages, use the no form of this command.

Format ipv6 unreachables

no ipv6 unreachables

Default Enable

Mode Interface Config

8.3.2.24. ipv6 unresolved-traffic rate-limit

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.

To disable the rate limit, use the no form of this command.

Format ipv6 unresolved-traffic rate-limit <50-1024>

no ipv6 unresolved-traffic rate-limit

Default Enable

Mode Global Config

8.3.2.25. 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. To disable ICMPv6 rate limiting, set burst-interval to zero (0).

To return burst-interval and burst-size to their default values, use the no form of this command.

Format ipv6 icmp error-interval <burst-interval> [<burst-size>]

no ipv6 icmp error-interval

Fields	Definition
<burst-interval>	Specifies how often the token bucket is initialized with burst-size tokens. burst-interval is from 0 to 2147483647 milliseconds (msec).
<burst-size>	The number of ICMPv6 error messages that can be sent during one burst-interval. The range is from 1 to 200 messages.

Default burst-interval of 1000 msec

burst-size of 100 messages

Mode Global Config

8.3.2.26. clear ipv6 route counters

This command resets to zero the IPv6 routing table counters reported in the command “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

Default None

Mode Privileged Exec

8.3.2.27. ipv6 nd mtu

Use this command to set the advertised IPv6 MTU. To restore to the default value, use the no form of this command.

Format ipv6 nd mtu <1280-9394>

no ipv6 nd mtu

Default 0

Mode Interface Config

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. Show commands

8.4.1.1. show ipv6 ospf

This command displays information relevant to the OSPF router.

Some of the information below displays only if you enable OSPF and configure certain features.

Format show ipv6 ospf

Default None

Mode Privileged Exec

Display Messages

Fields	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	Shows the maximum number of non-default AS-external-LSAs entries that can be stored in the link-state database.
Exit Overflow Interval	Shows 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 auto-cost reference bandwidth configured on the router.
Default Passive Setting	Shows whether the interfaces are passive by default.

Prefix Suppression	Display whether prefix-suppression is enabled or disabled.
Maximum Paths	The maximum number of paths that OSPF can report for a given destination.
Default Metric	Default value for redistributed routes.
Maximum Routes	The maximum number of routes that OSPF can support.
Stub Router Configuration	Indicates whether stub router is configured.
BFD Mode	Indicates whether BFD is enabled or disabled.
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.
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	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 learnt 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	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 re-originates its own router LSAs, setting the cost of all non-stub interfaces to infinity. To restore OSPF to normal operation, disable and re-enable OSPF.
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	Shows the number of external (LS type 5) link-state advertisements in the link-state database.

External LSA Checksum	Shows the sum of the LS checksums of external link-state advertisements contained in the link-state database.
New LSAs Originated	Shows the number of new link-state advertisements that have been originated.
LSAs Received	Shows 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, or BGP.
Metric	The metric of the routes being redistributed.
Metric Type	Shows whether the routes are EX1 ro EX2.
Tag	The decimal value attached to each external route.
NSF Helper Support	Indicate whether helpful neighbor functionality has been enabled for OSPF for planned restarts, unplanned restarts, or Always (Both).
NSF Helper Strict LSA Checking	Indicate whether strict LAS 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.

8.4.1.2. 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

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	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.

8.4.1.3. 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>

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	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).
Stub Area Metric Value	The metric value of the stub area. This field displays only if the area is configured as a stub area.

The following OSPF NSSA specific information displays only if the area is configured as an NSSA.

Fields	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	Shows the metric value for the default route advertised into the NSSA.
Default Metric Type	Shows the metric type for the default route advertised into the NSSA.
Translator Role	Shows the NSSA translator role of the ABR, which is always or candidate.
Translator Stability Interval	Shows 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.

8.4.1.4. 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

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	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.

8.4.1.5. 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}]

Fields	Definition
<areaid>	Configures to display database information about a specific area.
<lsid>	Specify the link state ID.
<rtrid>	Specify an IP Address.

Default None

Mode Privileged Exec

User Exec

Display Messages

Fields	Definition
Link Id	A number that uniquely identifies an LSA that a router originates from all other self originated LSA's 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.
Csum	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.

8.4.1.6. show ipv6 ospf database database-summary

This command displays 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

Default None

Mode Privileged Exec

User Exec

Display Messages

Fields	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.
Subtotal	Number of entries for the identified area.
Self-Originated Type-7 Ext	Total number of self originated Type-7 external LSAs in the database.
Type-5 Ext	Total number of AS external LSAs in the database.
Self-Originated Type-5 Ext	Total number of self originated AS external LSAs in the database.
Total	Total number of router LSAs in the OSPFv3 link state database.

8.4.1.7. show ipv6 ospf interface

This command displays the information for the physical or virtual interface tables.

Format show ipv6 ospf interface {<slot/port> | loopback <0-63> | tunnel <0-7> | vlan <vlan-id>}

Fields	Definition
<slot/port>	Interface number.
<0-63>	Loopback Interface ID.

<0-7>	Tunnel Interface ID.
<vland-id>	VLAN ID. The range is from 0 to 4093.

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	Definition
IPv6 Address	Shows the IPv6 address of the interface.
ifIndex	Shows the interface index number associated with the interface.
OSPF Admin Mode	Shows whether the admin mode is enabled or disabled.
OSPF Area ID	Shows the area ID associated with this interface.
Router Priority	Shows the router priority. The router priority determines which router is the designated router.
Retransmit Interval	Shows the frequency, in seconds, at which the interface sends LSA.
Hello Interval	Shows the frequency, in seconds, at which the interface sends Hello packets.
Dead Interval	Shows the amount of time, in seconds, the interface waits before assuming a neighbor is down.
LSA Ack Interval	Shows the amount of time, in seconds, the interface waits before sending an LSA acknowledgement after receiving an LSA.
Transmit Delay Interval	A number representing the OSPF Transmit Delay for the specified interface.
Authentication Type	Shows the type of authentication the interface performs on LSAs it receives.
Metric Cost	Shows the priority of the path. Low costs have a higher priority than high costs.
Prefix-suppresion	Shows whether prefix-suppresion 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 Suppresion	Shows the configured state of Link LSA Suppresion for the interface.

The following information only displays if OSPF is initialized on the interface:

Fields	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.

8.4.1.8. show ipv6 ospf interface brief

This command displays brief information for the physical or virtual interface tables.

Format show ipv6 ospf interface brief

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	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. This is a configured value.
OSPF Area ID	Represents the OSPF Area ID for the specified interface. This is a configured value.
Router Priority	Shows 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	Shows the frequency, in seconds, at which the interface sends Hello packets.
Dead Interval	Shows the amount of time, in seconds, the interface waits before assuming a neighbor is down.
Retransmit Interval	Shows the frequency, in seconds, at which the interface sends LSA.
Retransmit Delay Interval	Shows the number of seconds the interface adds to the age of LSA packets before transmission.
LSA Ack Interval	Shows the amount of time, in seconds, the interface waits before sending an LSA acknowledgement after receiving an LSA.

8.4.1.9. show ipv6 ospf interface stats

This command displays the statistics for a specific interface. The command only displays information if OSPF is enabled

Format show ipv6 ospf interface stats {<slot/port> | loopback <loopback-id> | vlan <vlan-id>}

Fields	Definition
<slot/port>	Interface number.
<loopback-id>	The loopback ID ranges from 0 to 63.
<vlan-id>	VLAN ID. The range is from 0 to 4093.

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	Definition
OSPFv3 Area ID	The area id of this OSPF interface.
Area Border Router Count	The number of the area border router.
AS Border Router Count	The number of the AS border router.
Area LSA Count	The number of area LSAs.

IPv6 Address	The IPv6 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.
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.
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.
Hello 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.

8.4.1.10. show ipv6 ospf lsa-group

This command displays the number of self-originated LSAs within each LSA group.

Format show ipv6 ospf lsa-group

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	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.

8.4.1.11. show ipv6 ospf max-metric

This command displays the configured maximum metrics for stub router mode.

Format show ipv6 ospf max-metric

Default None

Mode Privileged Exec
User Exec

8.4.1.12. 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 **<ipaddr>** 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> | tunnel <0-7> | vlan <vlan-id>} | <ipaddr>}]

Fields	Definition
<ipaddr>	IP address of the neighbor.

<slot/port>	Interface number.
<vlan-id>	VLAN ID ranges from 1 to 4093.

Default None

Mode Privileged Exec
User Exec

Display Messages

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:

Fields	Definition
Router ID	Shows the 4-digit dotted-decimal number of the neighbor router.
Priority	Displays 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	Shows the interface ID of the neighbor.
Interface	Shows the interface of the local router.
State	Shows 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	Shows 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:

Fields	Definition
Interface	Shows 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.
Router Priority	Displays the router priority for the specified interface.
Dead Timer Due	Shows the amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.
State	Shows the state of the neighboring routers.
Events	The 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.

8.4.1.13. show ipv6 ospf range

This command displays information about the area ranges for the specified <areaid>. The <areaid> identifies the OSPFv3 area whose ranges are being displayed.

Format show ipv6 ospf range <areaid>

Fields	Definition

<areaid>	The area ID of the requested OSPFv3 area

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	Definition
Area ID	The area ID of the requested OSPFv3 area
IPv6 Prefix/Prefix Length	The summary prefix and prefix length.
Lsdb Type	The type of link advertisement associated with this area range.
Advertisement	The status of the advertisement. Advertisement has two possible settings: enabled or disabled.

8.4.1.14. show ipv6 ospf statistics

This command displays information about the 15 most recent Shortest Path First (SPF) calculations.

Format show ipv6 ospf statistics

Default None

Mode Privileged Exec
User Exec

Display Messages

The command displays the following information with the most recent statistics displayed at the end of the table.

Fields	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.
Reason	The event or events that triggered the SPF. The reaons 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.

8.4.1.15. show ipv6 ospf stub table

This command displays the OSPF stub table. The information bello will only be displayed if OSPF is initialized on the switch.

Format show ipv6 ospf stub table

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	Definition
Area ID	A 32-bit identifier for the created stub area.
Type of Service	The type of service associated with the stub metric. 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.

8.4.1.16. show ipv6 ospf virtual-link

This command displays the OSPF Virtual Interface information for a specific area and neighbor.

Format show ipv6 ospf virtual-link <areaid> <neighbor>

Fields	Definition
<areaid>	Area ID.
<neighbor>	Neighbor's router ID.

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	Definition
Area ID	The area ID of the requested OSPFv3 area.
Neighbor Router ID	The input neighbor Router ID.
Hello Interval	The configured hello interval for the OSPFv3 virtual interface.
Dead Interval	The configured dead interval for the OSPFv3 virtual interface.
Interface Transmit Delay	The configured transit delay for the OSPFv3 virtual interface.
Retransmit Interval	The configured retransmit interval for the OSPFv3 virtual interface.
State	The OSPFv3 Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router. This is the state of the OSPFv3 interface.
Metric	The OSPFv3 virtual interface metric.
Neighbor State	The neighbor state.

8.4.1.17. 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

Default None

Mode Privileged Exec
User Exec

Display Messages

Fields	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.
Transit Delay	The configured transit delay for the OSPFv3 virtual interface.

8.4.2. Configuration commands

8.4.2.1. ipv6 ospf

This command enables OSPF on a router interface or loopback interface.

To disable OSPF on a router interface or loopback interface, use the no form of this command.

Format ipv6 ospf
no ipv6 ospf

Default Disable

Mode Interface Config

8.4.2.2. ipv6 ospf area

This command sets the OSPF area to which the specified router interface belongs. The <areaid> is an 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, which does not exist on an interface, causes the area to be created with default values.

Format ipv6 ospf area {<0-4294967295> | <areaid>}

Fields	Definition
<areaid>	An 32-bit integer, formatted as a 4-digit dotted-decimal number.
<0-4294967295>	A decimal value for an area ID.

Default None

Mode Interface Config

8.4.2.3. ipv6 ospf bfd

This command enables BFD for OSPF on the specified interface.

To disable BFD for OSPF on the specified interface, use the no form of this command.

Format ipv6 ospf bfd

Default Disable

Mode Interface Config

8.4.2.4. ipv6 ospf cost

This command configures the cost on an OSPF interface. The <cost> parameter has a range of 1 to 65535.

To reset to the default cost on an OSPF interface, use the no form of this command.

Format ipv6 ospf cost <1-65535>
no ipv6 ospf cost

Default 10

Mode Interface Config

8.4.2.5. ipv6 ospf dead-interval

This command sets the OSPF dead interval for the specified interface. 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).

To set the default OSPF dead interval for the specified interface, use the no form of this command.

Format ipv6 ospf dead-interval <seconds>

no ipv6 ospf dead-interval

Fields	Definition
<seconds>	This value ranges from 1 to 65535.

Default 40

Mode Interface Config

8.4.2.6. 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.

To set the default OSPF hello interval for the specified interface, use the no form of this command.

Format ipv6 ospf hello-interval <seconds>

no ipv6 ospf hello-interval

Fields	Definition
<seconds>	This value ranges from 1 to 65535.

Default 10

Mode Interface Config

8.4.2.7. ipv6 ospf link-lsa-suppression

This command enables Link LSA Suppression on an interface. When Link LSA Suppression is enabled on a P2P interface, no Link LSA protocol packets are originated on the interface. This configuration does not apply to non-P2P interfaces.

To disables Link LSA Suppression on an interface, use the no form of this command. When Link LSA suppression is disabled, Link LSA protocol packets are originated on the P2P interfaces.

Format ipv6 ospf link-lsa-suppresion

no ipv6 ospf link-lsa-suppresion

Default Disable

Mode Interface Config

8.4.2.8. ipv6 ospf mtu-ignore

This command disables OSPF maximum transmission unit (MTU) mismatch detection. 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.

To enable the OSPF MTU mismatch detection, use the no form of this command.

Format ipv6 ospf mtu-ignore

no ipv6 ospf mtu-ignore

Default Enable

Mode Interface Config

8.4.2.9. ipv6 ospf network

This command changes the default OSPF network type for the interface. 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.

To set the interface type to the default value, use the no form of this command.

Format ipv6 ospf network {broadcast | point-to-point}

no ipv6 ospf network {broadcast | point-to-point}

Default Broadcast

Mode Interface Config

8.4.2.10. ipv6 ospf prefix-suppression

This command suppresses the advertisement of the IPv6 prefixs 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.

To remove prefix-suppression configurations for the specified interface, use the no form of this command. When this no command is issued, global prefix-suppression applies to the interface.

Format ipv6 ospf prefix-suppression [disable]

no ipv6 ospf prefix-suppression

Fields	Definition
Disable	This is for excluding specified interfaces from performing prefix-suppression when the feature is enabled globally.

Default None

Mode Interface Config

8.4.2.11. ipv6 ospf priority

This command sets the OSPF priority for the specified router interface. 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.

To set the default OSPF priority for the specified router interface, use the no form of this command.

Format ipv6 ospf priority <0-255>

no ipv6 ospf priority

Default 1, which is the highest router priority

Mode Interface Config

8.4.2.12. ipv6 ospf retransmit-interval

This command sets the OSPF retransmit Interval for the specified interface. 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.

To set the default OSPF retransmit Interval for the specified interface, use the no form of this command.

Format ipv6 ospf retransmit-interval <seconds>

no ipv6 ospf retransmit-interval

Fields	Definition
<seconds>	Valid value ranges from 0 to 3600 (1 hour).

Default 5

Mode Interface Config

8.4.2.13. ipv6 ospf transmit-delay

This command sets the OSPF Transit Delay for the specified interface. 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.

To set the default OSPF Transit Delay for the specified interface, use the no form of this command.

Format ipv6 ospf transmit-delay <seconds>

no ipv6 ospf transmit-delay

Fields	Definition
<seconds>	Valid value ranges from 1 to 3600 (1 hour).

Default 1

Mode Interface Config

8.4.2.14. ipv6 router ospf

Use this command to enter Router OSPFv3 Config mode.

Format ipv6 router ospf

Default None

Mode Global Config

8.4.2.15. area default-cost

This command configures the monetary default cost for the stub area. The operator must specify the area id and an integer value between 1-16777214.

Format area <areaid> default-cost <1-16777214>

Fields	Definition
<areaid>	Area ID.

Default None

Mode Router OSPFv3 Config

8.4.2.16. area nssa

This command configures the specified areaid to function as an NSSA.

To disable nssa from the specified area id, use the no form of this command.

Format area <areaid> nssa

no area <areaid> nssa

Fields	Definition
<areaid>	Area ID.

Default None

Mode Router OSPFv3 Config

8.4.2.17. area nssa default-info-originate

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).

To disable the default route advertised into the NSSA, use the no form of this command.

Format area <areaid> nssa default-info-originate [<1-16777214>] [{comparable | non-comparable}]

no area <areaid> nssa default-info-originate [<1-16777214>] [{comparable | non-comparable}]

Fields	Definition
<areaid>	Area ID.
<1-16777214>	The metric of the default route. The range is 1 to 16777214.
comparable	Specify the metric type as NSSA-External 1.
non-comparable	Specify the metric type as NSSA-External 2.

Default Disable

Mode Router OSPFv3 Config

8.4.2.18. area nssa no-redistribute

This command configures the NSSA ABR so that learned external routes will not be redistributed to the NSSA.

To disable the NSSA ABR so that learned external routes are redistributed to the NSSA, use the no form of this command.

Format area <areaid> nssa no-redistribute

no area <areaid> nssa no-redistribute

Fields	Definition
<areaid>	Area ID.

Default Disable

Mode Router OSPFv3 Config

8.4.2.19. area nssa no-summry

This command configures the NSSA so that summary LSAs are not advertised into the NSSA.

To disable the NSSA from the summary LSAs, use the no form of this command.

Format area <areaid> nssa no-summary

no area <areaid> nssa no-summary

Fields	Definition
<areaid>	Area ID.

Default None

Mode Router OSPFv3 Config

8.4.2.20. area nssa translator-role

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.

To disable the NSSA translator role from the specified area id, use the no form of this command.

Format area <areaid> nssa translator-role {always | candidate}

no area <areaid> nssa translator-role

Fields	Definition
<areaid>	Area ID.
always	A value of *always* will cause the router to assume the role of the translator when it becomes a border router.
Candidate	A value of *candidate* will cause the router to participate in the translator election process when it attains border router status.

Default None

Mode Router OSPFv3 Config

8.4.2.21. area nssa translator-stab-intv

This command configures the translator stability interval 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.

To disable the NSSA translator stability interval from the specified area id, use the no form of this command.

Format area <areaid> nssa translator-stab-intv <0-3600>

no area <areaid> nssa translator-stab-intv

Fields	Definition
<areaid>	Area ID.
<0-3600>	The range is 0 to 3600.

Default None

Mode Router OSPFv3 Config

8.4.2.22. area range

This command creates a specified area range for a specified NSSA. The **<ipv6-prefix>** is a valid IPv6 address. The **<prefix-length>** is a valid subnet mask. The LSDB type must be specified by either summarylink or nssaexternallink, and the advertising of the area range can be allowed or suppressed.

To delete a specified area range, use the no form of this command.

Format area <areaid> range <ipv6-prefix>/<prefix-length> {summarylink | nssaexternallink} [advertise | not-advertise]

no area <areaid> range <ipv6-prefix>/<prefix-length> {summarylink | nssaexternallink}

Fields	Definition
<areaid>	Area ID.
<ipv6-prefix>	IPv6 Address.
<prefix-length>	The subnetmask of the IPv6 address.
summarylink	The area range is used when summarizing prefixes advertised in type 3 summary LSAs.
nssaexternallink	The area range is used when translating type 7 LSAs to type 5 LSAs.
advertise	Allow advertising the specified area range. When this option is specified, the summary link is advertised when the area range is active. This is default.
not-advertise	Disallow advertising the specified area range. When this option is specified, neither the summary prefix nor the contained prefixes are advertised when the area range is active.

Default None

Mode Router OSPFv3 Config

8.4.2.23. area stub

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.

To delete a stub area for the specified area ID, use the no form of this command.

Format area <areaid> stub

no area <areaid> stub

Fields	Definition
<areaid>	Area ID.

Default None

Mode Router OSPFv3 Config

8.4.2.24. area stub no-summary

This command disables the import of Summary LSAs for the stub area identified by the specified area ID.

To sets the Summary LSA import mode to the default for the stub area identified by the specified area ID, use the no form of this command.

Format area <areaid> stub no-summary

no area <areaid> stub no-summary

Fields	Definition
<areaid>	Area ID.

Default Enable

Mode Router OSPFv3 Config

8.4.2.25. area virtual-link

This command creates the OSPF virtual interface for the specified <areaid> and <neighbor>. The <neighborid> parameter is the Router ID of the neighbor.

To delete the OSPF virtual interface from the given interface identified by **<areaid>** and **<neighborid>**, use the no form of this command.

Format area <areaid> virtual-link <neighborid>

no area <areaid> virtual-link <neighborid>

Fields	Definition
<areaid>	Area ID.

<neighborid>	Router ID of the neighbor.

Default The default authentication type is none

Mode Router OSPFv3 Config

8.4.2.26. area virtual-link dead-interval

This command configures the dead interval for the OSPF virtual interface on the virtual interface identified by **<areaid>** and **<neighborid>**.

To configures the default dead interval for the OSPF virtual interface on the virtual interface identified by **<areaid>** and **<neighbor>**, use the no form of this command.

Format area <areaid> virtual-link <neighborid> dead-interval <1-65535>

no area <areaid> virtual-link <neighborid> dead-interval

Fields	Definition
<areaid>	Area ID.
<neighborid>	Router ID of the neighbor.
<1-65535>	The range of the dead interval is 1 to 65535, in seconds.

Default 40 seconds

Mode Router OSPFv3 Config

8.4.2.27. area virtual-link hello-interval

This command configures the hello interval for the OSPF virtual interface on the interface identified by **<areaid>** and **<neighborid>**.

To configures the default hello interval for the OSPF virtual interface on the virtual interface identified by **<areaid>** and **<neighbor>**, use the no form of this command.

Format area <areaid> virtual-link <neighborid> hello-interval <1-65535>

no area <areaid> virtual-link <neighborid> hello-interval

Fields	Definition
<areaid>	Area ID.

<neighborid>	Router ID of the neighbor.
<1-65535>	The range of the dead interval is 1 to 65535, in seconds.

Default 10 seconds

Mode Router OSPFv3 Config

8.4.2.28. area virtual-link retransmit-interval

This command configures the retransmit interval for the OSPF virtual interface on the interface identified by **<areaid>** and **<neighborid>**.

To configures the default retransmit interval for the OSPF virtual interface on the virtual interface identified by **<areaid>** and **<neighbor>**, use the no form of this command.

Format area <areaid> virtual-link <neighborid> retransmit-interval <0-3600>

no area <areaid> virtual-link <neighborid> retransmit-interval

Fields	Definition
<areaid>	Area ID.
<neighborid>	Router ID of the neighbor.
<0-3600>	The range of the retransmit interval is 0 to 3600, in seconds.

Default 5 seconds

Mode Router OSPFv3 Config

8.4.2.29. area virtual-link transmit-delay

This command configures the transmit delay for the OSPF virtual interface on the virtual interface identified by **<areaid>** and **<neighborid>**.

To configures the default transmit delay for the OSPF virtual interface on the virtual interface identified by **<areaid>** and **<neighbor>**, use the no form of this command.

Format area <areaid> virtual-link <neighborid> transmit-delay <0-3600>

no area <areaid> virtual-link <neighborid> transmit-delay

Fields	Definition
<areaid>	Area ID.
<neighborid>	Router ID of the neighbor.
<0-3600>	The range of the retransmit interval is 0 to 3600, in seconds.

Default 1 seconds

Mode Router OSPFv3 Config

8.4.2.30. auto-cost reference-bandwidth

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. The different reference bandwidth can be independently configured for OSPFv2 and OSPFv3.

To set the reference bandwidth to the default value, use the no form of this command.

Format auto-cost reference-bandwidth <1-4294967>

no auto-cost reference-bandwidth

Fields	Definition
<1-4294967>	The range of reference bandwidth.

Default 100Mbps

Mode Router OSPFv3 Config

8.4.2.31. bfd

This command configures BFD for all interfaces.

To reset BFD for interfaces to default, use the no form of this command.

Format bfd

no bfd

Default Disable

Mode Router OSPFv3 Config

8.4.2.32. default-information originate

This command is used to control the advertisement of default routes.

To configure the default advertisement of default routes, use the no form of this command.

Format default-information originate [always] [metric <1-16777214>] [metric-type {1 | 2}]

no default-information originate

Fields	Definition
[always]	Specify this option to roginate default route without depending on wheterh routing table has a default route.
metric	The range of the metric is 1 to 16777214.
metric type	The value of metric type is type 1 or type 2.

Default Metric: unspecified

Type: 2

Mode Router OSPFv3 Config

8.4.2.33. default-metric

This command is used to set a default for the metric of distributed routes.

To set a default for the metric of distributed routes, use the no form of this command.

Format default-metric <1- 16777214>

no default-metric

Fields	Definition
<1-16777214>	The range of default metric is 1 to 16777214.

Default None

Mode Router OSPFv3 Config

8.4.2.34. distance 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 can be intra, inter, or external. All the external type routes are given the same preference value. The <preference> range is 1 to 255. A route with a preference of 255 cannot be used to forward traffic.

To set the default route preference value of OSPF in the router, use the no form of this command.

Format distance ospf {intra-area <1-255> | inter-area <1-255> | external <1-255>}

no distance ospf {intra-area | inter-area | external }

Fields	Definition
<1-255>	The range of preference value.

Default 110

Mode Router OSPFv3 Config

8.4.2.35. enable

This command resets the default administrative mode of OSPF in the router (active).

To set the administrative mode of OSPF in the router to inactive, use the no form of this command.

Format enable

no enable

Default Enable

Mode Router OSPFv3 Config

8.4.2.36. exit-overflow-interval

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.

To configure the default exit overflow interval for OSPF, use the no form of this command.

Format exit-overflow-interval <0-2147483647>

no exit-overflow-interval

Fields	Definition
<0-2147483647>	The range of exit overflow interval for OSPF, in seconds.

Default 0

Mode Router OSPFv3 Config

8.4.2.37. external-isdb-limit

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 its database. The external LSDB limit MUST be set identically in all routers attached to the OSPF backbone and/or any regular OSPF area.

To configure the default external LSDB limit for OSPF, use the no form of this command.

Format external-lsdb-limit <-1-2147483647>

no external-lsdb-limit

Fields	Definition
<0-2147483647>	The range of external LSDB limit for OSPF is -1 to 2147483647.

Default -1

Mode Router OSPFv3 Config

8.4.2.38. max-metric

This command sets the number of paths that OSPF can report for a given destination where <maxpaths> is platform dependent.

To disable stub router mode, use the no form of this command. The command clears either type of stub router mode (always or on-startup) and resets all LSA options.

Format max-metric router-lsa [on-startup <5-86400>] [summary-lsa [<1-16777215>]] [external-lsa [<1-16777215>]] [inter-area-lsas [<1-16777215>]]

no max-metric router-lsa [on-startup] [summary-lsa] [external-lsa] [inter-area-lsas]

Fields	Definition

on-startup	OSPF starts in stub router mode after a reboot.
<5-86400>	The number of seconds that OSPF remains in stub router mode after a reboot. The range is from 5 to 86,400 seconds. There is no default value.
summary-lsa	Set the maximum metric value for summary LSAs. The range is from 1-16777215.
external-lsa	Set the maximum metric value for external LSAs. The range is from 1-16777215.
Inter-area-lsas	Set the maximum metric value for inter-area LSAs. The range is from 1-16777215.

Default OSPF is not in stub router mode by default

Mode Router OSPFv3 Config

8.4.2.39. maximum-paths

This command sets the number of paths that OSPF can report for a given destination where <maxpaths> is platform dependent.

To resets the number of paths that OSPF can report for a given destination back to its default value, use the no form of this command.

Format maximum-paths <1-48>

no maximum-paths

Fields	Definition
<1-48>	The maximum number of paths that OSPF can report for a given destination. The range of the value is 1 to 48.

Default 1

Mode Router OSPFv3 Config

8.4.2.40. passive-interface default

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.

To disable the global passive mode by default for all interfaces, use the no form of this command. Any interface previously configured to be passive reverts to non-passive mode.

Format passive-interface default

no passive-interface default

Default Disable

Mode Router OSPFv3 Config

8.4.2.41. passive-interface

Use this command to set the interface or tunnel as passive. It overrides the global passive mode that is currently effective on the interface or tunnel.

To set the interface or tunnel as non-passive, use the no form of this command. It overrides the global passive mode that is currently effective on the interface or tunnel.

Format passive-interface {< slot/port> | tunnel <tunnel-id> | vlan <vlan-id>}

no passive-interface {< slot/port> | tunnel <tunnel-id> | vlan <vlan-id>}

Fields	Definition
<slot/port>	Specify the interface.
<tunnel-id >	Specify the Tunnel ID. Range 0 -7.
<vlan-id>	Specifies the VLAN interface. The range of the VLAN ID is 1 to 4093.

Default Disable

Mode Router OSPFv3 Config

8.4.2.42. prefix-suppression

This command enables the global prefix suppression for OSPFv3.

To disable the global prefix suppression for OSPFv3, use the no form of this command.

Format prefix-suppression

Default Disable

Mode Router OSPFv3 Config

8.4.2.43. redistribute

This command configures the OSPFv3 protocol to allow redistribution of routes from the specified source protocol/routers.

To configure OSPF to prohibit redistribution of routes from the specified soure protocol/rotuers, use the no form of this command.

Format redistribute {static | connected | bgp} [metric <0-16777214>] [metric-type {1 | 2}] [tag <0-4294967295>]

no redistribute { static | connected| bgp} [metric] [metric-type] [tag]

Fields	Definition
<0-16777214>	The range of metric is 0 to 16777214.
<0-4294967295>	The range of tag is 0 to 4294967295.

Default Metric is unspecified

Type is 2

Tag is 0

Mode Router OSPFv3 Config

8.4.2.44. router-id

This command sets a 4-digit dotted-decimal number uniquely identifying the router ospf id.

Format router-id <ipaddress>

Fields	Definition
<ipaddress>	IP Address.

Default None

Mode Router OSPFv3 Config

8.4.2.45. clear ipv6 ospf

This command disable and reenable OSPF.

Format clear ipv6 ospf

Default None

Mode Privileged Exec

8.4.2.46. clear ipv6 ospf configuration

This command resets the OSPF configuration to factory defaults.

Format clear ipv6 ospf configuration

Default None

Mode Privileged Exec

8.4.2.47. clear ipv6 ospf counters

This command reset global and interface statistics.

Format clear ipv6 ospf counters

Default None

Mode Privileged Exec

8.4.2.48. clear ipv6 ospf neighbor

This command drops the adjacency with all OSPF neighbors. On each neighbor's interface, send a oneway hello. Adjacencies may then be established. To drop all adjacencies with a specific router ID, specify the neighbor's Router ID using the optional parameter <ipaddr>

Format clear ipv6 ospf neighbor [<ipaddr>]

Fields	Definition
<ipaddr>	Neighbor's Router ID.

Default None

Mode Privileged Exec

8.4.2.49. clear ipv6 ospf neighbor interface

This command drops the adjacency with all OSPF neighbors on a specific interface. To drop adjacency with a specific router ID on a specific interface, specify the neighbor's Router ID using the optional parameter <ipaddr>.

Format clear ipv6 ospf neighbor interface {<slot/port> | vlan <1-4093>} [ipaddr]

Fields	Definition
<slot/port>	Specify the interface.
<1-4093>	Specifies the VLAN interface. The range of the VLAN ID is 1 to 4093.
<ipaddr>	Neighbor's Router ID.

Default None

Mode Privileged Exec

8.4.2.50. clear ipv6 ospf redistribution

This command flushes all self-originated external LSAs. Reapply the redistribution configuration and reoriginate prefixes as necessary.

Format clear ipv6 ospf redistribution

Default None

Mode Privileged Exec

8.4.2.51. clear ipv6 ospf stub-router

This command forces 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 if it 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

Default None

Mode Privileged Exec

8.5. Routing Policy Commands

8.5.1. Show commands

8.5.1.1. 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 sequencenumber] [longer] [first-match]

Default None

Mode Privileged Exec

Display Message

Fields	Definition
detail | summary	(Optional) Displays detailed or summarized information about all prefix lists.
listname	(Optional) The name of a specific prefix list.
ipv6-prefix/prefixlength	(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.

The command outputs the following information:

Fields	Definition
count	Mumber of entries in the prefix list.
range entries	Mumber of entries that match the input range.
ref count	Mumber 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.

8.5.2. Configuration commands

8.5.2.1. ipv6 prefix-list

To create a IPv6 prefix list or add a prefix list entry, use the **ipv6 prefix-list** command in Global Configuration mode. 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 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.

An IPv6 prefix list may be used within a route map to match a route's prefix using the command "match ipv6 address" A route map may contain both IPv4 and IPv6 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.

To delete a IPv6 prefix list or a statement in a prefix list, use the **no** form of this command. The command **no ipv6 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 ipv6 prefix-list <list-name> {[seq <seq number>] {permit | deny} ip6-prefix/prefix-length [ge <length>] [le <length>] | description <text> | renumber [<renumber-interval> [<first-statement-number>]]}

no ipv6 prefix-list <list-name> {[seq <seq number>] {permit | deny} ip6-prefix/prefix-length [ge <length>] [le <length>] | description}

Fields	Definition
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 IPv6 prefix where the address is specified in hexadecimal using 16-bit values between colons. The prefix-length is 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.
<renumber-interval> **<first-statement-number>**	(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. The valid range for renumber-interval is 1 - 100, and the valid range for first-statement-number is 1 - 1000

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.

Mode Global Config

8.5.2.2. match ipv6 address

Use this command to configure a route map to match based on a destination prefix. *prefix-list prefix-listname* identifies the name of an IPv6 prefix list used to identify the set of matching routes. Up to eight prefix lists may be specified. If multiple prefix lists are specified, a match occurs if a prefix matches any one of the prefix lists. If you configure a match ipv6 address statement within a route map section that already has a match ipv6 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.

To delete a match statement from a route map, use the **no** form of this command.

Format match ipv6 address prefix-list <list-name> [list-name...]

no match ipv6 address prefix-list <list-name> [list-name...]

Default No match criteria are defined by default

Mode Route Map Config

Display Messages

Fields	Definition
list-name	The name of a prefix list used to identify the set of matching routes. Up to eight prefix lists may be specified.

8.5.2.3. set ipv6 next-hop

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.

To remove a set command from a route map, use the **no** form of this command.

Format set ipv6 next-hop <next-hop-ipv6-address >

no set ipv6 next-hop

Default None

Mode Route Map Config

Display Messages

Fields	Definition
next-hop-ipv6-address	The IPv6 address set as the Network Address of Next Hop field in the MP_NLRI attribute of an UPDATE message.

8.5.2.4. 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 [list-name] [ipv6-prefix/prefix-length]

Mode Privileged Exec

Display Messages

Fields	Definition
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.

8.6. DHCPv6 Snooping Commands

DHCPv6 snooping is a security feature that monitors DHCPv6 messages between a DHCPv6 client and DHCPv6 servers to filter harmful DHCPv6 messages and to build a bindings database of {MAC address, IPv6 address, VLAN ID, port} tuples that are considered authorized. You can enable DHCPv6 snooping globally and on specific VLANs, and configure ports within the VLAN to be trusted or untrusted. DHCPv6 servers must be reached through trusted ports.

DHCPv6 snooping enforces the following security rules:

DHCPv6 packets from a DHCPv6 server (Advertise and Reply) are dropped if received on an untrusted port.

DHCPv6 Release and DHCPv6 Decline messages are dropped if for a MAC address in the snooping database, but the binding's interface is other than the interface where the message was received.

DHCPv6 Snooping doe not support the DHCPv6 relay function, and other behaviors are the same as DHCP Snooping. For more information, refer to the DHCP Snooping Commands section.

8.6.1. show ipv6 dhcp snooping

This command displays the DHCPv6 snooping global configurations and summaries of port configurations.

Format show ipv6 dhcp snooping

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show ipv6 dhcp snooping

DHCP snooping is Enabled
DHCP snooping source MAC verification is enabled
DHCP snooping is enabled on the following VLANs:
1

 Interface    Trusted     Log Invalid Pkts
-----------  ----------   ----------------
0/1          Yes          No
0/2          No           No
0/3          No           No
0/4          No           No
0/5          No           No
0/6          No           No
0/7          No           No
0/8          No           No
0/9          No           No
0/10         No           No
0/11         No           No
0/12         No           No
0/13         No           No
0/14         No           No
0/15         No           No
```

```
(M4500-32C) #
```

8.6.2. show ipv6 dhcp snooping per interface

This command displays the DHCPv6 snooping detail configurations for all interfaces or for a specific interface.

Format show ipv6 dhcp snooping interfaces [<slot/port> | port-channel <portchannel-id>]

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show ipv6 dhcp snooping interfaces

Interface     Trust State     Rate Limit      Burst Interval
                                 (pps)          (seconds)
----------   -------------   -------------   ---------------
0/1          Yes             None            N/A
0/2          No              None            N/A
0/3          No              None            N/A
0/4          No              None            N/A
0/5          No              None            N/A
0/6          No              None            N/A
0/7          No              None            N/A
0/8          No              None            N/A
0/9          No              None            N/A
0/10         No              None            N/A
0/11         No              None            N/A
0/12         No              None            N/A
0/13         No              None            N/A
0/14         No              None            N/A
0/15         No              None            N/A
0/16         No              None            N/A
0/17         No              None            N/A
0/18         No              None            N/A
0/19         No              None            N/A

(M4500-32C) #
```

8.6.3. show ipv6 dhcp snooping binding

This command displays the DHCP Snooping binding entries.

The parameter “static” means to restrict the output based on static entries which are added by user manually.

The parameter “static” means to restrict the output based on dynamic entries which are added by DHCPv6 Snooping automatically

Format show ipv6 dhcp snooping binding [{static | dynamic}] [interface {<slot/port> | port-channel <portchannel-id>}] [vlan <vlan-id>]

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show ipv6 dhcp snooping binding

Total number of bindings:  363
Total number of Tentative bindings:  61

   MAC Address         IPv6 Address                VLAN   Interface    Type    Lease (Secs)
-----------------  ------------------------------  ----  -----------  -------  -----------
44:0A:A7:8A:00:00  2001::100                       1         0/10  DYNAMIC        86383
44:0A:A7:8A:00:01  2001::101                       1         0/10  DYNAMIC        86383
44:0A:A7:8A:00:02  2001::102                       1         0/10  DYNAMIC        86383
44:0A:A7:8A:00:03  2001::103                       1         0/10  DYNAMIC        86383
44:0A:A7:8A:00:04  2001::104                       1         0/10  DYNAMIC        86383
44:0A:A7:8A:00:05  2001::105                       1         0/10  DYNAMIC        86383
44:0A:A7:8A:01:00  2001::106                       1         0/10  DYNAMIC        86383
44:0A:A7:8A:01:01  2001::107                       1         0/10  DYNAMIC        86383
44:0A:A7:8A:01:02  2001::108                       1         0/10  DYNAMIC        86383
44:0A:A7:8A:01:03  2001::109                       1         0/10  DYNAMIC        86383
44:0A:A7:8A:01:04  2001::111                       1         0/10  DYNAMIC        86383
44:0A:A7:8A:01:05  2001::112                       1         0/10  DYNAMIC        86383
44:0A:A7:8A:02:00  2001::113                       1         0/10  DYNAMIC        86383
44:0A:A7:8A:02:01  2001::114                       1         0/10  DYNAMIC        86383
44:0A:A7:8A:02:02  2001::115                       1         0/10  DYNAMIC        86383
44:0A:A7:8A:02:03  2001::116                       1         0/10  DYNAMIC        86383

 (M4500-32C) #
```

8.6.4. show ipv6 dhcp snooping database

This command displays the DHCPv6 Snooping configuration related to the database persistency.

Format show ipv6 dhcp snooping database

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show ipv6 dhcp snooping database

agent url:  local

write-delay:  300

(M4500-32C) #
```

8.6.5. ipv6 dhcp snooping

This command enables or disables the DHCPv6 Snooping globally.

Format [no] ipv6 dhcp snooping

Default Disabled

Mode Global Config

8.6.6. ipv6 dhcp snooping vlan

This command enables or disables the DHCPv6 Snooping to the specific VLAN.

Format [no] ipv6 dhcp snooping vlan <vlan-list>

Default Disabled

Mode Global Config

8.6.7. ipv6 dhcp snooping verify mac-address

This command enables or disables the verification of the source MAC address with the client hardware address in the received DHCPv6 message.

Format [no] ipv6 dhcp snooping verify mac-address

Default Disabled

Mode Global Config

8.6.8. ipv6 dhcp snooping database

This command configures the persistent location of the DHCPv6 Snooping database. This can be local or a remote file on a given IP machine.

The parameter “local” means to set database access inside device.

The parameter “tftp://hostIP/filename” means to set database access on remote TFTP Server.

Format ipv6 dhcp snooping database {local | <url>}

Default local

Mode Global Config

8.6.9. ipv6 dhcp snooping database write-delay

This command configures the interval in seconds at which the DHCPv6 Snooping database will be persisted, and this database stores the results of DHCPv6 snooping bindings. Use keyword “no” to restore the default value of this command.

The parameter “<interval>” value ranges is from 15 to 86400 seconds.

Format ipv6 dhcp snooping database write-delay <interval>

no ipv6 dhcp snooping database write-delay

Default 300

Mode Global Config

8.6.10. ipv6 dhcp snooping binding

This command configures the static DHCPv6 Snooping binding which binds a MAC address to assigned IPv6 address on a specific VLAN ID and interface. Use keyword “no” to remove an existing entry of DHCPv6 Snooping binding.

Format ipv6 dhcp snooping binding <mac-address> vlan <vlan id> <ipv6 address> interface {<slot/port> | port-channel < portchannel-id>}

no ipv6 dhcp snooping binding <mac-address>

Default None

Mode Global Config

Example: To add a static entry of DHCPv6 snooping binding which binds MAC address 00:11:22:33:44:55 to IPv6 address 2001::1 on vlan 1 and port interface 0/1.

```
(M4500-32C) #configure
(M4500-32C) (Config)#ipv6 dhcp snooping binding 00:11:22:33:44:55 vlan 1 2001::1 interface 0/1
(M4500-32C) (Config)#
```

8.6.11. ipv6 dhcp snooping limit

This command controls the rate at which the DHCPv6 Snooping messages come. If packet rate exceeds limitation over burst interval, the assigned port will shut down automatically. User could use interface command “shutdown” and then “no shutdown” to recover it. Use keyword “no” to restore the default value of this command.

The parameter “rate” means to the limitation of packet rate. Its range is from 0 to 300 packets per second.

The parameter “burst interval” means the time interval of packet burst could be over rate limitation. Its range is from 1 to 15 seconds.

Format ipv6 dhcp snooping limit {rate <pps> [burst interval <seconds>]} | none

no ipv6 dhcp snooping limit rate

Default “rate” is None

“burst interval” is 1 second.

Mode Interface Config

Example: While the packet rate of DHCPv6 message received from port 0/1 exceeds 100 pps and consecutive time interval is over 10 seconds, the port 0/1 will be shutdown automatically.

```
(M4500-32C) #configure
(M4500-32C) (Config)#interface 0/1
(M4500-32C) (Interface 0/1)# ipv6 dhcp snooping limit rate 100 burst interval 10
(M4500-32C) (Interface 0/1)#
```

8.6.12. ipv6 dhcp snooping log-invalid

This command controls logging the illegal DHCPv6 messages to logging buffer.

Format [no] ipv6 dhcp snooping log-invalid

Default Disabled

Mode Interface Config

8.6.13. ipv6 dhcp snooping trust

This command enables or disables a port as DHCPv6 Snooping trust port.

Format [no] ipv6 dhcp snooping trust

Default Disabled

Mode Interface Config

8.6.14. clear ipv6 dhcp snooping binding

This command is used to clear all DHCPv6 Snooping bindings on all interfaces or on a specific interface.

Format clear ipv6 dhcp snooping binding [interface <slot/port>]

Default None

Mode Privileged EXEC

8.6.15. clear ipv6 dhcp snooping statistics

This command is used to clear all DHCPv6 Snooping statistics.

Format clear ipv6 dhcp snooping statistics

Default None

Mode Privileged EXEC

8.6.16. show ipv6 dhcp snooping statistics

This command displays the statistics of DHCPv6 snooping.

Format show ipv6 dhcp snooping statistics

Mode Privileged Exec

Display Message

Fields	Definition
Interface	The IPv6 address of the interface.
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.
DHCP Server Msgs Rec'd	Represents the number of DHCP server messages received on untrusted ports.

8.6.17. show ipv6 dhcp binding

This command displays the DHCPv6 binding information.

Format show ipv6 dhcp binding [<ipv6-address>]

Mode Privileged Exec

8.6.18. clear ipv6 dhcp binding

This command clears ipv6 dhcp bindings.

Format clear ipv6 dhcp binding [<ipv6-address>]

Default None

Mode Privileged Exec

8.7. DHCPv6 Commands

8.7.1. show ipv6 dhcp interface

This command displays the DHCPv6 information for the specific interface.

Format show ipv6 dhcp interface {<slot/port> | vlan <vlan-id>} [statistics]

Default None

Mode Privileged Exec

Example:

```
(M4500-32C) #show ipv6 dhcp interface 0/1

IPv6 Interface.............................. 0/1
Mode........................................ Relay
Relay Address............................... ::
Relay Interface Number...................... 0/2
Relay Remote ID.............................
Option Flags................................
```

8.7.2. show ipv6 dhcp statistics

This command displays the DHCPv6 statistics for all interfaces.

Format show ipv6 dhcp statistics

Default None

Mode Privileged Exec

Example:

```
DHCPv6 Interface Global Statistics
----------------------------------
DHCPv6 Solicit Packets Received............... 0
DHCPv6 Request Packets Received............... 0
DHCPv6 Confirm Packets Received............... 0
DHCPv6 Renew Packets Received................. 0
DHCPv6 Rebind Packets Received................ 0
DHCPv6 Release Packets Received............... 0
DHCPv6 Decline Packets Received............... 0
DHCPv6 Inform Packets Received................ 0
DHCPv6 Relay-forward Packets Received......... 0
DHCPv6 Relay-reply Packets Received........... 0
DHCPv6 Malformed Packets Received............. 0
Received DHCPv6 Packets Discarded............. 0
Total DHCPv6 Packets Received................. 0
DHCPv6 Advertisement Packets Transmitted...... 0
```

```
DHCPv6 Reply Packets Transmitted.............. 0
DHCPv6 Reconfig Packets Transmitted........... 0
DHCPv6 Relay-reply Packets Transmitted........ 0
DHCPv6 Relay-forward Packets Transmitted...... 0
Total DHCPv6 Packets Transmitted.............. 0
```

8.7.3. ipv6 dhcp relay destination

This command configures an interface for DHCPv6 relay functionality on an interface or range of interfaces. Use the *destination* keyword to set the relay server IPv6 address. Use the *interface* keyword to set the relay server interface. Use the *remote-id* keyword to add the Relay Agent Information Option “remote ID”suboption to relayed messages. It can either be DUID plus IFID or a user-defined string.

If *relay-address* is an IPv6 global address, *relay-interface* is not required. If *relay-address* is a link-local address, *relay-interface* is required.

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

Fields	Definition
relay-address	IPv6 address of a DHCPv6 relay server
relay-interface	The interface to reach a relay server
duid-ifid	Specify that the remote ID is derived from the DHCPv6 server DUID and the relay interface

Default None

Mode Interface Config

8.7.4. ipv6 dhcp relay interface

This command configures the relay interface to reach a relay server. Use the *remote-id* keyword to add the Relay Agent Information Option “remote ID”suboption to relayed messages. It can either be DUID plus IFID or a user-defined string.

Format ipv6 dhcp relay interface <relay-interface> [remote-id {<user-defined-string> | duid-ifid}]

Default None

Mode Interface Config

8.7.5. service dhcpv6

This command enables the DHCPV6 relay. Use the no form of this command to disable the DHCPV6 relay.

Format service dhcpv6

no service dhcpv6

Default Disabled

Mode Global Config

9. Data Center Bridging Commands

9.1. FIP Snooping

9.1.1. show fip-snooping

This command displays information about the global FIP snooping configuration and status.

Format show fip-snooping

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
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.

9.1.2. show fip-snooping enode

This command displays the information about the interfaces connected to ENodes.

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.

Format show fip-snooping enode <enode-mac>

Fields	Definition
<enode-mac>	MAC address of the ENode to dispaly.

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
Interface	Interface to which the ENode is connected.
VLAN	ID number of the VLAN to which the ENode belongs.
Name-ID	Name of the ENode.
ENode-MAC	MAC address of the ENode.
FCFs	Number of FCFs connected.
Session Established	Number of successful virtual connections established.

The command displays the following additional information when the optional argument is supplied.

Fields	Definition
Sessions Waiting	Number of virtual connections waiting for FCF acceptance.
Session 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 ENode.

9.1.3. show fip-snooping sessions

This command displays information about the active FIP snooping sessions.

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.

Format show fip-snooping sessions [[[vlan <1-4093> | [interface <slot/port>] | [fcf <fcf-mac> [enode <enode-mac>]]] [detail]]

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
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.
FCID	Fiber channel ID number of the virtual port that was created by 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.

Fields	Definition
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:

Fields	Definition
Interface	The 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:

Fields	Definition
Interface	The 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 associated VLAN.
Waiting	Total number of virtual connections waiting for FCF acceptance in the associated VLAN.

Session Information:

Fields	Definition
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.
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 number of hours, and **z** represents minutes elapsed following this successful virtual session. This field has no useful information for waiting sessions.

9.1.4. show fip-snooping fcf

This command displays information about the interfaces connected to FCFs.

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.

Format show fip-snooping fcf [fcf-mac]

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
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.

Fields	Definition
Sessions	Total number of virtual sessions accepted by FCF in the assocated VLAN.
D-bit	This reflects the value of the D-bit provided by the most recently received Discovery Adtvertisements 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 Advertisement sent by FCF. When D-bit is set to 1, switch discards snopped 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 Adtvertisements 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 login.
Priority	The priority returned from the FCF in 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 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.

9.1.5. show fip-snooping vlan

This command displays the FCoE VLANs information, and additionally, the FIP snooping port status when optional argument is specified.

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.

Format show fip-snooping vlan [<1-4093>]

Fields	Definition
<1 - 4093>	VLAN ID.

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
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.

9.1.6. show fip-snooping statistics

This command displays 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. When an interface is provided as an argument, interface applicable statistics are only displayed.

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.

Format show fip-snooping statistics [interface <slot/port> | vlan <1-4093>]

Fields	Definition
<slot/port>	Specify the interface.
<1-4093>	Specifies the VLAN interface. The range of the VLAN ID is 1 to 4093.

Default None

Mode Privileged EXEC

Display Message

The following table describes the packet counters per FIP operation.

Fields	Definition
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 Discovery Logins accepted on the VLAN.
FDISC_RJT	Number of Fabric Discovery Logins 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.

Fields	Definition
Number of Virtual Session Timeouts	Number of Virtual sessions removed due to session timer expiry.
Number of FCF Session Timeouts	Number of Active sessions time 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 Session 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 Session 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 Session 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.

9.1.7. feature fip-snooping

This command globally enables Fiber Channel over Ethernet Initialization Protocol (FIP) snooping on the switch. When FIP snooping is globally 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.

To return the settings to the default values and globally disable FIP snooping, use the **no** form of this command. 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 feature fip-snooping

no feature fip-snooping

Default Disable

Mode Global Config

9.1.8. fip-snooping enable

This command enables FIP snooping on the configured VLAN. 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 *feature fip-snooping* command. Otherwise, it does not appear in the CLI.

To return the mode to the default (disabled), use the **no** form of this command.

Format fip-snooping enable

no fip-snooping enable

Default Disable

Mode VLAN Config

9.1.9. fip-snooping fc-map

This command configures the FP-MAP value on a VLAN. The FC map value is used to help in securing the swith 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 values 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 *feature fip-snooping* command. Otherwise, it does not appear in the CLI.

To set the FC-MAP value for the VLAN to the default value, use the **no** form of this command.

Format fip-snooping fc-map <0x0-0xffffff>

no fip-snooping fc-map

Fields	Definition
<0x0-0xffffff>	Valid FC map values are in the range of 0x0 to 0xffffff.

Default 0x0efc00

Mode VLAN Config

9.1.10. fip-snooping port-mode fcf

This command configures the interface that is connected towards FCF. To relay the FIP packets received from the hosts toward the FCF, the switch needs to know the interfaces to which the FCFs are connected. 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 propogate it to the CNAs on the downstream (host-facing) ports. Intefaces 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 *feature fip-snooping* command. Otherwise, it does not appear in the CLI.

To set the interface to be connected towards the host, use the **no** form of this command.

Format fip-snooping port-mode fcf

no fip-snooping port-mode fcf

Default Configuration as a host-facing interface

Mode Interface Config

9.1.11. clear fip-snooping statistics

This command clears 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.

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.

Format clear fip-snooping statistics [interface <slot/port> | vlan <1-4093>]

Fields	Definition
<slot/port>	Specifies the interface.
<1-4093>	Specifies the VLAN interface. The range of the VLAN ID is 1 to 4093.

Default Disable

Mode Privileged Exec

9.2. Priority-based Flow Control

9.2.1. show interface priority-flow-control

This command displays the PFC information of a given interface or all interfaces.

Format show interface [<slot/port] priority-flow-control

Fields	Definition
<slot/port>	Interface number.

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
Interface Detail	The port for which data is displayed.
Operational State	The operational status of the interface.
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 pause.
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.
Operational 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 allowed delay on 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 duplicated 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 example shows the CLI display output for the command *show interface priority-flow-control*.

```
(M4500-32C) #show interface priority-flow-control

Port    Drop              No-Drop           Operational
        Priorities        Priorities        Status
------  ----------------  ----------------  -----------
0/1     0-7                                 Inactive
0/2     0-7                                 Inactive
0/3     0-7                                 Inactive
0/4     0-7                                 Inactive
0/5     0-7                                 Inactive
0/6     0-7                                 Inactive
0/7     0-7                                 Inactive

Port:  all physical interfaces
Operational Status:  Active/Inactive
```

9.2.2. priority-flow-control mode

This command enables or disables Priority-Flow-Control (PFC) on the given interface.

To return the mode to the default, use the **no** form of this command. VLAN tagging must be enabled on the interface in order to carry the dot1p value through the network. Additionally, the dot1p mapping 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.

Format priority-flow-control mode { on | off}

no priority-flow-control mode

Default Off

Mode DCB (Data Center Bridging) interface mode

9.2.3. priority-flow-control priority

This command enables or disables 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 users must configure the same no-drop priorities across the network in order to ensure end-to-end lossless behavior.

This command has no effect on interfaces not enabled of PFC. VLAN tagging needs to be turned on in order to carry the dot1p value through the network. Additionally, the dot1p mapping to class-of-service must be set to one-to-one.

To enable lossy behavior on all priorities on the interface, use the **no** form of this command. This has no effect on interfaces not enabled for PFC or with no lossless priorities configured.

Format priority-flow-control priority <0-7> { drop | no-drop }

no priority-flow-control priority

Fields	Definition
<drop>	Disable lossless behavior on the selected priorities.
<no-drop>	Enable lossless behavior on the selected priorities.

Default The default behavior for all priorities is drop

Mode DCB (Data Center Bridging) interface mode

9.2.4. clear priority-flow-control statistics

This command clears all global and interface PFC statistics

Format clear priority-flow-control statistics

Mode Privileged Exec

9.3. OpenFlow

9.3.1. show openflow

This command displays the OpenFlow feature status and configuration information.

Format show openflow

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
Administrative Mode	The OpenFlow feature administrative mode set by the command "*openflow enable*".
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 command "*openflow ip-mode*". The IP mode can be **Auto**, **Static**, or **ServicePort IP**.
Static IP Address	Static IP address assigned by the command "*openflow static-ip*".
OpenFlow Variant	OpenFlow Protocol Variant. The OpenFlow protocol can be 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 command "*openflow passive-mode*".

9.3.2. show openflow configured controller

This command displays a list of configured OpenFlow controllers.

Format show openflow configured controller

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
IP Address	IPv4 address of the controller.
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

9.3.3. 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 <10,60> | vlan <1-4093> | vlan_prio <0-7>]

Fields	Definition
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.

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
Flow type	The type of flow. (For example, 1DOT3)
Macth criteria	The match criteria specified by the flow.
Flow table	The hardward table in which the flow is installed.
Flow priority	The priority of the flow versus other flows.
Ingress port	The port on which the flow is active.
Actions	The action specified by the flow.
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.
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.

9.3.4. show openflow installed groups

This command displays the list of configured groups on the switch.

Format show openflow installed groups

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
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.

9.3.5. show openflow table-status

This command displays the supported OpenFlow tables and report usage information for the tables.

Format show openflow table-status openflow13

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
Flow Table	OpenFlow table identifier. The range is 0 to 255.
Flow Table Name	The name of 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.
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.
Insertaion Failure Count	Total number of hardware insertion attempts that were rejected due to lack of space since the switch powered up.
Flow Table Description	A detailed description for this table.

9.3.6. openflow enable

This command enables or disables the OpenFlow feature. If the OpenFlow feature is not in disabled state, then enabling has no effect on the OpenFlow feature.

To return the mode to the default, use the **no** form of this command. 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 openflow enable

no openflow enable

Default Disabled

Mode Global Config

9.3.7. 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.

To set the OpenFlow Static IP address to 0.0.0.0, use the **no** form of this command. Issuing this command when OpenFlow is enabled and using a static IP causes the OpenFlw feature to become operationally disabled.

Format openflow static-ip <ip-address>

no openflow static-ip

Default 0.0.0.0

Mode Global Config

9.3.8. 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 1.3 modes.

To delete the specified OpenFlow Controller IP address or delete all Controller addresses, use the **no** form of this command. If the IP Port number is omitted then all entries for the specified IP address are deleted.

Format openflow controller <ip-address> [ip-port][connection mode]

no openflow controller { ip-address [ip-port] | all}

Fields	Definition
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.

Mode Global Config

9.3.9. 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.

To direct the OpenFlow feature to automatically assign the IP address to itself, use the **no** form of this command.

Format openflow ip-mode {auto | static | serviceport}

no openflow ip-mode

Default Disabled

Mode Global Config

9.3.10. openflow passive-mode

This command enables OpenFlow passive-mode.

To disable OpenFlow passive-mode, use the **no** form of this command.

Format openflow passive-mode

no openflow passive-mode

Default Disabled

Mode Global Config

9.3.11. openflow failmode

This command configures the OpenFlow fail mode of connection interruption. It can choose the Fail-Secure or Fail-Standalone mode.

In the case that a switch loses contact with all controllers, the switch should immediately enter either “fail secure mode” or “fail standalone mode”. In “fail secure mode”, the only change to switch behavior is that packets and messages destined to the controllers are dropped. Flow entries should continue to expire according to their timeouts. In “fail standalone mode”, the switch processes all packets using the OFPP_NORMAL reserved port; in other words, the switch acts as a legacy Ethernet switch or router.

To reset to the default failmode, use the **no** form of this command.

Format openflow failmode {secure | standalone}

no openflow failmode

Default Secure

Mode Global Config

9.3.12. 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

10. Fluentd Commands

10.1. Show Commands

10.1.1. show fluentd

This command is used to display fluentd status and configuration settings.

Format show fluentd [<fluentd-entry>]

Fields	Definition
<fluentd-entry>	The fluentd entry name (up to 31 alphanumeric characters).

Default None

Mode Privileged EXEC

Display Message

Example #1:

```
(M4500-32C) #show fluentd

Fluentd mode: Disable

Current number of fluentd entries: 1

Current number of enabled fluentd entries: 1

Maximum number of fluentd entries: 20

------------------------------------------------------------

Fluentd Entry              : fluent

Fluentd Entry Status       : Enable

Source Status              : Enable

Source Tag                 : syslog.switch

Source Type                : syslog

Match Pattern              : syslog.**

Match Type                 : forward
```

Example #2:

```
(M4500-32C) #show fluentd fluent

Fluentd Entry                : fluent

Fluentd Entry Status         : Enable

Source Status                : Enable

Source Tag                   : syslog.switch

Source Type                  : syslog

Port                         : 5140

Bind                         : 0.0.0.0

Protocol Ty[e                : udp

Match Pattern                : flu.**

Match Type                   : forward

Host Type                    : ipv4

Host                         : 172.16.2.101

Port                         : 24224

Heartbeat Interval           : 1s

Heartbeat Type               : UDP

Phi Failure Detector         : Enable

Phi Threshold                : 16

Send Timeout                 : 60s

Buffer Type                  : Memory

Buffer Queue Limit           : 16

Buffer Chunk Limit           : 8m

Buffer Flush Interval        : 60s
```

10.2. Configuration Commands

10.2.1. fluentd

This command enables or disables FluentD service.

Format fluentd
no fluentd

Default Disabled

Mode Global Config

10.2.2. fluentd <fluentd-entry>

This command creates or deletes FluentD entry.

Format fluentd <fluentd-entry>
no fluentd <fluentd-entry>

Fields	Definition
<fluentd-entry>	The fluentd entry name (up to 31 alphanumeric characters).

Default None

Mode Global Config

10.2.3. enable

This command enables FluentD entry.

Format enable
no enable

Default Disabled

Mode Fluentd Configuration

10.2.4. sourcetag

This command configures the tag of the FluentD source.

Format sourcetag <tag> type {syslog | localsyslog | dstat | exec}
no sourcetag <tag>

Fields	Definition
<tag>	The sourcetag (up to 31 alphanumeric characters).

Default None

Mode Fluentd Configuration

10.2.5. syslog

This command configures syslog settings.

Format [enable | advance [port <1-65534> | bind <bind> | protocol-type {tcp | udp}]]
no enable

Fields	Definition
<1-65534>	The port to listen to.
<bind>	The bind address to listen to.

Default Port: 5140
Bind: 0.0.0.0 (all address)
Protocol-type: udp

Mode Syslog configuration

10.2.6. localsyslog

This command configures localsyslog settings.

Format [enable | severity <0-7>]
no enable

Fields	Definition
<0-7>	The logging severity level.

Default Severity: 5

Mode Localsyslog configuration

10.2.7. dstat

This command configures dstat settings.

Format [enable | advance [option <option> | delay <1-86400>]

no enable

Fields	Definition
<option>	The dstat option.
<1-86400>	The delay time (seconds).

Default Option: -fcdnm

Delay: 1

Mode Dstat configuration

10.2.8. exec

This command configures exec settings.

Format enable | command <command> | format {tsv <keys> | json | msgpack} | advance {tag-key <tag-key>| time-key <time-key> [<time-format>] | run-interval <run-interval>}

no enable

Fields	Definition
<command>	The command (program) to execute.
<keys>	The comma-separated (,) keys parameter (contains alphanumeric characters, dots (.), dashes (-), and underscores (_)).
<tag- key>	The key to use as the event tag instead of the value in the event record (up to 31 alphanumeric characters including ".“).
<time-key>	The key to use as the event time instead of the value in the event record.
<time-format>	The format of the event time used for the time_key parameter.
<run-interval>	The interval time between periodic program runs (the value in the range <1 - 60>, and suffix s (seconds), m (minutes), or h (hours)).

Default Time-key: current time

Time-format: %Y-%m-%d %H:%M:%S

Mode Exec configuration

10.2.9. matchpattern

This command configures fluentd match.

Format matchpattern <pattern> type {forward | webhdfs | elasticsearch}

no matchpattern <pattern>

Fields	Definition
<pattern>	The pattern (up to 31 alphanumeric characters).

Default None

Mode Fluentd configuration

10.2.10. forward

This command configures forward settings.

Format server {ipv4 <ipaddr> | hostname <hostname>} [<1-65535>] | advance{send-timeout <send-timeout> | heartbeat-type {tcp | udp} | heartbeat-interval <heartbeat-interval> | phi-failure-detector {disable | enable} | phi-threshold <1-60> | buffer {buffer-type {memory | file <buffer-path>} | buffer-queue-limit <1-16> | buffer-chunk-limit <chunk> | flush-interval <flush-interval>}}

Fields	Definition
<ipaddr>	The ipv4 address of server.
<hostname>	The host name of server.
<1-65535>	The host port number.
<send-timeout>	The timeout time when sending event logs (the value in the range <1 - 60>, and suffix s(seconds), m(minutes), or h(hours)).
<heartbeat-interval>	The interval of the heartbeat packer (the value in the range <1 - 60>, and suffix s(seconds), m(minutes), or h(hours)).
<1-60>	The interval time between periodic program runs (the value in the range <1 - 60>, and suffix s (seconds), m (minutes), or h (hours)).

<buffer-path>	The path where buffer chunks are stored.
<1-16>	The length limit of the chunk queue.
<chunk>	The size of each buffer chunk (the value in the range <1 - 8>, and suffix k(KB) or m(MB)).
<flush-interval>	The interval between data flushes (the value in the range <1 - 60>, and suffix s(seconds), m(minutes), or h(hours)).

Default Port: 24224
Send-timeout: 60s
Heartbeat-type: udp
Heartbeat-interval: 1s
Phi-threshold: 16
Buffer-type: memory
Buffer-queue-limit: 16
Buffer-chunk-limit: 8m
Flush-interval: 60s

Mode Forward configuration

10.2.11. webhdfs

This command configures webhdfs settings.

Format host-name <host name> | port <1-65535> | path <path> | advance {buffer [buffer-type {memory | file <buffer-path>}] | buffer-queue-limit <1-16> | buffer-chunk-limit <chunk> | flush-interval <flush-interval>}| localtime {disable | enable}

Fields	Definition
<host>	The namenode hostname.
<1-65535>	The namenode port number.
<path>	The path on HDFS.
<buffer-path>	The path where buffer chunks are stored.
<1-16>	The length limit of the chunk queue.
<chunk>	The size of each buffer chunk (the value in the range <1 - 8>, and suffix k(KB) or m(MB)).

<flush-interval>	The interval between data flushes (the value in the range <1 - 60>, and suffix s(seconds), m(minutes), or h(hours)).

Default Localtime: enable
Buffer-type: memory
Buffer-queue-limit: 16
Buffer-chunk-limit: 8m
Flush-interval: 60s

Mode Webhdfs configuration

10.2.12. elasticsearch

This command configures elasticsearch settings.

Format host {ipv4 <ipaddr> | hostname <hostname>} [<1-65535>] | hosts <host:port> | user <user> <password> <path> | advance {logstash-format {disable | enable <prefix>} | scheme <scheme> | utc-index {disable | enable} | index-name <index-name> | type-name <type-name> | request-timeout <request-timeout> | reload-connections {disable | enable} | reload-on-failure {disable | enable} | buffer {buffer-type {memory | file <buffer-path>} | buffer-queue-limit <1-16> | buffer-chunk-limit <chunk> | flush-interval <flush-interval>}}

Fields	Definition
<ipaddr>	The ipv4 address of server.
<hostname>	The host name of server.
<1-65535>	The host port number.
<host:port>	Multiple elasticsearch hosts with separator ",".
<user>	The elasticsearch cluster host user info.
<password>	The elasticsearch cluster host user password.
<path>	The elasticsearch cluster host path.
<prefix>	The logstash-prefix (up to 31 alphanumeric characters).
<index-name>	Store in a document the index it belongs to (up to 31 alphanumeric characters).
<type-name>	Each type has a list of fields that can be specified for documents of that type (up to 31 alphanumeric characters).
<tag-key>	The tag-key (up to 31 alphanumeric characters, include dashes(-), and underscores(_)).

<request-timeout>	HTTP request timeout (the value in the range <1 - 60>, and suffix s(seconds), m(minutes), or h(hours)).
<buffer-path>	The path where buffer chunks are stored.
<1-16>	The length limit of the chunk queue.
<chunk>	The size of each buffer chunk (the value in the range <1 - 8>, and suffix k(KB) or m(MB)).
<flush-interval>	The interval between data flushes (the value in the range <1 - 60>, and suffix s(seconds), m(minutes), or h(hours)).

Default Port: 9200
Logstash-format: disable
Prefix: logstash
Utc-index: enable
Index-name: fluentd
Type-name: fluentd
Tag-key: tag
Request-timeout: 5s
Reload-connections: enable
Reload-on-failure: disable
Buffer-type: memory
Buffer-queue-limit: 16
Buffer-chunk-limit: 8m
Flush-interval: 60s

Mode Elasticsearch configuration

11. SDVoE Commands

SDVoE (Software Defined Video-over-Ethernet) is the latest high-performance, software-based AV-over-IP platform for control and distribution of audio and video over Ethernet & Fiber networks.

In an SDVoE environment, L2 multicast is used by default. All these enhancements are applicable for L2 multicast only. If the user configures L3 multicast then L3 multicast should behave as per the standard. In addition, the enhancement is applicable only to IGMP version 1 and version 2. Version 3 works very differently and is not part of this enhancement.

11.1. Show Commands for an SDVoE Environment

11.1.1. show igmpsnooping group

This command is used to display the information of the IGMP groups. When no VLAN or interface is provided, the entire table is listed. When the **interface** or **port-channel** parameter is specified, only the hosts detected on that port or LAG are displayed.

Format show igmpsnooping group [<vlan-id> | interface <intf id> | port-channel <lag-id>]

Fields	Definition
<vlan-id>	1 to maximal VLAN ID
<intf id>	The physical port
<lad-id>	The ID of the port channel

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
VLAN ID	VLAN ID
Subscriber	The IP and MAC address of the IGMP host
MC Group	The multicast group this entry belongs to.
Interface	The interface number via which the host joins the multicast group
Type	IGMPv1 or IGMPv2
Timeout (sec)	The number of seconds after which the multicast entry is expired

Example:

```
(M4500-32C) #show igmpsnooping group

VLAN  Subscriber                    MC Group                          Interface Type   Timeout

===== ============================= ================================= ========= ====== ======

1     192.85.1.3/00:10:26:00:00:01  225.0.0.63/01:00:5e:00:00:3f      0/2       IGMPv2 244

1     192.85.1.3/00:10:26:00:00:01  225.0.0.64/01:00:5e:00:00:40      0/2       IGMPv2 244

2     192.85.1.4/00:10:27:00:00:01  225.0.0.1/01:00:5e:00:00:01       0/30      IGMPv2 238

2     192.85.1.4/00:10:27:00:00:01  225.0.0.2/01:00:5e:00:00:02       0/30      IGMPv2 229
```

11.1.2. show igmpsnooping fast-leave

This command is used to display the operational status of the Fast leave for each interface.

Format show igmpsnooping fast-leave

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
Interface	The specific interface
Fast-leave operation mode	The operational mode of the Fast-leave on the specific interface

Example:

```
(M4500-32C) #show igmpsnooping fast-leave

     Interface  Fast-Leave Operational Mode
     ---------  --------------------------
     0/1        Enable
     0/2        Enable
     0/3        Enable
     0/4        Disable
     0/5        Disable
     0/6        Disable
```

11.2. Configuration Commands for an SDVoE Environment

11.2.1. igmp-plus <vlan-id>

This command enables IGMP plus to support SDVoE on the specific VLAN. That is, this command enables IGMP enhancements for the specified VLAN to support audio and video devices in an SDVoE environment.

Format igmp-plus <vlan-id>

no igmp-plus <vlan-id>

Default igmp-plus 1

Mode Global Config

11.2.2. set igmp flood-report <vlan-id>

This command enables the flooding of the IGMP Join/Leave PDUs received on a downstream port (from a host) to all other ports for the specific VLAN.

Format set igmp flood-report <vlan-id>

no set igmp flood-report <vlan-id>

Default Enable

Mode VLAN Config

11.2.3. set igmp exclude-mrouter-intf <vlan-id>

This command enables the blocking of all known and unknown multicast streams to mrouter port for the specific VLAN. The multicast data stream are forwarded only if an IGMP membership (v1/v2) has been received through this mrouter port.

Format set igmp exclude-mrouter-intf <vlan-id>

no set igmp exclude-mrouter-intf <vlan-id>

Default Enable

Mode VLAN Config

11.2.4. set igmp fast-leave auto-assignment

Use this command to configure automatic assignment of fast-leave in system level (to all ports and LAGs). Use the no form to restore to default mode.

Format set igmp fast-leave auto-assignment

no set igmp fast-leave auto-assignment

Default Enable

Mode Global Config

12. Serviceability Packet Tracing Commands

12.1. CPU Traffic Commands

12.1.1. show cpu-traffic

Use this command to display the current configuration parameters.

Format show cpu-traffic

Mode Privileged EXEC

12.1.2. show cpu-traffic interface

Use this command to display per-interface statistics for configured filters. The statistics can be displayed for a specific filter such as stp, udld, arp, and so on. If no filter is specified, statistics are displayed for all configured filters. Similarly, source IP, destination IP, TCP, UDP, or MAC, along with a custom filter can be used as a command option to get statistics.

Format show cpu-traffic interface {all | <intf-range> | cpu} [<filter>]

Mode Privileged EXEC

12.1.3. show cpu-traffic summary

Use this command to display summary statistics for the configured filters for all interfaces.

Format show cpu-traffic summary

Mode Privileged EXEC

12.1.4. show cpu-traffic trace

Use this command to display traffic trace information. The trace information can be displayed either for all available packets or for a specific filter such as stp, udld, arp, and so on. Similarly, source IP, destination IP, or MAC, along with a custom filter can be used as a command option to get specific traces from the history. If enabled, packet dump information is displayed along with packet trace statistics. By default, the packet dump buffer size is set to store the first 64 bytes of a packet.

Format show cpu-traffic trace [<filter>]

Mode Privileged EXEC

12.1.5. 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 must consider the VLAN tag headers becuase the packet to the CPU is always a tagged packet.

Format cpu-traffic direction {tx | rx | both} interface {<intf-range> [cpu] | cpu [<intf-range>]}

no cpu-traffic direction {tx|rx|bot} interface

Default None

Mode Global Config

12.1.6. cpu-traffic direction match cust-filter

Use this command to configure a custom filter. The statistics, traces, or both for configured filters are obtained for the packet matching the configured data at the specific offset. If the mask is not specified, the default mask is 0xFF. You can specify three different offsets as match conditions. Each time a custom filter is configured, the switch overrides the previous configuration.

NOTE: The offset must consider the VLAN tag headers becuase the packet to the CPU is always a tagged packet.

Format cpu-traffic direction {tx | rx | both} match cust-filter <offset1> <data1> [mask1 <mask1>] <offset2> <data2> [mask2 <mask2>] <offset3> <data3> [mask3 <mask3>]

no cpu-traffic direction {tx|rx|both} match cust-filter

Default None

Mode Global Config

12.1.7. cpu-traffic direction match srcip

Use this command to configure the source IP address-specific filter. The statistics, traces, or both for configured filters are obtained for the packet matching the configured source IP/mask.

Format cpu-traffic direction {tx | rx | both} match srcip <ipaddress> [mask <mask>]

no cpu-traffic direction {tx | rx | both} match srcip

Default None

Mode Global Config

12.1.8. cpu-traffic direction match dstip

Use this command to configure the destination IP address-specific filter. The statistics, traces, or both for configured filters are obtained for the packet matching the configured destination IP/mask.

Format cpu-traffic direction {tx | rx | both} match dstip <ipaddress> [mask <mask>]

no cpu-traffic direction {tx | rx | both} match dstip

Default None

Mode Global Config

12.1.9. cpu-traffic direction match tcp

Use this command to configure the source or destination TCP port-specific filter. The statistics, traces, or both for configured filters are obtained for the packet matching the configured source or destination TCP port.

Format cpu-traffic direction {tx | rx | both} match {srctcp | dsttcp} <0-65535> [mask <0-65535>]

no cpu-traffic direction {tx | rx| both} match {srctcp | dsttcp}

Default None

Mode Global Config

12.1.10. cpu-traffic direction match udp

Use this command to configure the source or destination UDP port-specific filter. The statistics, traces, or both for configured filters are obtained for the packet matching the configured source or destination UDP port.

Format cpu-traffic direction {tx | rx | both} match {srcudp | dstudp} <0-65535> [mask <0-65535>]

no cpu-traffic direction {tx | rx | both} match {srcudp | dstudp}

Default None

Mode Global Config

12.1.11. cpu-traffic direction match mac

Use this command to configure the source or destination MAC filter. The statistics, traces, or both for configured filters are obtained for the packet matching the configured source or destination MAC address.

Format cpu-traffic direction {tx | rx | both} match {srcmac | dstmac} <0-65535> [mask <mask>]

no cpu-traffic direction {tx | rx | both} match {srcmac | dstmac}

Default None

Mode Global Config

12.1.12. cpu-traffic direction match filter

Use this command to configure the filter. The statistics, traces, or both for configured filters are obtained for the packet matching the configured filter item.

Format cpu-traffic direction {tx | rx | both} match filter {all | arp | bcast | bgp | custom | dhcp | dstip | dstmac | dsttcp | dstudp | ip | lacpdu | lldp | mcast | ospf | srcip | srcmac | srctcp | srcudp | stp | ucast | udld} [arp | bcast | bgp | custom | dhcp | dstip | dstmac | dsttcp | dstudp | ip | lacpdu | lldp | mcast | ospf | srcip | srcmac | srctcp | srcudp | stp | ucast | udld]

no cpu-traffic direction {tx | rx | both} match filter {all | arp | bcast | bgp | custom | dhcp | dstip | dstmac | dsttcp | dstudp | ip | lacpdu | lldp | mcast | ospf | srcip | srcmac | srctcp | srcudp | stp | ucast | udld} [arp | bcast | bgp | custom | dhcp | dstip | dstmac | dsttcp | dstudp | ip | lacpdu | lldp | mcast | ospf | srcip | srcmac | srctcp | srcudp | stp | ucast | udld]

Default None

Mode Global Config

12.1.13. cpu-traffic mode

Use this command to configure the CPU traffic mode. The packets in the RX/TX direction are matched when the mode is enabled.

Format cpu-traffic mode

no cpu-traffic mode

Default Disabled

Mode Global Config

12.1.14. 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 the dump-pkt keyword is enabled, the first 64 bytes of the packet are displayed along with the trace statistics.

Format cpu-traffic trace [dump-pkt]

no cpu-traffic trace

Default Disabled

Mode Global Config

12.1.15. clear cpu-traffic

Use this command to clear CPU traffic statistics or trace information on all interfaces.

Format clear cpu-traffic {counters | traces}

Default None

Mode Global Config

12.2. Exception Kernel Dump Commands

12.2.1. 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

12.2.2. show exception kernel-dump list

Use this command to display the currently captured dumps.

Format show exception kernel-dump list

Mode Privileged Exec

12.2.3. show exception kernel-dump log

Use this command to display the dmesg log from a specified kernel crash core dump (kdump) slot.

Format show exception kernel-dump log <crashlog-number>

Mode Privileged Exec

12.2.4. exception kernel-dump

Use this command to enable the kernel crash core dump (kdump) functionality. If the command was not enabled since the last reboot, enabling this command requires a reboot

Format exception kernel-dump

no exception kernel-dump <0-2>

Default Disabled

Mode Global Config

12.2.5. exception kernel-dump path

Use this command to set the path where the kernel crash core dump (kdump) entries are stored.

Format exception kernel-dump path <directory>

no exception kernel-dump path

Default None

Mode Global Config

12.3. Memory Buffer Commands

12.3.1. show mbuf

Use this command to display the memory buffer (MBUF) utilization monitoring parameters.

Format show mbuf

Mode Privileged Exec

Display Message

Fields	Definition
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.

12.3.2. show mbuf total

Use this command to display the memory buffer (MBUF) information.

Format show mbuf total

Mode Privileged Exec

Display Message

Fields	Definition
Mbufs Total	Total number of message buffers in the system.
Mbufs Free	Number of message buffers currently available.
Mbufs Rx Used	Number of message buffers of class RX currently in use.
Mbufs Rx Norm Used	Number of message buffers of class RX Norm currently in use.
Mbufs Rx Mid2 Used	Number of message buffers of class RX Mid2 currently in use.
Mbufs Rx Mid1 Used	Number of message buffers of class RX Mid1 currently in use.
Mbufs Rx Mid0 Used	Number of message buffers of class RX Mid0 currently in use.

Mbufs Rx High Used	Number of message buffers of class RX High currently in use.
Mbufs Tx Used	Number of message buffers of class TX currently in use.
Total Rx Norm Alloc Attempts	Number of times the system tried to allocate a message buffer allocation of class RX Norm.
Total Rx Mid2 Alloc Attempts	Number of times the system tried to allocate a message buffer allocation of class RX Mid2.
Total Rx Mid1 Alloc Attempts	Number of times the system tried to allocate a message buffer allocation of class RX Mid1.
Total Rx Mid0 Alloc Attempts	Number of times the system tried to allocate a message buffer allocation of class RX Mid0.
Total Rx High Alloc Attempts	Number of times the system tried to allocate a message buffer allocation of class RX High.
Total Tx Alloc Attempts	Number of times the system tried to allocate a message buffer allocation of class TX.
Total Rx Norm Alloc Failures	Number of message buffer allocation failures for RX Norm class of message buffer.
Total Rx Mid2 Alloc Failures	Number of message buffer allocation failures for RX Mid2 class of message buffer.
Total Rx Mid1 Alloc Failures	Number of message buffer allocation failures for RX Mid1 class of message buffer.
Total Rx Mid0 Alloc Failures	Number of message buffer allocation failures for RX Mid0 class of message buffer.
Total Rx High Alloc Failures	Number of message buffer allocation failures for RX High class of message buffer
Total Rx Tx Used Failures	Number of message buffer used failures for RX and TX class of message buffer.
Total Tx Alloc Failures	Number of message buffer allocation failures for TX class of message buffer.

12.3.3. mbuf

Use this command to configure the memory buffer (MBUF) threshold limits and generate notifications when MBUF limits have been reached.

Format mbuf {falling-threshold | rising threshold | severity}

no mbuf {falling-threshold | rising threshold | severity}

Mode Global Config

Fields	Definition
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).

13. Troubleshooting

13.1. M4500 series Linux system and password recovery for SSH port 22

This is a process to regain access to the switch so that you can use SSH to connect to port 22 and perform a firmware upgrade. You do need physical access to the switch console port to complete the process. You also need a computer with a serial port or a USB-to-serial-port adaptor and the serial-to-RJ45 cable that comes with the M4500 series switch.

When you start the switch for the first time, the default Linux user name is **admin** and the default password is **EndGame**. (This password is different from the password that you use to log to the switch CLI after you have completed the recovery process.)

1. Use the console to access the switch, press **Ctrl+Z** to display the menu, and after *Enter your menu option*, enter your Linux password to enable the Linux system password reset.

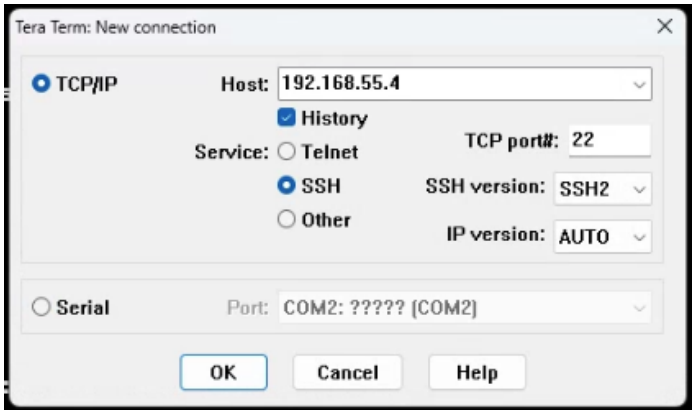
2. After new options display in the menu, enter **6** to reset the Linux system password, and type **Yes** to confirm the action.

```
=======================
NETGEAR M4500 Menu
=======================
1: CLI Console
2: Firmware update with verification using SCP
3: Firmware update with verification using TFTP
4: BIOS update
5: Reboot
6: Reset Linux system password
=======================
Enter your menu option: 6
Do you really want to reset password? (Yes) Yes
**** Linux system password is updated ****
**** Remember change password via SSH ****
```

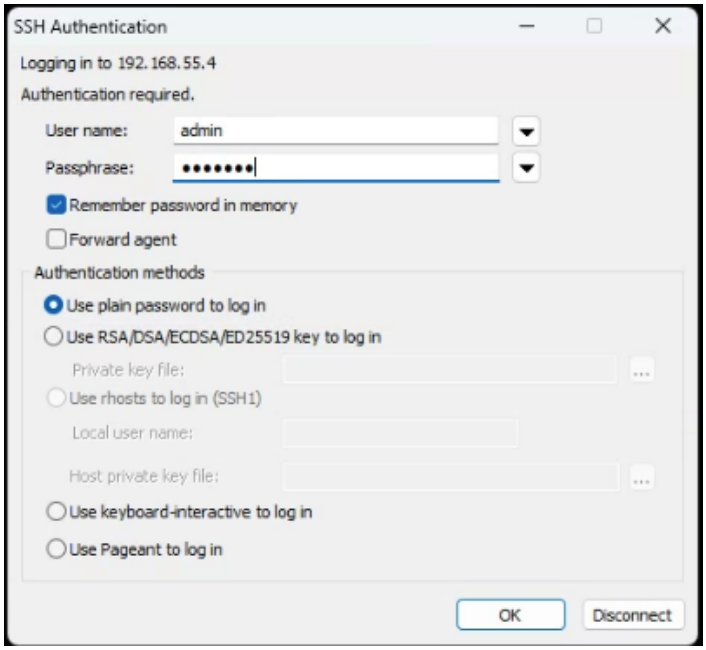
The following message displays on the console, and the password is reset to defaults:

**** Linux system password is updated ****
**** Remember change password via SSH ****

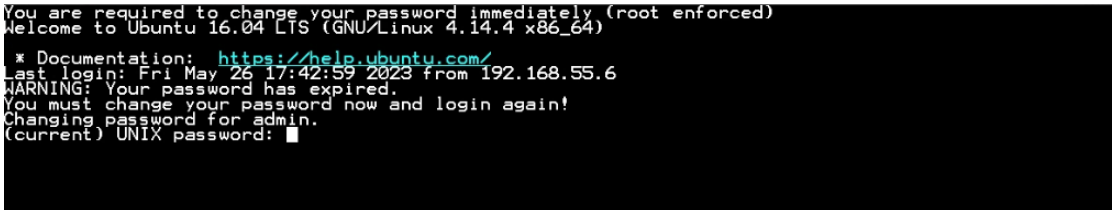
3. Open the Tera Term program and use SSH to connect to port 22.



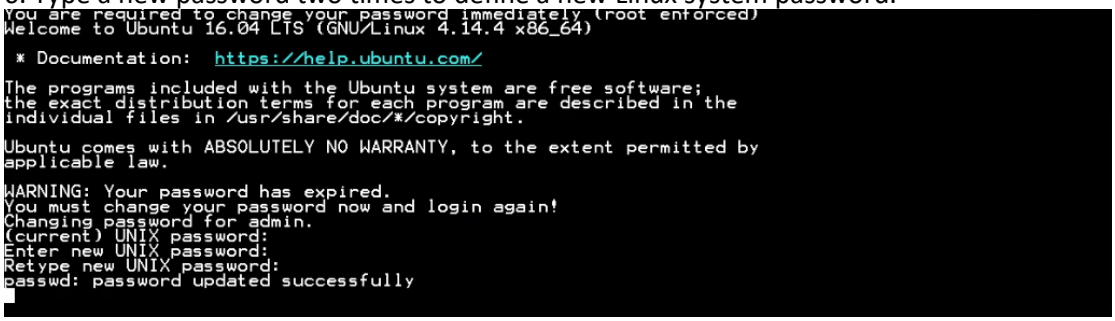
4. In the **User name** field, type **admin**, and in the **Passphrase** field, type **EndGame**.



5. After the SSH connection is successfully established, type **EndGame** as the current UNIX password.



6. Type a new password two times to define a new Linux system password.



7. With your new password, use SSH to log in to port 22. Then, press **Ctrl+Z** to display the menu, and select to update the firmware.