

OpenSwitch CLI User Guide

OpenSwitch CLI User Guide

Table of Contents

1. Overview	1
2. Console and Telnet Administration Interface	2
2.1. Local Console Management	3
2.2. Set Up your Switch Using Console Access	4
2.3. Set Up your Switch Using Telnet Access	5
2.4. Accessing the CLI	6
2.5. Command Conventions	7
2.6. Command Modes	8
2.7. Command Completion and Abbreviation	10
2.8. CLI Error Messages	11
2.9. CLI Line-Editing Conventions	12
2.10. Using CLI Help	13
3. Management And Utility Commands	15
3.1. General CLI commands	17
3.1.1. Setting the session timeout	17
3.1.2. Setting a command alias	17
3.1.3. Displaying the session-timeout value	18
3.1.4. Displaying the aliases	18
3.2. Audit framework	19
3.3. Management Interface Commands	20
3.3.1. interface mgmt	20
3.3.2. ip static	20
3.3.3. ip dhcp	20
3.3.4. default-gateway	21
3.3.5. nameserver	21
3.3.6. show interface mgmt	22
3.3.7. show running-config	23
3.3.8. show running-config interface mgmt	23
3.4. Hostname commands	25
3.4.1. hostname	25
3.4.2. show hostname	25
3.5. Domain name commands	26
3.5.1. domain-name	26
3.5.2. show domain-name	26
3.6. Configuration support for AAA	28
3.6.1. aaa authentication login	28
3.6.2. aaa authentication login fallback error local	28
3.6.3. radius-server host	28
3.6.4. radius-server retries	29
3.6.5. radius-server timeout	29
3.6.6. ssh	30
3.7. TACACS	31
3.7.1. Adding global timeout	31
3.7.2. Deleting global timeout	31
3.7.3. Adding global passkey	32
3.7.4. Deleting global passkey	32
3.7.5. Adding global authentication mechanism	32
3.7.6. Deleting global authentication mechanism	32
3.7.7. Adding a server	33

3.7.8. Deleting a server	33
3.7.9. Adding a server-group	34
3.7.10. Deleting a server-group	34
3.7.11. Configuring authentication sequence	34
3.7.12. Deleting authentication sequence	35
3.7.13. Enabling authentication fail-through	35
3.7.14. Disabling authentication fail-through	36
3.7.15. Configuring AAA Authorization with fallback	36
3.7.16. Deleting AAA Authorization with fallback	36
3.7.17. Viewing global config and TACACS+ servers	36
3.7.18. Viewing TACACS+ server groups	37
3.7.19. Viewing AAA Authentication sequence	38
3.7.20. Viewing AAA Authorization sequence	38
3.7.21. Viewing Privilege level information for current user	39
3.8. User Account and Password Commands	40
3.8.1. user add	40
3.8.2. password	40
3.8.3. user remove	40
3.8.4. show aaa authentication	41
3.8.5. show radius-server	41
3.8.6. show SSH authentication-method	41
3.8.7. show running-config	42
3.9. Configuration Support for SNMP Support	43
3.9.1. SNMP master agent configuration	43
3.9.1.1. JSON	43
3.9.2. SNMPv1, SNMPv2c community strings	43
3.9.2.1. JSON	43
3.9.3. Configuring SNMPv3 users	43
3.9.3.1. JSON	44
3.9.4. Configuring SNMP trap	44
3.9.4.1. JSON	45
3.9.5. Configuring SNMPv3 trap	45
3.9.5.1. JSON	46
3.9.6. Configuring SNMP system MIB objects	46
3.9.6.1. JSON	47
3.9.7. show snmp community	47
3.9.8. show snmp system	47
3.9.9. show snmp trap	48
3.9.10. show snmpv3 users	48
3.10. DHCP Relay CLI Commands	50
3.10.1. Configure dhcp-relay	50
3.10.2. Configure a helper-address	50
3.10.3. Configure dhcp-relay option 82	50
3.10.4. Unconfigure dhcp-relay option 82	51
3.10.5. Unconfigure response validation for the drop or replace policy of option 82	51
3.10.6. Configure DHCP relay bootp-gateway	51
3.10.7. Configure dhcp-relay hop-count-increment	52
3.10.8. Show dhcp-relay configuration	52
3.10.9. Show helper-address configuration	53
3.10.10. Show bootp-gateway configuration	53

3.10.11. Show running configuration	54
3.11. DHCP server	55
3.11.1. Changing to dhcp server context	55
3.11.2. Setting DHCP dynamic configuration	55
3.11.3. Removing DHCP dynamic configuration	56
3.11.4. Setting DHCP static configuration	56
3.11.5. Removing DHCP static configuration	57
3.11.6. Setting DHCP options configuration using an option name	58
3.11.7. Removing DHCP options configuration using an option name	58
3.11.8. Setting DHCP options configuration using an option number	58
3.11.9. Removing DHCP options configuration using an option number	59
3.11.10. Setting DHCP match configuration using an option name	59
3.11.11. Removing DHCP match configuration using an option name	60
3.11.12. Setting DHCP match configuration using an option number	60
3.11.13. Removing DHCP match configuration using an option number	61
3.11.14. Setting DHCP BOOTP configuration	61
3.11.15. Removing DHCP BOOTP configuration	61
3.11.16. Show DHCP server configuration	62
3.11.17. Showing DHCP server leases configurations	63
3.12. TFTP server	64
3.12.1. Changing to tftp server context	64
3.12.2. Enabling TFTP server	64
3.12.3. Disabling TFTP Server	64
3.12.4. Enabling TFTP server secure mode	64
3.12.5. Disabling TFTP server secure mode	65
3.12.6. Setting an TFTP root	65
3.12.7. Showing TFTP Server Configuration	65
3.13. SFTP Utility	67
3.13.1. SFTP Server Enable/Disable	67
3.13.2. Show command	67
3.13.3. SFTP client Interactive mode	67
3.13.4. SFTP client Non-Interactive mode	68
3.14. sFlow Commands	70
3.14.1. Enable sFlow globally	70
3.14.2. Disable sFlow globally	70
3.14.3. Set sFlow sampling rate	70
3.14.4. Remove sFlow sampling rate	70
3.14.5. Set sFlow polling interval	71
3.14.6. Remove sFlow polling interval	71
3.14.7. Set sFlow collector IP address	71
3.14.8. Remove sFlow collector ip address	72
3.14.9. Set sFlow agent interface name and family	72
3.14.10. Remove sFlow agent interface name and family	72
3.14.11. Set sFlow header size	73
3.14.12. Remove sFlow header size	73
3.14.13. Set sFlow max datagram size	73
3.14.14. Remove sFlow max datagram size	73
3.14.15. Enable sFlow on the interface	74
3.14.16. Disable sFlow on the interface	74
3.14.17. Show sFlow configuration	74
3.14.18. Show sFlow configuration interface	75

3.15. Remote Syslog Logging Configuration Commands	76
3.15.1. Logging configuration commands	76
3.16. Access Control List (ACL) Commands	77
3.16.1. Creation, modification, and deletion	77
3.16.2. Reset	79
3.16.3. Log timer	79
3.16.4. Interface Application, replacement, and removal	80
3.16.5. VLAN Application, replacement, and removal	81
3.16.6. Global context Display	82
3.16.7. Statistics (hit counts)	83
3.16.8. Log timer	84
3.17. Show Events Command	85
3.17.1. Display commands	85
3.18. Audit Log	87
3.18.1. Additional references	88
3.19. Ping Utility	89
3.19.1. IPv4 address	89
3.19.2. Hostname	89
3.19.3. Set data-fill pattern	89
3.19.4. Set datagram-size	90
3.19.5. Set interval	90
3.19.6. Set repetitions	91
3.19.7. Set timeout	91
3.19.8. Set TOS	92
3.19.9. Set ip-option	92
3.19.10. IPv6 address	94
3.19.11. IPv6 Hostname	95
3.19.12. IPv6 Set data-fill pattern	95
3.19.13. IPv6 Set datagram-size	96
3.19.14. IPv6 Set interval	96
3.19.15. IPv6 Set repetitions	96
3.20. Traceroute Utility	98
3.20.1. IPv4 address	98
3.20.2. Hostname	98
3.20.3. Set maximum TTL	98
3.20.4. Set minimum TTL	99
3.20.5. Set destination port	99
3.20.6. Set probes	100
3.20.7. Set timeout	100
3.20.8. Set ip-option loose source route	100
3.20.9. IPv6 address	101
3.20.10. IPv6 Hostname	101
3.20.11. IPv6 Set maximum TTL	102
3.20.12. IPv6 Set destination port	102
3.20.13. IPv6 Set probes	102
3.20.14. IPv6 Set timeout	103
3.21. Diagnostic Dump Commands	104
3.21.1. Show supported feature list	104
3.21.2. Show basic diagnostic	104
3.21.3. Capture basic diagnostic to file	105
3.22. Core Dump CLI Guide	106

3.22.1. Copy an instance of daemon coredump to tftp	106
3.22.2. Copy all instances of a corefile for a daemon	106
3.22.3. Copy kernel corefile to tftp server	107
3.22.4. Copy one instance of daemon corefile to sftp server	108
3.22.5. Copy all corefile instances for a daemon to a sftp server	109
3.22.6. Copy kernel corefile to sftp sruer	110
3.22.7. Copy coredump help string	111
3.22.8. show core dump	113
3.23. NTP Commands Reference	114
3.23.1. ntp server	114
3.23.2. ntp authentication	114
3.23.3. ntp authentication-key	114
3.23.4. ntp trusted-key	115
3.23.5. show ntp associations	115
3.23.6. show ntp status	116
3.23.7. show ntp authentication-keys	117
3.23.8. show ntp trusted-keys	117
3.23.9. show ntp statistics	117
3.24. Mirror Commands	119
3.24.1. mirror session	120
3.24.2. destination	120
3.24.3. shutdown	121
3.24.4. source	121
3.24.5. show mirror	122
3.25. CLI support for Autoprovisioning	124
3.25.1. autoprovisioning	124
3.25.2. show autoprovisioning	124
3.26. System commands	125
3.26.1. Setting the fan speed	125
3.26.2. Setting an LED state	125
3.26.3. Showing version information	125
3.26.4. Showing package information	126
3.26.5. Setting timezone on the switch	127
3.26.6. Showing system information	127
3.26.7. System fan information	129
3.26.8. Showing system temperature information	129
3.26.9. Showing system LED information	130
3.26.10. Showing system power-supply information	130
3.26.11. Showing system date information	131
3.26.12. Showing system CPU information using top	131
3.26.13. Showing system memory information using top	132
3.26.14. Showing time zone information	132
3.27. Secure Shell Commands	134
3.27.1. password-authentication	134
3.27.2. public-key-authentication	134
3.28. Control Plane Policing	135
3.28.1. show copp statistics	135
3.29. CLI support for Config Persistence	137
3.29.1. Copy startup configuration to running configuration	137
3.29.2. Copy running configuration to startup configuration	137
3.29.3. Show startup configuration	137

3.30. Logrotate Commands	138
3.30.1. logrotate period	138
3.30.2. logrotate maxsize	138
3.30.3. logrotate target	138
3.30.4. show logrotate	139
3.31. Show Tech Commands	140
3.31.1. show tech	140
3.31.2. show tech list	141
3.31.3. show tech feature	142
3.31.4. Show tech to file	142
3.32. Show Vlog Commands	144
3.32.1. Show vlog	144
3.32.2. Show vlog daemon	144
3.32.3. Show vlog severity	144
3.32.4. Show vlog config list	145
3.32.5. Show vlog config feature	145
3.32.6. Show vlog config daemon	145
3.32.7. Show vlog config	145
3.32.8. Show vlog daemon (daemon_name) severity (severity_level)	145
3.33. BroadView Commands	149
3.33.1. broadview client ip port	149
3.33.2. broadview agent-port	149
3.33.3. show broadview	149
3.34. Rebooting the switch.	150
3.34.1. reboot	150
3.34.2. reboot fast	150
3.34.3. reboot os	150
3.34.4. reboot primary	150
3.34.5. reboot secondary	150
3.34.6. reboot warm	150
4. Layer 2 features	151
4.1. Interface Commands	152
4.1.1. Change to interface context	152
4.1.2. Configure a range of interfaces	152
4.1.3. Enable an interface	152
4.1.4. Disable an interface	153
4.1.5. Enable routing on an interface	153
4.1.6. Disable routing on an interface	153
4.1.7. Set interface speed	153
4.1.8. Set interface speed to default	154
4.1.9. Set interface MTU	154
4.1.10. Set interface MTU to default	154
4.1.11. Set interface duplexity	155
4.1.12. Set interface duplexity to default	155
4.1.13. Enable flow control	155
4.1.14. Set flowcontrol to default	156
4.1.15. Set autonegotiation state	156
4.1.16. Set autonegotiation to default	156
4.1.17. Set an IPv4 address for an interface	157
4.1.18. Remove the IPv4 address for an interface	157
4.1.19. Set an IPv6 address for an interface	157

4.1.20.	Remove the IPv6 address for an interface	158
4.1.21.	Split a QSPF interface	158
4.1.22.	Show all interfaces	158
4.1.23.	Show the interface configuration	160
4.1.24.	Show transceiver information for all interfaces	160
4.1.25.	Show transceiver information for an interface	161
4.1.26.	Show the running configuration for all interfaces	162
4.1.27.	Show the running configuration for an interface	162
4.1.28.	Show transceiver DOM information for all interfaces	163
4.1.29.	Show transceiver DOM information for an interface	166
4.2.	MAC Address Table	169
4.2.1.	mac-address-table	169
4.2.2.	show mac-address-table	169
4.2.3.	show mac-address-table [dynamic]	170
4.2.4.	show mac-address-table address < mac-address >	171
4.3.	LACP commands	172
4.3.1.	Creation of LAG interface	172
4.3.2.	Deletion of LAG interface	172
4.3.3.	Configuring LACP system priority	172
4.3.4.	Configuring default LACP system priority	172
4.3.5.	Assigning interface to LAG	173
4.3.6.	Removing interface from LAG	173
4.3.7.	Configuring LACP port-id	173
4.3.8.	Configuring LACP port-priority	173
4.3.9.	Entering into LAG context	174
4.3.10.	Configuring LACP mode	174
4.3.11.	Configuring hash type	174
4.3.12.	Configuring LACP fallback	175
4.3.13.	Configuring LACP fallback mode	175
4.3.14.	Configuring LACP fallback timeout	175
4.3.15.	Configuring LACP rate	175
4.3.16.	Configuring no shutdown	176
4.3.17.	Configuring shutdown	176
4.3.18.	Display global LACP configuration	176
4.3.19.	Display LACP aggregates	176
4.3.20.	Display LACP interface configuration	177
4.3.21.	LAG show running-config	178
4.3.22.	LAG diag-dump basic	179
4.4.	VLAN commands	182
4.4.1.	Assigning an interface to access mode VLAN	182
4.4.2.	Removing an interface from access mode VLAN	182
4.4.3.	Assigning a trunk native VLAN to an interface	182
4.4.4.	Removing a trunk native VLAN from an interface	183
4.4.5.	Assigning tagging on a native VLAN to an interface	183
4.4.6.	Removing tagging on a native VLAN from an interface	183
4.4.7.	Assigning a VLAN to a trunk on the interface	184
4.4.8.	Removing a VLAN from a trunk on the interface	185
4.4.9.	Turning on a VLAN	185
4.4.10.	Turning off a VLAN	185
4.4.11.	Creating a VLAN	185
4.4.12.	Deleting a VLAN	186

4.4.13. Displaying a VLAN summary	186
4.4.14. Displaying a VLAN detail	186
4.5. MSTP commands	188
4.5.1. Enable MSTP protocol	188
4.5.2. Disable MSTP protocol	188
4.5.3. Set MSTP config name	188
4.5.4. Set default MSTP config name	188
4.5.5. Set MSTP config revision number	189
4.5.6. Set default MSTP config revision number	189
4.5.7. VLAN to an instance	189
4.5.8. Remove VLAN from instance	190
4.5.9. Set forward delay	190
4.5.10. Set default forward delay	190
4.5.11. Set hello time	190
4.5.12. Set default hello time	191
4.5.13. Set MSTP priority	191
4.5.14. Set default MSTP priority	191
4.5.15. Set transmit hold count	192
4.5.16. Set default transmit hold count	192
4.5.17. Set max age	192
4.5.18. Set default max age	192
4.5.19. Set max hops	193
4.5.20. Set default max hops	193
4.5.21. Set instance priority	193
4.5.22. Set default instance priority	194
4.5.23. Set port type	194
4.5.24. Set default port type	194
4.5.25. Enable bpdu guard	195
4.5.26. Set default bpdu guard	195
4.5.27. Enable root guard	195
4.5.28. Set default root guard	196
4.5.29. Enable loop guard	196
4.5.30. Set default loop guard	196
4.5.31. Enable bpdu filter	197
4.5.32. Set default bpdu filter	197
4.5.33. Set instance cost	197
4.5.34. Set instance default cost	198
4.5.35. Set instance port priority	198
4.5.36. Set instance default port priority	198
4.5.37. Show spanning tree global configuration	199
4.5.38. Show spanning tree detail configuration	199
4.5.39. Show MSTP global configuration	200
4.5.40. Show MSTP configuration	200
4.5.41. Show MSTP detail configuration	201
4.5.42. Show MSTP instance configuration	202
4.5.43. Show MSTP instance configuration	202
4.5.44. Show MSTP running configuration	203
4.6. LLDP Commands	205
4.6.1. Enable LLDP	205
4.6.2. Disable LLDP	205
4.6.3. Clear LLDP counters	205

4.6.4. Clear LLDP neighbor details	205
4.6.5. Set LLDP holdtime	206
4.6.6. Set LLDP holdtime to default	206
4.6.7. Set LLDP reinit delay	206
4.6.8. Set LLDP reinit delay to default	206
4.6.9. Set management IP address	207
4.6.10. Remove management IP address	207
4.6.11. Select TLVs	207
4.6.12. Remove TLVs	208
4.6.13. Set LLDP timer	209
4.6.14. Set LLDP timer to default	209
4.6.15. Enable LLDP transmission	210
4.6.16. Disable LLDP transmission	210
4.6.17. Enable LLDP reception	210
4.6.18. Disable LLDP reception	210
4.6.19. Show LLDP configuration	211
4.6.20. Show LLDP TLV	211
4.6.21. Show LLDP neighbor information	212
4.6.22. Show LLDP neighbor information for the interface	212
4.6.23. Show LLDP statistics	213
4.6.24. Show LLDP statistics for the interface	213
4.6.25. Show LLDP local device information	213
4.7. Error Disable / Recovery	216
4.7.1. errdisable detect	216
4.7.2. errdisable flap-setting	216
4.7.3. errdisable recovery cause	216
4.7.4. errdisable recovery interval	217
4.7.5. show errdisable detect	217
4.7.6. show errdisable flap-values	217
4.7.7. show errdisable recovery	218
4.8. Unidirectional Link Detection Commands	219
4.8.1. udld enable (Global Config)	219
4.8.2. no udld enable (Global Config)	219
4.8.3. udld message time	219
4.8.4. udld timeout interval	219
4.8.5. udld debug	219
4.8.6. udld enable (Interface Config)	220
4.8.7. no udld enable (Interface Config)	220
4.8.8. udld port	220
4.8.9. show udld	220
4.8.10. show udld interface	221
4.9. Storm-Control Commands	222
4.9.1. storm-control action	222
4.9.2. storm-control broadcast	222
4.9.2.1. no storm-control broadcast	223
4.9.3. storm-control multicast	223
4.9.3.1. no storm-control multicast	223
4.9.4. storm-control unicast	223
4.9.4.1. no storm-control unicast	223
4.9.5. show storm-control interface	224
4.10. FEC	225

4.10.1. fec	225
5. Layer 3 features	226
5.1. L3 Interfaces	227
5.1.1. routing	227
5.1.2. vrf attach	227
5.1.3. ip address	227
5.1.4. ipv6 address	228
5.1.5. ip proxy-arp	228
5.1.6. ip local-proxy-arp	228
5.1.7. interface vlan	229
5.1.8. interface	229
5.1.9. show interface	229
5.1.10. show interface vlan-name	231
5.1.11. show ip interface	231
5.1.12. show ipv6 interface	232
5.2. Loopback Interface Commands	233
5.2.1. Create loopback interface	233
5.2.2. Delete loopback interface	233
5.2.3. Set/Unset IPv4 address	233
5.2.4. Set or unset IPv6 addresses	233
5.2.5. Show running configuration	234
5.2.6. Show loopback interfaces	234
5.2.7. Show loopback interface	235
5.2.8. Supportability Commands	235
5.2.8.1. Display event logs	235
5.2.8.2. Daignostic Dump	236
5.2.8.3. show tech command	236
5.3. ARP commands	237
5.3.1. show ipv6 neighbors	237
5.3.2. arp aging	237
5.3.3. arp response	237
5.3.4. arp retry count	238
5.4. L3 Subinterfaces Commands	239
5.4.1. Create subinterface	239
5.4.2. Delete subinterface	239
5.4.3. Set or unset IPv4 addresses	239
5.4.4. Set or unset IPv6 addresses	240
5.4.5. Set or unset an IEEE 802.1Q VLAN encapsulation	240
5.4.6. Enable interface	240
5.4.7. Disable interface	241
5.4.8. Show running configuration	241
5.4.9. Show subinterfaces	241
5.4.10. Show subinterface	242
5.4.11. Supportability Commands	243
5.4.11.1. Display event logs	243
5.4.11.2. Daignostic Dump	244
5.5. UDP Broadcast Forwarder	245
5.5.1. Global enable/disable UDP broadcast forwarding	245
5.5.2. Configure UDP forward-protocol on an interface	245
5.5.3. Show UDP forward-protocol	245
5.6. Static routes	247

5.6.1. ip route	247
5.6.2. ipv6 route	247
5.6.3. show ip route	248
5.6.4. show ipv6 route	249
5.7. ECMP commands	250
5.7.1. ip ecmp load-balance dst-ip disable	250
5.7.2. ip ecmp load-balance src-ip disable	250
5.7.3. ip ecmp load-balance dst-port disable	250
5.7.4. ip ecmp load-balance src-port disable	250
5.7.5. ip ecmp load-balance resilient	251
5.7.6. show ip ecmp	251
5.8. eBGP Command Reference	252
5.8.1. router bgp	252
5.8.2. bgp router-id	252
5.9. IPv4 network	253
5.9.1. maximum-paths	253
5.9.2. timers bgp	253
5.9.3. IPv6 network	254
5.9.4. bgp fast-external-failover	254
5.9.5. bgp log-neighbor-changes	254
5.9.6. redistribute routes	254
5.9.7. neighbor remote-as	255
5.9.8. neighbor description	255
5.9.9. neighbor password	256
5.9.10. neighbor timers	256
5.9.11. neighbor allowas-in	256
5.9.12. neighbor remove-private-AS	257
5.9.13. neighbor soft-reconfiguration inbound	257
5.9.14. neighbor shutdown	257
5.9.15. neighbor peer-group	258
5.9.16. neighbor route-map	258
5.9.17. neighbor advertisement-interval	258
5.9.18. neighbor ebgp-multihop	259
5.9.19. neighbor filter-list	259
5.9.20. neighbor prefix-list	260
5.9.21. neighbor soft-reconfiguration	260
5.9.22. neighbor ttl-security	260
5.9.23. as-path access-list	261
5.9.24. route-map	261
5.9.25. match as-path	262
5.9.26. match community	262
5.9.27. match community exact-match	262
5.9.28. match extcommunity	263
5.9.29. match ip address prefix-list	263
5.9.30. match ipv6 address prefix-list	263
5.9.31. match ipv6 next-hop	264
5.9.32. match metric	264
5.9.33. match origin	264
5.9.34. match probability	265
5.9.35. Route-map set	265
5.9.36. set aggregator	265

5.9.37. set as-path exclude	266
5.9.38. set as-path prepend	266
5.9.39. set atomic-aggregate	266
5.9.40. set comm-list delete	267
5.9.41. set community	267
5.9.42. set community rt	267
5.9.43. set extcommunity soo	268
5.9.44. set ipv6 next-hop global	268
5.9.45. set local-preference	268
5.9.46. set metric	269
5.9.47. set origin	269
5.9.48. set weight	270
5.9.48.1. Route-map description	270
5.9.49. Route-map call	270
5.9.50. Route-map continue	271
5.9.51. IPv4 prefix-list	271
5.9.52. IPv6 prefix-list	271
5.9.53. Community lists configuration commands	272
5.9.54. Extended community lists configuration commands	273
5.9.55. show ip bgp	273
5.9.56. show ip bgp summary	274
5.9.57. show bgp neighbors	274
5.9.58. show ip bgp route-map WORD	275
5.9.59. show ip prefix list	275
5.9.60. show ip prefix-list WORD seq num	276
5.9.61. show ip prefix list detail WORD	276
5.9.62. show ip prefix list summary WORD	276
5.9.63. show ipv6 prefix list	277
5.9.64. show ipv6 prefix list WORD	277
5.9.65. show ipv6 prefix-list WORD seq num	277
5.9.66. show ipv6 prefix list detail	278
5.10. show ipv6 prefix list detail WORD	279
5.10.1. show ipv6 prefix list summary	279
5.10.2. show ipv6 prefix list summary WORD	279
5.10.3. show ipv6 prefix list WORD X:X::X:X/M	280
5.10.4. show ipv6 prefix list WORD X:X::X:X/M first-match	280
5.10.5. show ipv6 prefix list WORD X:X::X:X/M longer	280
5.10.6. show ip community list	281
5.10.7. show ip extcommunity list	281
5.10.8. show as-path access list	281
5.10.9. show as-path access list WORD	281
5.11. OSPFv2 commands	283
5.11.1. Create OSPF instance	283
5.11.2. Remove OSPF instance	283
5.11.3. Set router ID	283
5.11.4. Set router ID to default	284
5.11.5. Set OSPF network for the area	284
5.11.6. Unset OSPF network for the area	284
5.11.7. Enable OSPF area authentication	285
5.11.8. Disable OSPF area authentication	285
5.11.9. Set cost for default LSA summary	285

5.11.10. Set cost for default LSA summary to default	286
5.11.11. Set the area as NSSA	286
5.11.12. Unset the area as NSSA	287
5.11.13. Configure the area as stub	287
5.11.14. Unset the area as stub	288
5.11.15. Summarize intra-area paths	288
5.11.16. Unset summarization	289
5.11.17. Filter networks between OSPF areas	289
5.11.18. Disable filtering of networks between OSPF areas	290
5.11.19. Configure OSPF virtual links	290
5.11.20. Delete OSPF virtual links	291
5.11.21. Set OSPF virtual links authentication keys	291
5.11.22. Delete OSPF virtual links authentication keys	292
5.11.23. Set OSPF virtual link delays and intervals	293
5.11.24. Set OSPF virtual links delay or interval to default	293
5.11.25. Control distribution of default route information	294
5.11.26. Disable distribution of default route information	294
5.11.27. Set default metric for redistributed routes	295
5.11.28. Set default metric of redistributed routes to default	295
5.11.29. Define OSPF administrative distance	295
5.11.30. Set OSPF administrative distance to default	296
5.11.31. Set OSPF administrative distance for a particular route type	296
5.11.32. Set OSPF administrative distance for a particular route type to default	296
5.11.33. Stub router advertisement	297
5.11.34. Advertise normal cost metric	297
5.11.35. Log changes in the adjacency state	298
5.11.36. Disable logging changes in the adjacency state	298
5.11.37. Enable OSPF RFC1583 compatibility	298
5.11.38. Disable OSPF RFC1583 compatibility	299
5.11.39. Redistribute routes into OSPF	299
5.11.40. Disable redistributing routes into OSPF	299
5.11.41. OSPF BFD configuration	300
5.11.42. Set OSPF timers	300
5.11.43. Set OSPF timers to default	300
5.11.44. Set OSPF throttling parameters	301
5.11.45. Set OSPF throttling parameters to default	301
5.11.46. Configure NBMA neighbor	301
5.11.47. Remove NBMA neighbor	302
5.11.48. Set the interface as OSPF passive interface	302
5.11.49. Set the interface as OSPF active interface	303
5.11.50. Enable authentication on the interface	303
5.11.51. Disable authentication on the interface	304
5.11.52. Set time interval between hello packets for the interface	304
5.11.53. Set time interval between hello packets for the interface to default	304
5.11.54. Set neighbor dead interval for the interface	305
5.11.55. Set neighbor dead interval for the interface to default	305
5.11.56. Disable MTU mismatch detection	305
5.11.57. Enable MTU mismatch detection	306
5.11.58. Set the interface cost	306
5.11.59. Set the interface cost to default	306
5.11.60. Set OSPF network type for the interface	306

5.11.61. Set OSPF network type for the interface to default	307
5.11.62. Set the OSPF priority for the interface	307
5.11.63. Set the OSPF priority for the interface to default	307
5.11.64. Set the retransmit interval for the interface	308
5.11.65. Set the retransmit interval for the interface to default	308
5.11.66. Set the transmit delay for the interface	308
5.11.67. Set the transmit delay for the interface to default	309
5.11.68. Show general OSPF configurations	309
5.11.69. Show OSPF database information	310
5.11.70. Show OSPF interface information	315
5.11.71. Show OSPF neighbor information	316
5.11.72. Show OSPF routing table	317
5.11.73. Show OSPF active non default configurations	317
5.12. Source Interface Commands	319
5.12.1. Setting a source-interface IP address to the TFTP protocol	319
5.12.2. Setting a source-interface IP address for all the specified protocols	319
5.12.3. Setting a source-interface to TFTP protocol	319
5.12.4. Setting a source-interface for all the specified protocols	320
5.12.5. Unsetting a source-interface to TFTP protocol	320
5.12.6. Unsetting a source-interface for all the specified protocols	321
5.12.7. Showing source-interface selection configuration assigned to the TFTP protocol.	321
5.12.8. Showing source-interface selection configuration for all the specified proto- cols.	321
5.13. Virtual Router Redundancy Protocol Commands	323
5.13.1. ip vrrp	323
5.13.2. ip vrrp authentication	323
5.13.3. ip vrrp ip	323
5.13.4. ip vrrp mode	324
5.13.5. ip vrrp preempt	324
5.13.6. ip vrrp priority	325
5.13.7. ip vrrp timers advertise	325
6. Data Center Command	327
6.1. Priority-Based Flow Control Commands	328
6.1.1. priority-flow-control mode	328
6.1.1.1. no priority-flow-control mode	329
6.1.2. priority-flow-control priority	329
6.1.2.1. no priority-flow-control priority	329
6.2. OpenFlow CLI Commands	330
6.2.1. openflow	330
6.2.2. controller	330
6.2.3. hybridmode	331
6.2.4. openflow-port	331
6.2.5. show openflow	332
6.2.6. show openflow flows	332
6.2.7. show openflow groups	333
6.2.8. show openflow meters	333
6.3. VXLAN Commands	335
6.3.1. vxlan source-interface	335
6.3.1.1. no vxlan source	335
6.3.2. vxlan tenant-system	335

6.3.2.1. no vxlan tenant-system	336
6.3.3. vni Tunnel Configuration	336
6.3.4. vxlan-vni	336
6.3.4.1. no vxlan vlan	337
6.3.5. show vxlan	337
6.3.6. show vxlan tenant-system	337
6.3.7. show vxlan tenant-system configuration	338
6.3.8. show vxlan tunnel	338
7. Quality of Service Commands	339
7.1. Definition of terms	340
7.2. QoS global configuration commands	341
7.2.1. apply qos queue-profile	341
7.2.2. apply qos wred-profile	343
7.2.3. qos cos-map	343
7.2.4. qos dscp-map	343
7.2.5. qos queue-profile	344
7.2.6. qos schedule-profile	345
7.2.7. qos trust	346
7.2.8. qos wred-profile	346
7.2.8.1. qos wred-profile queue	347
7.3. QoS interface configuration commands	348
7.3.1. interface apply qos	348
7.3.2. interface qos dscp	350
7.3.3. interface qos trust	350
7.4. QOS queue profile configuration commands	352
7.4.1. name	352
7.4.2. map	353
7.5. QoS schedule profile configuration commands	354
7.5.1. strict	354
7.5.2. dwrr	355
7.6. Display commands	356
7.6.1. show interface	356
7.6.2. show interface queues	356
7.6.3. show qos cos-map	357
7.6.4. show qos dscp-map	357
7.6.5. show qos queue-profile	359
7.6.6. show qos schedule-profile	360
7.6.7. show qos trust	360
7.6.8. show running config	360
7.6.9. show running config interface	361
7.7. Common troubleshooting	362
7.8. Traffic shape	363

List of Figures

2.1. Console Setting Environment	4
--	---

List of Tables

2.1. CLI Command Modes	8
2.2. CLI Mode Access and Exit	8
2.3. CLI Error Messages	11
2.4. CLI Editing Conventions	12

Chapter 1. Overview

The next natural step in the evolution of DC network disaggregation is to move to an open source operating system, which gives users and developers control over their networks and freedom from the costs and limitations of packaged software.

OpenSwitch is a Linux-based, fully featured L2/L3 operating system that is built on modularity and high availability using modern development tools and environments. The architecture and modularity of OpenSwitch allows users and developers to build solutions using modern tools that reduce the time to service while resulting in more reliable solutions.

Built under the open source model, OpenSwitch offers the freedom of innovation while maintaining stability and limiting vulnerability.

OpenSwitch is a network operating system for disaggregated switches that are built around OCP compliant hardware and that utilizes the ONIE boot loader to install and uninstall network operating systems. It is aimed at accelerating the transition to open networking as well as the adoption of disaggregated data center networks. OpenSwitch provides a fully-featured control plane stack with support for layer 2 and layer 3 networking protocols. The NOS is built around a reliable architecture focusing on modularity and a central state repository.

OpenSwitch is an extensible NOS that utilizes modern development tools and offers extensive APIs and management interfaces.

Developers can build on the reliable and modern architecture to create unique networking features and applications using an agile development approach for faster development and more stable applications with fewer post-release defects.

Chapter 2. 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 later in this guide.

2.1. 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. 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.

2.2. Set Up 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.

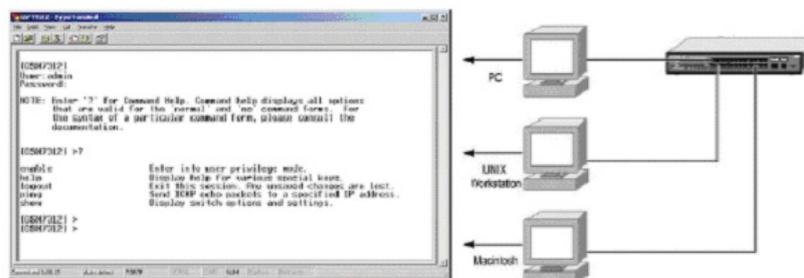
Make sure the terminal or PC you are using to make this connection is configured to match these settings. If you are having problems making this connection on a PC, make sure the emulation is set to VT-100 or ANSI. If you still don't see anything, try pressing <Ctrl> + r to refresh the screen.

The 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 - an RS-232 port with a 9-pin 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/adaptor 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/adaptor 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 2.1. Console Setting Environment



2.3. Set Up your Switch Using Telnet Access

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.

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. Most of the screens are identical, whether accessed through the console port or a Telnet interface.

2.4. Accessing the CLI

Once console or Telnet access is established, and the system completes the boot cycle, the User: prompt appears.

Default user credentials are "admin/admin."

After a successful login, the screen shows the Linux system prompt, switch:~\$

1. Elevate your privilege level using **sudo -i** command.
2. To view the service port network information use the **ip a** command. Eth0 interface serves as a service port.
3. To access the CLI use the "vtysh" command.

Example:

```
switch:~$ sudo -i
root@switch:~# vtysh
switch#
```

By default, the DHCP client on the service port is enabled. If your network has a DHCP server, then you need only to connect the switch service port to your management network to allow the switch to acquire basic network information.

2.5. Command Conventions

The parameters for a command might include mandatory values, optional values, or keyword choices.

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.

2.6. Command Modes

The CLI groups commands into modes according to the command function. Each of the command modes supports specific OpenSwitch software commands. The commands in one mode are not available until you switch to that particular mode.

The command prompt changes in each command mode to help you identify the current mode. The table below describes the command modes and the prompts visible in that mode.



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

Table 2.1. CLI Command Modes

Command Mode	Prompt	Mode Description
Global Config	Switch (Config)#	Groups general setup commands and permits you to make modifications to the running configuration.
VLAN Config	Switch (Vlan)#	Groups all the VLAN commands.
Interface Config	Switch (Interface number)# Switch (Interface vlan vlan-id)# Switch (Interface lag vlan-id)# Switch (Interface Loopback id)# Switch (Interface tunnel id)# Switch (Interface (startrange)-(endrange))#	Manages the operation of an interface and provides access to the router interface configuration commands. Use this mode to set up a physical port for a specific logical connection operation. You can also use this mode to manage the operation of a range of interfaces. For example for the range of interfaces from ports 2 to 4, the prompt displays as follows: switch(config)# interface range intf 2-4
Line SSH	Switch (config-ssh)#	Contains commands to configure SSH login/ enable authentication.
Router Config	Switch (Config-router)#	Contains the OSPF and BGP4 configuration commands.
Route Map Config	Switch (config-route-map)#	Contains the route map configuration

The next table explains how to enter each mode. To exit a mode and return to the previous mode, enter exit. To exit to Privileged EXEC mode, press Ctrl+z.

Table 2.2. CLI Mode Access and Exit

Command Mode	Access Method
Global Config	From the Privileged EXEC mode, enter the <i>configure</i> command.
VLAN Config	From the Privileged EXEC mode, enter <i>vlan number</i> command.

Console and Telnet Administration Interface

Command Mode	Access Method
Interface Config	From the Global Config mode, enter one of the following: interface number interface vlan vlan-id interface lag lag-number interface loopback id interface tunnel id interface range intf/lag/vlan
Router OSPF Config	From the Global Config mode, enter <i>router ospf</i>
BGP Router Config	From the Global Config mode, enter <i>router bgp <asnumber></i>
Route Map Config	From the Global Config mode, enter <i>route-map map-tag</i>

2.7. Command Completion and Abbreviation

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

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

2.8. CLI Error Messages

If you enter a command, and the system is unable to execute it, an error message appears. The table below describes the most common CLI error messages.

Table 2.3. CLI Error Messages

Message Text	Description
% Invalid input detected at '^'marker.	Indicates that you entered an incorrect or unavailable command. The carat (^) shows where the invalid text is detected. This message also appears if any of the parameters or values is not recognized.
Command not found / Incomplete command. Use ? to list commands.	Indicates that you did not enter the required keywords or values.
Ambiguous command	Indicates that you did not enter enough letters to identify uniquely the command.

2.9. CLI Line-Editing Conventions

The table below describes the key combinations you can use to edit commands or increase the speed of command entry. You can access this list from the CLI by entering help from the User or Privileged EXEC modes.

Table 2.4. CLI Editing Conventions

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

2.10. Using CLI Help

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

```
switch# ?
clear                Reset functions
configure            Configuration from vty interface
copy                Copy from one config to another
debug               Debug Configuration
diag-dump           Display diagnostic dump
disable             Turn off privileged mode command
end                 End current mode and change to enable mode
erase               Erase configuration
exit                Exit current mode and down to previous mode
list                Print command list
no                  Negate a command or set its defaults
page                Enable page break
password            Change user password
ping                Send ping requests to a device on the network
ping6               Send IPv6 ping requests to a device on the network
reboot              Reload the switch
show                Show running system information
start-shell         Start Bash shell
top                 Top command
traceroute          Trace the IPv4 route to a device on the network
traceroute6         Trace the IPv6 route to a device on the network
```

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

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

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

```
switch# configure ?
<cr>
terminal            Configuration terminal (default)
```

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

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

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

```
switch# show v ?
```

Console and Telnet Administration Interface

version	Displays switch version
vlan	Show VLAN configuration
vlog	Display all vlogs
vrf	VRF Configuration
vrrp	Shows all VRRP groups information
vxlan	VxLAN information.

Chapter 3. Management And Utility Commands

This section describes the following management commands available in the OpenSwitch CLI:

Section 3.1, "General CLI commands"

Section 3.2, "Audit framework"

Section 3.3, "Management Interface Commands"

Section 3.4, "Hostname commands"

Section 3.5, "Domain name commands"

Section 3.6, "Configuration support for AAA"

Section 3.7, "TACACS"

Section 3.8, "User Account and Password Commands"

Section 3.9, "Configuration Support for SNMP Support"

Section 3.10, "DHCP Relay CLI Commands"

Section 3.11, "DHCP server"

Section 3.12, "TFTP server"

Section 3.13, "SFTP Utility"

Section 3.14, "sFlow Commands"

Section 3.15, "Remote Syslog Logging Configuration Commands"

Section 3.16, "Access Control List (ACL) Commands"

Section 3.17, "Show Events Command"

Section 3.18, "Audit Log"

Section 3.19, "Ping Utility"

Section 3.20, "Traceroute Utility"

Section 3.21, "Diagnostic Dump Commands"

Section 3.22, "Core Dump CLI Guide"

Section 3.23, "NTP Commands Reference"

Section 3.24, "Mirror Commands"

Section 3.25, "CLI support for Autoprovision"

Section 3.26, "System commands"

Section 3.27, "Secure Shell Commands"

Section 3.28, "Control Plane Policing"

Section 3.29, "CLI support for Config Persistence"

Section 3.30, "Logrotate Commands"

Section 3.31, "Show Tech Commands"

Section 3.32, "Show Vlog Commands"

Section 3.34, "Rebooting the switch."

3.1. General CLI commands

3.1.1. Setting the session timeout

Use this command to set the amount of time a CLI session can be idle before it is automatically logged out.

The **no** form resets the session timeout to the default value of 30 minutes.

Syntax	[no] session-timeout <time>
Command Mode	Configuration mode (config).
Authority	All users.
<time>	0-4320, Idle timeout in minutes. A value of 0 means no timeout.

Examples

```
switch(config)# session-timeout 2
switch(config)#
```

After being idle for 2 minutes ...

```
Idle session timeout reached, logging out.
```

```
Halon 0.3.0 switch ttyS1
```

```
switch login:
switch(config)# no session-timeout
switch(config)# do show session-timeout
session-timeout: 30 minutes (Default)
switch(config)#
```

3.1.2. Setting a command alias

Use this command to define an alias for a CLI command.

Syntax	
Command Mode	Configuration mode (config).
Authority	All users.
<command>	Command for which to create an alias. These parameters are replaced by the corresponding arguments from the command line. Maximum length is 400 characters.



Alias commands available only in the configuration context.

Examples

```
switch(config)# alias hst hostname $1
switch(config)# hst myhost
myhost(config)#
myhost(config)# do show alias
Alias Name                Alias Definition
-----
hst                        hostname $1
myhost(config)#
```

```
myhost(config)# no alias hst
myhost(config)# do show hst
Alias Name                Alias Definition
-----
myhost(config)#
```

3.1.3. Displaying the session-timeout value

This command shows the idle timeout in minutes.

Syntax show session-timeout

Authority All users.

Examples

```
switch# show session-timeout
session-timeout: 2 minutes
switch#
```

3.1.4. Displaying the aliases

This command shows all aliases that are defined.

Syntax show alias

Authority All users.

Examples

```
switch# show alias
Alias Name                Alias Definition
-----
abc                        hostname $1
```

3.2. Audit framework

The audit framework is used to create audit events for tracking configuration changes made by users to switch. When users execute CLI configuration commands, the audit events are logged in the file: `/var/log/audit/audit.log`.

Example

```
switch(config)# session-timeout 100
```

Log format

```
type = USYS_CONFIG msg=audit(1456270989.650:31): pid=1507 uid=0
aid=4294967295 ses=4425671256 msg = 'op=CLI:command
data=73657373696F6E2D74696D656F757420313030 exec="/usr/bin/vtysh"
hostname=switch add=fe80::40af:cfff:feaf:d17c terminal=ttyS1 res=success'
```

The **data** field has an encoded version of the command that was executed. To decode the encoded data use the Linux **ausearch -i** command.

```
$ausearch -i -a 31
type = USYS_CONFIG msg=audit(03/22/16 08:29:57.452:10) : pid=604 uid=netop
aid=unset ses=unset msg='op=CLI:command data="session-timeout 100 "
exe=/usr/bin/vtysh hostname=switch addr=fe80::4a0f:cfff:feaf:81dc
terminal=ttyS1 res=success'
```

Where: "-a" or "--event" : Display events based on given event ID. "-i" or "--interpret" : Converts numeric values to text. Decodes uid/gid to the actual user/group name and displays encoded strings as their original ASCII values.

3.3. Management Interface Commands

This section describes the commands you use to configure a logical interface for management access.

3.3.1. interface mgmt

Switches to management interface configuration mode from configuration mode. All the management interface commands are available in this mode only.

Syntax	interface mgmt
Command Mode	Configuration mode (config).
Authority	Admin.

Example: Switching to management interface mode

```
switch(config)# interface mgmt
switch(config-if-mgmt)#
```

3.3.2. ip static

Assigns a static IP address to the management interface. You can assign both an IPv4 and IPv6 address at the same time.

Syntax	ip static <address>/<mask>
Command Mode	Management interface mode (config-if-mgmt).
Authority	Admin.
<address>	Required. Static IP address in either IPv4 format (A.B.C.D), or IPv6 format (X:X::X:X). Reserved, multicast, broadcast, and loopback addresses are not allowed.
<mask>	Required. Subnet mask associated with the static address in CIDR format.

Examples:

Setting an IPv4 address on the management interface

```
switch(config-if-mgmt)# ip static 192.168.1.10/16
```

Setting an IPv6 address on the management interface

```
switch(config-if-mgmt)# ip static 2001:db8:0:1::129/64
```

3.3.3. ip dhcp

Enables the DHCP client on the management interface. When enabled, the management interface attempts to retrieve its configuration settings from a DHCP server. If successful, these settings overwrite any statically configured values.

Syntax ip dhcp
Command Mode Management interface mode (config-if-mgmt).

Authority:Admin.

Example: Enabling DHCP on the management interface

```
switch(config-if-mgmt)# ip dhcp
```

3.3.4. default-gateway

Defines the default gateway when a static IP address is set on the management interface. An IPv4 default gateway can be configured only if an IPv4 address is configured on the management interface. An IPv6 default gateway can be configured only if an IPv6 address is configured on the management interface. It is possible to configure both an IPv4 and IPv6 address.

Use the **no** form of this command to remove a default gateway.

Syntax default-gateway <gateway-address>
Syntax no default-gateway <gateway-address>
Command Mode Management interface mode (config-if-mgmt).

Authority Admin.

<gateway_address> Gateway IP address in either IPv4 format (A.B.C.D), or IPv6 format (X:X::X:X). Reserved IP, Multicast IP, Broadcast IP, and loopback addresses are not allowed.

Examples:

Setting the default gateway using IPv4

```
switch(config-if-mgmt)# default-gateway 192.168.1.5
```

Setting the default gateway using IPv6

```
switch(config-if-mgmt)# default-gateway 2001:db8:0:1::128
```

Removing the default gateway using IPv4

```
switch(config-if-mgmt)# no default-gateway 192.168.1.5
```

Removing the default gateway using IPv6

```
switch(config-if-mgmt)# no default-gateway 2001:db8:0:1::128
```

3.3.5. nameserver

Configures the address of the primary and secondary DNS servers when the management interface is configured with a static IP address. It is possible to configure both IPv4 and IPv6 addresses. It is also possible to configure one DNS server with an IPv4 address and the other one with an IPv6 address. An IPv4 DNS server can be configured only if an IPv4 address is configured on the

management interface. An IPv6 DNS server can be configured only if an IPv6 address is configured on the management interface.

Use the **no** form of this command to remove a DNS server. You cannot remove the secondary DNS server without first removing the primary DNS server.

Syntax nameserver <address-1> [<address-2>]

Syntax no nameserver <address-1> [<address-2>]

Command Mode Management interface mode (config-if-mgmt).

Mode

Authority Admin.

<address-1> IP address of the primary DNS server in either IPv4 format (A.B.C.D), or IPv6 format (X:X::X:X). Reserved, multicast, broadcast, and loopback addresses are not allowed.

<address-2> IP address of the primary DNS server in either IPv4 format (A.B.C.D), or IPv6 format (X:X::X:X). Reserved, multicast, broadcast, and loopback addresses are not allowed.

Examples

Setting the primary DNS server using IPv4

```
switch(config-if-mgmt)# nameserver 192.168.1.1
```

Setting the primary and secondary DNS server using IPv4

```
switch(config-if-mgmt)# nameserver 192.168.1.2 192.168.1.3
```

Setting the primary DNS server using IPv6

```
switch(config-if-mgmt)# nameserver 2001:db8:0:1::100
```

Setting the primary and secondary DNS server using IPv6

```
switch(config-if-mgmt)# nameserver 2001:db8:0:2::100 2001:db8:0:3::150
```

Removing the primary and secondary DNS server using IPv4

```
switch(config-if-mgmt)# no nameserver 192.168.1.2 192.168.1.3
```

Removing the primary and secondary DNS server using IPv6

```
switch(config-if-mgmt)# no nameserver 2001:db8:0:2::100 2001:db8:0:3::150
```

3.3.6. show interface mgmt

Displays the current configuration of the management interface.

Syntax show interface mgmt

Command Mode Enable mode.

Mode

Authority All users.

Example

```
switch#show interface mgmt
Address Mode                : static
IPv4 address/subnet-mask    : 192.168.1.100/16
Default gateway IPv4       : 192.168.1.5
IPv6 address/prefix        : 2001:db8:0:1::129/64
IPv6 link local address/prefix : fe80::7272:cfff:fe485/64
Default gateway IPv6       : 2001:db8:0:1::128
Primary Nameserver         : 2001:db8:0:2::100
Secondary Nameserver        : 2001:db8:0:3::150
```

3.3.7. show running-config

Use this command to display the current configuration of the switch.

Syntax show running-config

Command Enable mode.

Mode

Authority Admin.

Example

```
switch# show running-config
Current configuration:
!
hostname "new-name"
!
interface mgmt
 ip static 192.168.1.100/16
 ip static 2001:db8:0:1::129/64
 default-gateway 192.168.1.5
 default-gateway 2001:db8:0:1::128
 nameserver 2001:db8:0:2::100 2001:db8:0:3::150
```

3.3.8. show running-config interface mgmt

Displays the current configuration of the switch from interface mode.

Syntax show running-config interface mgmt

Command Enable mode.

Mode

Authority Admin.

Example

```
switch# show running-config interface mgmt
Current configuration:
```

```
!  
interface mgmt  
  ip static 192.168.1.100/16  
  ip static 2001:db8:0:1::129/64  
  default-gateway 192.168.1.5  
  default-gateway 2001:db8:0:1::128  
  nameserver 2001:db8:0:2::100 2001:db8:0:3::150
```

3.4. Hostname commands

3.4.1. hostname

Configures the hostname assigned to the switch. The hostname is shown as part of each CLI prompt. The default hostname is switch.

Use the **no** form of this command to set the hostname to the default value.

Syntax hostname <name>

Syntax no hostname

Command Enable mode.

Mode

Authority Admin.

<name> Hostname starting with a letter and having a maximum length of 32 characters.

Example

Setting and then removing the host name "new-name"

```
switch(config)# hostname new-name
new-name(config)# no hostname
```

3.4.2. show hostname

Displays the currently configured hostname.

Syntax show hostname

Command Enable mode.

Mode

Authority All users.

Example

```
switch# show hostname
switch
```

3.5. Domain name commands

3.5.1. domain-name

Sets the domain name of the switch.

Use the **no** form of this command to remove the domain name.

Syntax domain-name <name>

Syntax no domain-name

Command Mode Configuration mode (config).

Authority Admin.

<name> Domain name starting with a letter and having a maximum length of 32 characters.

Examples

Setting the domain name to "example.com"

```
switch(config)# domain-name example.com
switch(config)# do show domain-name
example.com
```

Removing the domain

```
switch(config)# no domain-name
switch(config)# do show domain-name
```

```
switch(config)#
```



The **do** options runs a command in the enable mode.

3.5.2. show domain-name

Displays the domain name currently assigned to the switch.

Syntax show domain-name

Command Mode Enable mode.

Mode

Authority All users.

Example

Setting the domain to "example.com" and then displaying it

```
switch(config)# domain-name example.com
switch(config)# exit
```

```
switch# show domain-name  
example.com
```

3.6. Configuration support for AAA

3.6.1. aaa authentication login

Enables local authentication or RADIUS authentication. By default local authentication is enabled.

Syntax	aaa authentication login <local radius [auth-type <pap chap>]>
Authority	Admin
<local>	Enable local authentication.
<radius>	Enable RADIUS authentication.
<chap>	Use CHAP with RADIUS authentication.
<pap>	Use PAP with RADIUS authentication.

Examples

```
(config)# aaa authentication login local
(config)# aaa authentication login radius
(config)# aaa authentication login radius auth-type chap
```

3.6.2. aaa authentication login fallback error local

Enables fallback to local switch access authentication when the RADIUS server is configured but not reachable.

The **no** form disables falling back to local switch access authentication.

Syntax	[no] aaa authentication login fallback error local
Authority	Admin user.

Examples

```
(config)# aaa authentication login fallback error local
(config)# no aaa authentication login fallback error local
```

3.6.3. radius-server host

Configures a RADIUS server host on the switch with the authentication port or the key for a specific RADIUS server. The authentication takes place accordingly.

The priority of the RADIUS servers depends on the order in which they are configured.

The **no** form removes the specified host configuration of a switch.

Syntax	[no] radius-server host <A.B.C.D> [auth-port <0-65535> key <WORD>]
Authority	Admin user.
<A.B.C.D>	A valid IPv4 address (Broadcast, Multicast and Loopback addresses are not allowed).

- <0-65535> The authentication port, with a default of port 1812.
 <WORD> The key for a specific RADIUS server. The default is **testing123-1**

Examples

```
(config)# radius-server host 10.10.10.10
(config)# no radius-server host 10.10.10.10
(config)# radius-server host 20.20.20.20 key testRadius
(config)# no radius-server host 20.20.20.20 key testRadius
(config)# radius-server host 30.30.30.30 auth-port 2015
(config)# no radius-server host 30.30.30.30 auth-port 2015
```

3.6.4. radius-server retries

Configures the number of retries when connecting to the RADIUS server host from the switch. The authentication takes place accordingly.

The priority of the RADIUS servers depends on the order in which they are configured.

The **no** form removes the configuration for the number of retries.

- Syntax** [no] radius-server retries <0-5>
Authority Admin user.
 <0-5> The number of retries.

Examples

```
(config)# radius-server retries 5
(config)# no radius-server retries 5
```

3.6.5. radius-server timeout

Configures the timeout in seconds when connecting to the RADIUS server host from the switch. The authentication takes place accordingly.

The priority of the RADIUS servers depends on the order in which they are configured.

The **no** form removes the configuration for the timeout.

- Syntax** [no] radius-server timeout <1-60>
Authority Admin user.
 <1-60> The maximum amount of seconds the RADIUS client waits for a response from the RADIUS authentication server before it times out.

Examples:

```
(config)# radius-server timeout 10
(config)# no radius-server timeout 10
```

3.6.6. ssh

Enables the selected SSH authentication method. Public key authentication uses authorized keys saved in the user's .ssh folder, either by autoprovisioning script or manually. By default public key authentication and password authentication are enabled.

The **no** form disables the selected SSH authentication method.

Syntax [no] ssh <password-authentication | public-key-authentication>
Authority Admin user.
<password-authentication> Sets the SSH authentication method for password authentication.
<public-key-authentication> Sets the SSH authentication method for public key authentication.

Examples:

```
(config)# ssh password-authentication
(config)# no ssh password-authentication
(config)# ssh public-key-authentication
(config)# no ssh public-key-authentication
```

3.7. TACACS

TACACS+ is a protocol that handles authentication, authorization, and accounting (AAA) services. TACACS+ client functionality is supported on the switch.

Prerequisites

- A TACACS+ server (either local or remote) is needed for AAA services.
- OpenSwitch needs to have management interface UP and enabled.

Limitations

- A maximum of 64 TACACS+ servers can be configured.
- Server can be configured with a unicast IPV4/IPV6 address or FQDN.
- A maximum of 28 user-defined AAA servers-groups can be configured.
- Session-type (console/ssh/telnet) configuration provided together as *default* configuration for authentication.
- TACACS+ server reachability is over the management interface.

Defaults

- The default authentication tcp-port is 49.
- The default authentication timeout value is five.
- The default authentication key (shared-secret between client and server) is testing123-1.
- The default authentication-protocol is pap.

3.7.1. Adding global timeout

The timeout value specifies the number of seconds to wait for a response from the TACACS+ server before moving to next TACACS+ server. If not specified, a default value of five seconds is used. This can be over-ridden by a fine-grained per server timeout while configuring individual servers.

Syntax	tacacs-server timeout <1-60>
Authority	All users.
<1-60>	Timeout value

Examples

```
switch(config)# tacacs-server timeout 10
```

3.7.2. Deleting global timeout

Reset the global timeout to default authentication timeout value 5

Syntax no tacacs-server timeout

Authority All users.

Examples

```
switch(config)# no tacacs-server timeout
```

3.7.3. Adding global passkey

This key is used as shared-secret for encrypting the communication between all tacacs-server and OpenSwitch. This can be over-riden by a fine-grained per server passkey configuration.

Syntax tacacs-server key WORD

Authority All users.

<WORD> The key used while communicating with the server

Examples

```
switch(config)# tacacs-server key testing-key
```

The length of key should be less than 32 characters.

3.7.4. Deleting global passkey

Reset the global key to the default authentication key value of testing123-1.

Syntax no tacacs-server key

Authority All users.

Examples

```
switch(config)# no tacacs-server key
```

3.7.5. Adding global authentication mechanism

This is the authentication protocol which is used for communication with TACACS+ servers. This can be over-riden by a fine-grained per server auth-type configuration.

Syntax tacacs-server auth-type [pap/chap]

Authority All users.

<pap/chap> Authentication protocol name

Examples

```
switch(config)# tacacs-server auth-type [pap/chap]
```

3.7.6. Deleting global authentication mechanism

Reset the global authentication mechanism to the default authentication mechanism pap.

Syntax no tacacs-server auth-type

Authority All users.

Examples

```
switch(config)# no tacacs-server auth-type
```

3.7.7. Adding a server

Add a TACACS+ SERVER and the configured TACACS+ server is added to the default TACACS+ family group (named "tacacs_plus").

Syntax tacacs-server host <FQDN/IPv4/IPv6 address> [key passkey] [timeout <1-60>] [port <1-65535>] [auth-type pap/chap]

Authority All users.

<FQDN/IPv4/IPv6> The name or IPv4/IPv6 address of the server.

<passkey> The key used while communicating with the server, max 32 characters.

<1-60> Timeout value

<1-65535> TCP port number

<pap/chap> Authentication protocol name

Examples

```
switch(config)# tacacs-server host 1.1.1.1
switch(config)# tacacs-server host 1.1.1.2 port 12
switch(config)# tacacs-server host abc.com timeout 15 port 22
switch(config)# tacacs-server host 2001:0db8:85a3:0000:0000:8a2e:0370:7334
switch(config)# tacacs-server host 1.1.1.3 key test-123 timeout 15 port 22
auth-type chap
```

3.7.8. Deleting a server

Delete a previously added TACACS+ server.

Syntax tacacs-server host <FQDN/IPv4/IPv6> [port <1-65535>]

Authority All users.

<FQDN/IPv4/IPv6> The name or IPv4/IPv6 address of the server.

<1-65535> TCP port number

If a port number is not provided, the system will search the TACACS+ server by host name and default authentication port 49.

Examples

```
switch(config)# no tacacs-server host 1.1.1.1
switch(config)# no tacacs-server host abc.com port 22
```

3.7.9. Adding a server-group

Create an AAA server-group that contains 0 or more preconfigured TACACS+ servers. A maximum of 32 server-groups can be present in the system. Out of these four (4) are default server-groups (local, radius, tacacs_plus, none). Hence, 28 user-defined groups are allowed. The user-defined group cannot be named "local", "radius", "tacacs_plus" or "none". Predefined TACACS+ servers can then be added to this group. The server continues to be part of the default "tacacs_plus" family group. For authentication using a server-group, the servers are accessed in the same order in which they were added to the group.

Syntax aaa group server tacacs+ WORD
Authority All users.
<tacacs+> Create a TACACS+ server group.
<WORD> Server group name, max 32 characters.

Syntax server <FQDN/IPv4/IPv6> [port <1-65535>]
<FQDN/IPv4/IPv6> The name or IPv4/IPv6 address of the server.
IPv6>
<1-65535> TCP port number

If a port number is not provided, the system will search the TACACS+ server by host name and default authentication port 49.

Examples

```
switch(config)# aaa group server tacacs+ sg1
switch(config-sg)# server 1.1.1.2 port 12
switch(config)# aaa group server tacacs+ sg2
switch(config-sg)# server 2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

3.7.10. Deleting a server-group

Only a pre-configured user-defined TACACS+ server-group can be deleted. The servers belonging to the group being deleted are still a part of the default "tacacs_plus" family group.

Syntax no aaa group server tacacs+ WORD
Authority All users.
<tacacs+> Create a TACACS+ server group.
<WORD> Server group name, max 32 characters.

Examples

```
switch(config)# no aaa group server tacacs+ sg2
```

3.7.11. Configuring authentication sequence

Preconfigured server groups can be sequenced to be accessed for authentication. The server groups will be accessed in the order in which they are mentioned. Also the servers within the

groups will be accessed in the order in which they were added to the group. By default "local" authentication is triggered if no group is mentioned or if the mentioned list is exhausted. All servers will be accessed in a fail-through manner if aaa authentication allow-fail-through is configured. fail-through Upon failure in connection or failure in authentication, the next server will be reached out to.

Syntax aaa authentication login default <local | group group-list>
Authority All users.
<local> Enable local authentication.
<group-list> Space separated group or family names

Notes:

1. Valid family names are: local, tacacs+ and radius .
2. Each group should be given only once in a group-list.
3. The *local* literal can be given at most once, either before *group* literal or as part of group-list.
4. Either the *local* literal or user defined group-list must be given in command.

Examples

```
switch(config)# aaa authentication login default group sgl tacacs_plus local  
switch(config)# aaa authentication login default local
```

3.7.12. Deleting authentication sequence

Remove a configured sequence of server-groups for authentication.

Syntax no aaa authentication login default
Authority All users.

Examples

```
switch(config)# no aaa authentication login default
```

3.7.13. Enabling authentication fail-through

Enables Authentication fail-through. If failed to authenticate on a TACACS+ or RADIUS server, the system attempts to authenticate on the next TACACS+/RADIUS server according to the authentication priority sequence.

Syntax aaa authentication allow-fail-through
Authority All users.

Examples

```
switch(config)# aaa authentication allow-fail-through
```

3.7.14. Disabling authentication fail-through

Disables Authentication fail-through. If failed to authenticate on a TACACS+ or RADIUS server, the system will not attempt to authenticate on the next TACACS+/RADIUS server.

Syntax no aaa authentication allow-fail-through

Authority All users.

Examples

```
switch(config)# no aaa authentication allow-fail-through
```

3.7.15. Configuring AAA Authorization with fallback

By issuing the **aaa authorization commands default** command, the user can configure Authorization on the switch. Fallback preference is dictated by the sequence of groups and none are entered by the user. This command would mean that it would reach out to TACACS+ for each command entered for all users.

Syntax aaa authorization commands default {group <group-list> | none}

Authority All users.

Examples

```
switch(config)# aaa authorization commands default group tacacs+ none
switch(config)# aaa authorization commands default group TacGroup1
tacacs+ none
```

3.7.16. Deleting AAA Authorization with fallback

By issuing a **no aaa authorization commands default** command, the user can unconfigure AAA Authorization on the switch. If AAA Authorization is not configured, it uses RBAC authorization.

```
switch(config)# no aaa authorization commands default
```

3.7.17. Viewing global config and TACACS+ servers

The show **tacacs-server** and **show tacacs-server detail** commands display the configured TACACS+ servers. Both the commands show the global parameters as well as per server configurations. For TACACS+ server assigned to user defined groups, group priority (the sequence of TACACS+ server assignment to user defined group) is displayed, otherwise default priority (the sequence of TACACS+ server creation) is displayed instead.

Syntax show tacacs-server [detail]

Authority All users.

<detail> Display detailed TACACS+ servers information.

Examples

```
switch# show tacacs-server
```

```
***** Global TACACS+ Configuration *****
Shared-Secret: testing123-1
Timeout: 5
Auth-Type: pap
Number of Servers: 3
```

SERVER NAME	PORT
1.1.1.2	12
2001:0db8:85a3:0000:0000:8a2e:0370:7334	49
1.1.1.3	22

```
switch# show tacacs-server detail
```

```
***** Global TACACS+ Configuration *****
Shared-Secret: testing123-1
Timeout: 5
Auth-Type: pap
Number of Servers: 3
```

```
***** TACACS+ Server Information *****
```

```
Server-Name          : 1.1.1.2
Auth-Port            : 12
Shared-Secret (default) : testing123-1
Timeout (default)    : 5
Auth-Type (default)  : pap
Server-Group         : sgl
Group-Priority       : 1
```

```
Server-Name          : 2001:0db8:85a3:0000:0000:8a2e:0370:7334
Auth-Port            : 49
Shared-Secret (default) : testing123-1
Timeout (default)    : 5
Auth-Type (default)  : pap
Server-Group (default) : tacacs_plus
Default-Priority     : 4
```

```
Server-Name          : 1.1.1.3
Auth-Port            : 22
Shared-Secret       : test-123
Timeout             : 15
Auth-Type           : chap
Server-Group (default) : tacacs_plus
Default-Priority    : 5
```

3.7.18. Viewing TACACS+ server groups

Display a table of TACACS+ servers grouped by different TACACS+ server group assignment. For TACACS+ server assigned to user defined groups, group priority (the sequence of TACACS+ server assignment to user defined group) is displayed, otherwise default priority (the sequence of TACACS+ server creation) is displayed instead.

Syntax show aaa server-group

Authority All users.

Examples

```
switch# show aaa server-groups

***** AAA Mechanism TACACS+ *****
-----
GROUP NAME                | SERVER NAME                | PORT | PRIORITY
-----
sg1                        | 1.1.1.2                    | 12   | 1
-----
tacacs_plus (default)    | 2001:0db8:85a3:0000:0000:8a2e:0370:7334 | 49   | 4
tacacs_plus (default)    | 1.1.1.3                    | 22   | 5
-----
```

3.7.19. Viewing AAA Authentication sequence

Display a table of server groups based on the sequence of authentication access.



Group priority here represent the sequence of group, which is different from TACACS+ server group priority (which is sequence of server assigned to group)

Syntax show aaa authentication

Authority All users.

Example

```
switch(config)# aaa authentication login default group sg1 tacacs_plus local
switch(config)# exit
switch# show aaa authentication
AAA Authentication:
  Fail-through                : Disabled
  Fallback to local authentication : Enabled

Default Authentication for All Channels:
-----
GROUP NAME                | GROUP PRIORITY
-----
sg1                        | 1
tacacs_plus                | 2
local                      | 3
-----
```

3.7.20. Viewing AAA Authorization sequence

The show aaa authorization command displays detailed information on Authorization configuration on the switch.

Syntax show aaa authorization

Authority All users.

Example

```
switch(config)# aaa authorization commands default group sgl tacacs_plus
none
switch(config)# exit
switch# show aaa authorization
Command Authorization sequence for default channel:
-----
GROUP NAME                | GROUP PRIORITY
-----
sgl                        | 1
tacacs_plus                | 2
none                       | 3
```

3.7.21. Viewing Privilege level information for current user

The *show privilege-level* command displays the current user privilege level for the current session.

Syntax show privilege-level

Authority All users.

For example for user with ops_netop role, it would show as follows:

```
switch# show privilege-level
Privilege level is 14
```

3.8. User Account and Password Commands

3.8.1. user add

Adds users to the switch and configures their passwords.

Syntax user add <user_name>

Authority All users.

<user_name> The user name to be added to the switch.

Examples

```
siwtch# user add openswitch-user
Adding user openswitch-user
Enter new password:
Confirm new password:
user added successfully.
```

3.8.2. password

Configures an existing user password, except for the root user.

Syntax password <user_name>

Authority All users.

<user_name> The user name corresponding to the password to be changed.

Examples

```
switch2# password openswitch-user
Changing password for user openswitch-user
Enter new password:
Confirm new password:
password updated successfully
```

3.8.3. user remove

Deletes a user entry from the switch. The command cannot delete the root user or a user that is currently logged into the switch. Also, this command cannot delete the last existing user on the switch.

Syntax user remove <user_name>

Authority All users.

<user_name> The user name corresponding to the user entry to be removed from the switch.

Examples

```
switch# user remove openswitch-user
```

3.8.4. show aaa authentication

Displays the authentication used for the switch login.

Syntax show aaa authentication

Authority All users.

Examples

```
switch# show aaa authentication
AAA Authentication
  Local authentication           : Enabled
  Radius authentication         : Disabled
  Fallback to local authentication : Enabled
```

```
switch# show aaa authentication
AAA Authentication
  Local authentication           : Disabled
  Radius authentication         : Enabled
  Radius authentication type    : CHAP
  Fallback to local authentication : Enabled
```

3.8.5. show radius-server

Displays all configured RADIUS servers, with the following information for each server:

- IP addresses
- Shared secrets
- Ports used for authentication
- Retries and timeouts

Syntax show radius-server

Authority All users.

Examples

```
switch# show radius-server
***** Radius Server information *****
Radius-server:1
  Host IP address      : 1.2.3.4
  Shared secret        : testRadius
  Auth port            : 2015
  Retries              : 5
  Timeout              : 10
```

3.8.6. show SSH authentication-method

Displays the configured SSH authentication method.

Syntax show SSH authentication-method

Authority All users.

Examples

```
switch# show ssh authentication-method
SSH publickey authentication : Enabled
SSH password authentication  : Enabled
```

3.8.7. show running-config

Displays the current non-default configuration on the switch. No user information is displayed, as the user configuration is an exec command and is not saved in the OVSDB.

Syntax show running-config

Authority All users.

Examples

```
switch# show running-config
Current configuration:
!
aaa authentication login radius
no aaa authentication login fallback error local
no ssh password-authentication
no ssh public-key-authentication
radius-server host 1.2.3.4 key testRadius
radius-server host 1.2.3.4 auth_port 2015
radius-server retries 5
radius-server timeout 10
```

3.9. Configuration Support for SNMP Support

3.9.1. SNMP master agent configuration

The following command configures the port to which the SNMP master agent is bound.

The **no** version resets the SNMP master agent port to the default value of UDP port 161.

Default agent-port is 161.
Syntax [no] snmp-server agent-port <1-65535>
Authority Admin user.
<1-65535> The port on which the SNMP master agent listens for SNMP requests.

Examples

```
(config)# snmp-server agent-port 2000
(config)# no snmp-server agent-port 2000
```

3.9.1.1. JSON

CLI Command: snmp-server agent-port 5 REST Output: "other_config": { "snmp_agent_port": "5" },

3.9.2. SNMPv1, SNMPv2c community strings

This command is used to configure community strings for the SNMP agent. Maximum of 10 SNMP communities can be configured. Default community is restored only when count of configured SNMP communities is zero.

This command adds/removes community strings.

Defaults Default snmp community is *public*.
Syntax [no] snmp-server community <WORD>
Authority Admin user.
<no> Removes the specified community string.
<WORD> The name of the community string. Default is public.

Examples

```
(config)# snmp-server community private
(config)# no snmp-server community private
```

3.9.2.1. JSON

CLI Command: snmp-server community public REST Output: "snmp_communities": ["public"],

3.9.3. Configuring SNMPv3 users

This command is used to configure the credentials of SNMPv3 user. The SNMPv3 provides secure access to devices by a combination of authenticating and encrypting SNMP protocol packets over the network.

This command adds/removes SNMPv3 users.

Syntax [no] snmpv3 user <WORD> [auth <md5 | sha>] auth-pass <WORD> [priv <aes | des>] priv-pass <WORD>

Authority Admin user.

Parameters

<no>

Removes the specified SNMPv3 user.

<WORD>

The name of the SNMPv3 user.

<md5 or sha>

The SNMPv3 authentication protocol can be either MD5 or SHA.

<WORD>

The auth passphrase of the SNMPv3 user. It must be at least 8 characters in length.

<aes or des>

The SNMPv3 privacy protocol can be either aes or des.

<WORD>

The privacy passphrase of the SNMPv3 user. It must be at least 8 characters in length.

Examples

```
(config)# snmpv3 user Admin auth sha auth-pass mypassword priv des priv-pass myprivpass
```

```
(config)# no snmpv3 user Admin auth sha auth-pass mypassword priv des priv-pass myprivpass
```

3.9.3.1. JSON

CLI Command: snmpv3 user Admin auth sha auth-pass mypassword priv des priv-pass mypriv-pass REST Output: ["/rest/v1/system/snmpv3_users/Admin"]

3.9.4. Configuring SNMP trap

This command is used to configure the trap receivers to which the SNMP agent can send trap notifications.

This command is used to configure the SNMP Trap receivers with IP and port, notification type, version, community string.

Default community_name - public receiver_udp_port - 162

Syntax [no] snmp-server host <A.B.C.D | X:X::X:X > [trap] [version < v1 | v2c >] [community WORD] [port <UDP port>]

Syntax [no] snmp-server host <A.B.C.D | X:X::X:X > [trap | inform] [version < v2c >] [community WORD] [port <UDP port>]

Authority Admin user.

<no>	Removes the specified trap receiver configuration.
<A.B.C.D>	Valid IPv4 address of the trap receiver.
<X:X::X:X>	Valid IPv6 address of the trap receiver.
<trap or inform>	The SNMP notification type.
<v1 or v2c>	The SNMP protocol version.
<WORD>	The name of the community string to be used in the SNMP trap notifications. Default is public.
<UDP_port>	The port on which the trap receiver listens for SNMP trap notifications. Default is UDP port 162.

Examples

```
(config)# snmp-server host 10.10.10.10 trap version v1
(config)# no snmp-server host 10.10.10.10 trap version v1
(config)# snmp-server host 10.10.10.10 trap version v2c community public
(config)# no snmp-server host 10.10.10.10 trap version v2c community public
(config)# snmp-server host 10.10.10.10 trap version v2c community public
port 5000
(config)# no snmp-server host 10.10.10.10 trap version v2c community public
port 5000
(config)# snmp-server host 10.10.10.10 inform version v2c community public
(config)# no snmp-server host 10.10.10.10 inform version v2c community public
(config)# snmp-server host 10.10.10.10 inform version v2c community public
port 5000
(config)# no snmp-server host 10.10.10.10 inform version v2c community public
port 5000
```

3.9.4.1. JSON

CLI Command 1: snmp-server host 10.10.10.10 trap version v1 REST Output: ["/rest/v1/system/snmp_traps/10.10.10.10/162/%5Bu%27trap%27%5D/%5Bu%27v1%27%5D"]

CLI Command 2: snmp-server host 10.10.10.10 inform version v2c community public port 5000 REST Output: ["/rest/v1/system/snmp_traps/10.10.10.10/162/%5Bu%27trap%27%5D/%5Bu%27v2c%27%5D", "/rest/v1/system/snmp_traps/10.10.10.10/5000/%5Bu%27inform%27%5D/%5Bu%27v2c%27%5D"]

3.9.5. Configuring SNMPv3 trap

This command is used to configure the trap receivers to which the SNMP agent can send SNMPv3 trap notifications. To configure SNMPv3 trap, a SNMPv3 user should exist.

This command is used to configure the SNMPv3 trap receivers with IP and port, trap version, SNMPv3 user credentials.

Default	receiver_udp_port - 162
Syntax	[no] snmp-server host <A.B.C.D X:X::X:X > [trap inform] [version < v3 >] user <WORD> [port <UDP port>]
Authority	Admin user.
<no>	Removes the specified trap receiver configuration.
<A.B.C.D>	Valid IPv4 address of the trap receiver.
<X:X::X:X>	Valid IPv6 address of the trap receiver.
<trap or inform>	The SNMP notification type. Default is trap.
<v3>	The SNMP trap notification version. To send SNMPv3 trap/inform need to configured with option v3.
<WORD>	The SNMPv3 user name to be used in the SNMP trap notifications.
<UDP_port>	The port on which the trap receiver listens for SNMP trap notifications. Default is UDP port 162.

Examples

```
(config)# snmp-server host 10.10.10.10 trap version v3 auth user Admin
(config)# no snmp-server host 10.10.10.10 trap version v3 auth user Admin
(config)# snmp-server host 10.10.10.10 trap version v3 auth user Admin port 2000
(config)# no snmp-server host 10.10.10.10 trap version v3 auth user Admin port 2000
```

3.9.5.1. JSON

CLI Command: snmp-server host 10.10.10.10 trap version v3 user Admin port 2000 REST Output: ["/rest/v1/system/snmp_traps/10.10.10.10/162/%5Bu%27trap%27%5D/%5Bu%27v3%27%5D", "/rest/v1/system/snmp_traps/10.10.10.11/5000/%5Bu%27inform%27%5D/%5Bu%27v2c%27%5D", "/rest/v1/system/snmp_traps/10.10.10.10/162/%5Bu%27trap%27%5D/%5Bu%27v2c%27%5D", "/rest/v1/system/snmp_traps/10.10.10.10/5000/%5Bu%27inform%27%5D/%5Bu%27v2c%27%5D", "/rest/v1/system/snmp_traps/10.10.10.10/2000/%5Bu%27trap%27%5D/%5Bu%27v3%27%5D"]

3.9.6. Configuring SNMP system MIB objects

The following commands are used to configure the following SNMP system MIB objects -

- sysDescr
- sysLocation
- sysContact

This command is used to configure some SNMP system MIB objects.

Syntax [no] snmp-server system-description .LINE

Syntax [no] snmp-server system-contact .LINE
Syntax [no] snmp-server system-location LINE
Authority Admin user.
<no> Removes the specified trap receiver configuration.
<sys-tem-description .LINE> Configures sysDescr
<sys-tem-contact .LINE> Configures sysContact
<sys-tem-location .LINE> Configures sysLocation

Examples

```
switch(config)# snmp-server system-description this is openswitch system
switch(config)# snmp-server system-location Dock of the bay
switch(config)# snmp-server system-contact me@whatever.com
```

3.9.6.1. JSON

CLI Command 1: snmp-server system-description This is OpenSwitch System

CLI Command 2: snmp-server system-location Dock of the bay

CLI Command 3: snmp-server system-contact web@ui.com [mailto:web@ui.com]

REST Output: "other_config": { "system_contact": "web@ui.com", "system_location": "Dock of the bay", "system_description": "This is OpenSwitch System", },

3.9.7. show snmp community

This command displays details of all the configured community strings.

Syntax show snmp community
Authority Admin user.

Examples

```
switch# show snmp community
Community Names :
private
admin
```

3.9.8. show snmp system

This command displays details of all the configured system MIB objects.

Syntax show snmp system

Authority Admin user.

Examples

```
switch# show snmp system
SNMP system information
-----
System description : this is openswitch system
System location : Dock of the bay
System contact : me@whatever.com
```

3.9.9. show snmp trap

This command displays details of all the configured trap receivers:

- Host IP Address
- Port
- SNMP version
- Notification type
- Community Name (SNMPv1/2c)
- SNMPv3 User

Syntax show snmp trap

Authority Admin user.

Examples

```
switch# show snmp trap
Trap Receivers:
-----
Host          Port      Type      Version  SecName
-----
10.1.1.1      6000     trap      SNMPv1   private
10.1.1.1      162      inform    SNMPv2c  public
10.1.1.1      5000     inform    SNMPv3   -
```

3.9.10. show snmpv3 users

This command displays details of all the configured SNMPv3 users.

- User name
- Authentication protocol
- Privacy protocol

Syntax show snmpv3 users

Authority Admin user.

Examples

```
switch# show snmpv3 users
SNMPv3 Users :
```

User	AuthMode	PrivMode

Admin	MD5	AES
Guest	MD5	AES

3.10. DHCP Relay CLI Commands

3.10.1. Configure dhcp-relay

This command works in the configuration context, and is used to enable/disable the DHCP-relay feature on the device.

Syntax [no] dhcp-relay

Authority All users.

Examples

```
switch# configure terminal
switch(config)# dhcp-relay
switch(config)# no dhcp-relay
```

3.10.2. Configure a helper-address

This command is used to configure/unconfigure a remote DHCP server IP address on the device interface. Here the helper address is same as the DHCP server address. A maximum of 16 helper-addresses can be configured per interface. Even if routing is disabled on an interface, helper address configuration is allowed, but interface DHCP-relay functionality will be inactive. In case a client has received an IP address, and no routing is configured, the IP address is valid on the client until the lease time expires. DHCP-relay is supported only for IPv4. The helper address configuration is allowed only on data plane interfaces. The helper address should not be multicast or loop-back address.

Syntax [no] ip helper-address <IPv4-address>

Authority All users.

<IPv4-address> A DHCP server IP address.

Examples

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# ip helper-address 192.168.10.1
switch(config-if)# ip helper-address 192.168.20.1
switch(config-if)# no ip helper-address 192.168.10.1
switch(config-if)# no ip helper-address 192.168.20.1
switch(config)# interface 2
switch(config-if)# ip helper-address 192.168.30.1
```

3.10.3. Configure dhcp-relay option 82

This command is used to configure dhcp-relay option 82.

Syntax dhcp-relay option 82 < replace [validate] | drop [validate] | keep | validate [replace | drop] > [ip | mac]

Authority	All users.
<replace>	Replaces the existing option 82 field.
<keep>	Keeps the existing option 82 field.
<drop>	Drops the option 82 packets.
<mac>	Specifies the MAC address of the router.
<ip>	Specifies the IP address of the interface on which the client DHCP packet enters the switch.
<validate>	Validates the DHCP server responses.

Examples

```
switch# configure terminal
switch(config)# dhcp-relay option 82 replace validate mac
```

3.10.4. Unconfigure dhcp-relay option 82

This command is used to unconfigure dhcp-relay option 82.

Syntax	no dhcp-relay option 82
Authority	All users.

Examples

```
switch# configure terminal
switch(config)# no dhcp-relay option 82
```

3.10.5. Unconfigure response validation for the drop or replace policy of option 82

This command is used to unconfigure response validation only for the drop/replace policy.

Syntax	no dhcp-relay option 82 validate
Authority	All users.

Examples

```
switch# configure terminal
switch(config)# no dhcp-relay option 82
```

3.10.6. Configure DHCP relay bootp-gateway

This command is used to configure/unconfigure a gateway address for the DHCP relay agent to use for DHCP requests, rather than the DHCP relay agent automatically assigning the lowest-numbered IP address. This is supported only for IPv4. The BOOTP gateway configuration is allowed only on data plane interfaces.

Syntax	[no] ip bootp-gateway <IPv4-address>
---------------	--------------------------------------

Authority All users.
 <IPv4-ad- A gateway address.
 dress>

Examples

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# ip bootp-gateway 1.1.1.1
switch(config)# interface 2
switch(config-if)# ip bootp-gateway 1.1.1.2
switch(config)# interface 3
switch(config-if)# ip bootp-gateway 1.1.1.3
switch(config-if)# no ip bootp-gateway 1.1.1.3
```

3.10.7. Configure dhcp-relay hop-count-increment

This command works in the configuration context, and is used to enable/disable the DHCP relay hop count increment feature on the device.

Syntax [no] dhcp-relay hop-count-increment
Authority All users.

Examples

```
switch# configure terminal
switch(config)# dhcp-relay hop-count-increment
switch(config)# no dhcp-relay hop-count-increment
```

3.10.8. Show dhcp-relay configuration

This command is used to display the DHCP relay configuration.

Syntax show dhcp-relay
Authority All users.

Examples

```
switch# show dhcp-relay
DHCP Relay Agent           : Enabled
DHCP Request Hop Count Increment : Enabled
Option 82                  : Disabled
Response Validation        : Disabled
Option 82 Handle Policy    : replace
Remote ID                  : mac
DHCP Relay Statistics:
Client Requests           Server Responses
Valid      Dropped      Valid      Dropped
-----
60         10         60         10
```

```
DHCP Relay Option 82 Statistics:
Client Requests      Server Responses
Valid      Dropped  Valid      Dropped
-----
50          8        50          8
```

3.10.9. Show helper-address configuration

This command is used to display the DHCP relay helper-address configuration.

Syntax show ip helper-address [interface <interface-name>]

Authority All users.

<interface> The name of the interface.

Examples

```
switch# show ip helper-address
IP Helper Addresses
```

```
Interface: 1
IP Helper Address
-----
192.168.20.1
192.168.10.1
```

```
Interface: 2
IP Helper Address
-----
192.168.10.1
```

```
switch# show ip helper-address interface 1
IP Helper Addresses
```

```
Interface: 1
IP Helper Address
-----
192.168.20.1
192.168.10.1
```

3.10.10. Show bootp-gateway configuration

This command is used to display the DHCP relay BOOTP gateway configuration.

Syntax show dhcp-relay bootp-gateway [interface <interface-name>]

Authority All users.

<interface> The name of the interface.

Examples

```
switch# show dhcp-relay bootp-gateway
```

BOOTP Gateway Entries

Interface	BOOTP Gateway
1	1.1.1.1
2	1.1.1.2

```
switch# show ip helper-address interface 1  
BOOTP Gateway Entries
```

Interface	BOOTP Gateway
1	1.1.1.1

3.10.11. Show running configuration

This command displays the current non-default configuration on the switch.

Syntax show running-config

Authority All users.

Examples

```
switch# show running-config  
Current configuration:  
!  
!  
!  
no dhcp-relay  
no dhcp-relay hop-count-increment  
interface 1  
  helper-address 192.168.10.1  
  helper-address 192.168.20.1  
  ip bootp-gateway 1.1.1.1  
interface 2  
  helper-address 192.168.10.1  
  ip bootp-gateway 1.1.1.2
```

3.11. DHCP server

In vtysh, every command belongs to a particular context. All dhcp server configuration commands, except "dhcp-server", work in dhcp server context.

3.11.1. Changing to dhcp server context

This command changes vtysh context to dhcp server. This command works in config context.

Syntax dhcp-server

Authority All users.

Examples

```
switch# configure terminal
switch(config)# dhcp-server
switch(config-dhcp-server)#
```

3.11.2. Setting DHCP dynamic configuration

This command works in the dhcp-server context and sets DHCP dynamic configuration values for the DHCP server. The parameters netmask and broadcast should not be set for IPv6 and prefix-len should not be set for IPv4. The parameter end-ip-address must be set before setting netmask. The parameter netmask must be set before broadcast. The parameter static should be specified only for static IP address allocation within the range set. The parameters netmask, broadcast, match tags, set tags, prefix-len, lease-duration and static are optional. The default value of prefix-len is 64 and the default value of lease-duration is 60 minutes. The parameter match tags can have multiple tags and the parameter set tag should be single tag.

Syntax range <range-name> start-ip-address (<ipv4_address> | <ipv6_address>) end-ip-address (<ipv4_address> | <ipv6_address>) netmask <subnet_mask> broadcast <broadcast_address> match tags <match_tag_names> set tag <set_tag_name> prefix-len <prefix_length_value> lease-duration <lease_duration_value> static

Authority All users.

<range-name> Set DHCP dynamic configuration name.Length must be less than 15.

<ipv4_address>Set IPV4 address.

<ipv6_address>Set IPV6 address.

<subnet_mask>Set the network mask.

<broadcast_address>Set the broadcast address.

<match_tag_names>Set the match tags list. Each tag length must be less than 15.

<set_tag_name>Set the set tag name. Length must be less than 15.

<prefix-len> Set the IPV6 prefix length value.

<lease-duration> Set the lease duration value.
tion>

Example

```
switch# configure terminal
switch(config)# dhcp-server
switch(config-dhcp-server)# range dynamic start-ip-address 10.0.0.1
end-ip-address 10.255.255.254 netmask 255.0.0.0 broadcast 10.255.255.255
match tags tag1,tag2,tag3 set tag tag4
```

3.11.3. Removing DHCP dynamic configuration

This command works in the dhcp-server context and deletes DHCP dynamic configuration values.

Syntax no range <range-name> start-ip-address (<ipv4_address> | <ipv6_address>)
end-ip-address (<ipv4_address> | <ipv6_address>) netmask <subnet_mask>
broadcast <broadcast_address> match tags <match_tag_names> set
tag <set_tag_name> prefix-len <prefix_length_value> lease-duration
<lease_duration_value> static

Authority All users.

<range-name> Specify DHCP dynamic configuration name. Length must be less than 15.

<ipv4_address> Specify IPV4 address.

<ipv6_address> Specify IPV6 address.

<subnet_mask> Specify the network mask.

<broadcast_address> Specify the broadcast address.

<match_tag_names> Specify the match tags list. Each tag length must be less than 15.

<set_tag_name> Specify the set tag name. Length must be less than 15.

<prefix-len> Specify the IPV6 prefix length value.

<lease-duration> Specify the lease duration value in minutes

Example

```
switch# configure terminal
switch(config)# dhcp-server
switch(config-dhcp-server)# no range dynamic start-ip-address 10.0.0.1
end-ip-address 10.255.255.254 netmask 255.0.0.0 broadcast 10.255.255.255
match tags tag1,tag2,tag3 set tag tag4
```

3.11.4. Setting DHCP static configuration

This command works in the dhcp-server context and sets DHCP static configuration values for the DHCP server. Parameters match-mac-addresses, match-client-hostname, and match-client-id are optional but at least one of the three must be specified. Multiple MAC addresses can be specified for the parameter match-mac-addresses and multiple tags can be specified for the parameter set tags. Parameters set tags and lease-duration are optional and the default value of lease-duration is 60 minutes.

Syntax static (<ipv4_address> | <ipv6_address>) match-mac-addresses
<mac_addresses> match-client-hostname <hostname> match-client-id <client-id>
set tags <set_tag_names> lease-duration <lease_duration_value>

Authority All users.

<ipv4_address> Set IPV4 address.

<ipv6_address> Set IPV6 address.

<mac_addresses> Set the MAC address.

<hostname> Set the client hostname. Length must be less than 15.

<client-id> Set the client id. Length must be less than 15.

<set_tag_names> Set the set tags list. Each tag length must be less than 15.

<lease-duration> Set the lease duration value.

Example

```
switch# configure terminal
switch(config)# dhcp-server
switch(config-dhcp-server)#static 10.0.0.25 match-mac-addresses
36:d4:1b:12:ea:52 match-client-hostname 95_h2 set tags tag1,tag2,tag3
lease-duration 120
```

3.11.5. Removing DHCP static configuration

This command works in the dhcp-server context and removes DHCP static configuration values for the DHCP server.

Syntax no static (<ipv4_address> | <ipv6_address>) match-mac-addresses
<mac_addresses> match-client-hostname <hostname> match-client-id <client-id>
set tags <set_tag_names> lease-duration <lease_duration_value>

Authority All users.

<ipv4_address> Specify IPV4 address.

<ipv6_address> Specify IPV6 address.

<mac_addresses> Specify the MAC address.

<hostname> Specify the client hostname. Length must be less than 15.

<client-id> Specify the client id. Length must be less than 15.

<set_tag_names> Specify the set tags list. Each tag Length must be less than 15.

<lease-duration> Specify the lease duration value.

Example

```
switch# configure terminal
switch(config)# dhcp-server
switch(config-dhcp-server)#no static 10.0.0.25 match-mac-addresses
36:d4:1b:12:ea:52 match-client-hostname 95_h2 set tags tag1,tag2,tag3
lease-duration 120
```

3.11.6. Setting DHCP options configuration using an option name

This command works in the dhcp-server context and sets DHCP option configuration values for the DHCP server by specifying an option name. The parameter match-tags is optional and multiple tags can be specified for the parameter match-tags. The optional parameter IPv6 specifies whether the options are IPv6 options or not.

Syntax option set option-name <option_name> option-value <option_value> match tags <match_tag_names> ipv6

Authority All users.

<option_name> Set DHCP option name. Length must be less than 15.

<option_value> Set DHCP option value.

<match_tag_names> Specify the match tags list. Each tag length must be less than 15.

Example

```
switch# configure terminal
switch(config)# dhcp-server
switch(config-dhcp-server)# option set option-name Router option-value
10.0.0.1 match tags tag1,tag2,tag3
```

3.11.7. Removing DHCP options configuration using an option name

This command works in the dhcp-server context and removes DHCP option configuration values by specifying an option name.

Syntax no option set option-name <option_name> option-value <option_value> match tags <match_tag_names> ipv6

Authority All users.

<option_name> Set DHCP option name. Length must be less than 15.

<option_value> Set DHCP option value.

<match_tag_names> Specify the match tags list. Each tag length must be less than 15.

Example

```
switch# configure terminal
switch(config)# dhcp-server
switch(config-dhcp-server)# no option set option-name Router option-value
10.0.0.1 match tags tag1,tag2,tag3
```

3.11.8. Setting DHCP options configuration using an option number

This command works in the dhcp-server context and sets DHCP option configuration values for the DHCP server by specifying an option number. The parameter match-tags is optional and mul-

multiple tags can be specified for the parameter match-tags. The optional parameter IPv6 specifies whether the options are IPv6 options or not.

Syntax option set option-number <option_number> option-value <option_value> match tags <match_tag_names> ipv6

Authority All users.

<option_number> Set DHCP option number.

<option_value> Set DHCP option value.

<match_tag_names> Set the match tags list. Each tag length must be less than 15.

Example

```
switch# configure terminal
switch(config)# dhcp-server
switch(config-dhcp-server)# option set option-number 3 option-value
10.0.0.1 match tags tag1,tag2,tag3
```

3.11.9. Removing DHCP options configuration using an option number

This command works in the dhcp-server context and removes DHCP option configuration values by specifying an option number.

Syntax no option set option-number <option_number> option-value <option_value> match tags <match_tag_names> ipv6

Authority All users.

<option_number> Specify DHCP option name.

<option_value> Specify DHCP option value.

<match_tag_names> Specify the match tags list. Each tag length must be less than 15.

Example

```
switch# configure terminal
switch(config)# dhcp-server
switch(config-dhcp-server)# no option set option-number 3 option-value
10.0.0.1 match tags tag1,tag2,tag3
```

3.11.10. Setting DHCP match configuration using an option name

This command works in the dhcp-server context. The parameter option-value is optional, and if the option-value is not specified, this command sets the tag if the client sends a DHCP option of the given name. If the option-value is specified, then the tag would be set only if the option is sent and matches the value.

Syntax match set tag <set_tag_name> match-option-name <option_name> match-option-value <option_value>

Authority All users.

<set_tag_name> Set the set tag name. Length must be less than 15.

<option_name> Set DHCP option name. Length must be less than 15.

<option_value> Set DHCP option value.

Example

```
switch# configure terminal
switch(config)# dhcp-server
switch(config-dhcp-server)# match set tag tag1 match-option-name Router
match-option-value 10.0.0.1
```

3.11.11. Removing DHCP match configuration using an option name

This command works in the dhcp-server context and removes the dhcp match configuration.

Syntax no match set tag <set_tag_name> match-option-name <option_name> match-option-value <option_value>

Authority All users.

<set_tag_name> Set the set tag name. Length must be less than 15.

<option_name> Set DHCP option name. Length must be less than 15.

<option_value> Set DHCP option value.

Example

```
switch# configure terminal
switch(config)# dhcp-server
switch(config-dhcp-server)# no match set tag tag1 match-option-name Router
match-option-value 10.0.0.1
```

3.11.12. Setting DHCP match configuration using an option number

This command works in the dhcp-server context. The parameter option-value is optional and if an option-value is not specified, this command sets the tag if the client sends a DHCP option of the given number. If the option-value is specified, then the tag would be set only if the option is sent and matches the value.

Syntax match set tag <set_tag_name> match-option-number <option_number> match-option-value <option_value>

Authority All users.

<set_tag_name> Set the set tag name. Length must be less than 15.

<option_number> Set DHCP option number.

<option_value> Set DHCP option value.

Example

```
switch# configure terminal
switch(config)# dhcp-server
switch(config-dhcp-server)# match set tag tag1 match-option-number 3
match-option-value 10.0.0.1
```

3.11.13. Removing DHCP match configuration using an option number

This command works in the dhcp-server context and removes the dhcp match configuration.

Syntax no match set tag <set_tag_name> match-option-number <option_number> match-option-value <option_value>

Authority All users.

<set_tag_name> Set the set tag name.

<option_number> Set DHCP option number.

<option_value> Set DHCP option value.

Example

```
switch# configure terminal
switch(config)# dhcp-server
switch(config-dhcp-server)#no match set tag tag1 match-option-number 3
match-option-value 10.0.0.1
```

3.11.14. Setting DHCP BOOTP configuration

This command works in the dhcp-server context and sets the BOOTP options to be returned by the DHCP server.

Syntax boot set file <file_name> match tag <match_tag_name>

Authority All users.

<file_name> Set the file name.

<match_tag_name> Set match tag name. Length must be less than 15.

Example

```
switch# configure terminal
switch(config)# dhcp-server
switch(config-dhcp-server)# boot set file /tmp/tftp_file match tag tag1
```

3.11.15. Removing DHCP BOOTP configuration

This command works in the dhcp-server context and removes the BOOTP options.

Syntax no boot set file <file_name> match tag <match_tag_name>

Authority All users.

<file_name> Set the file name.

<match_tag_name> Set match tag name. Length must be less than 15.

Example

```
switch# configure terminal
switch(config)# dhcp-server
switch(config-dhcp-server)# no boot set file /tmp/tftp_file match tag tag1
```

3.11.16. Show DHCP server configuration

This command displays various DHCP server configurations. The configurations include the DHCP Dynamic configuration, the DHCP Static Configuration, the DHCP Options configuration, the DHCP Match configuration, and the DHCP BOOT configuration.

- Syntax** show dhcp-server
- Authority** All users.
- <path>** Set the tftp root path location.

Examples

```
switch# show dhcp-server

DHCP dynamic IP allocation configuration
-----
Name          Start IP Address      End IP Address      Netmask      Broadcast
-----
dynamic 10.0.0.1            10.255.255.254    255.0.0.0    10.255.255.255

DHCP static IP allocation configuration
-----
IP Address  Hostname  Lease time  MAC-Address      Set tags
-----
10.0.0.25  95_h2    65          36:d4:1b:12:ea:52  tag1,tag2,tag3

DHCP options configuration
-----
Option Number  Option Name      Option Value      ipv6  Match tags
-----
3              *                10.0.0.1          False tag1,tag2,tag3
*              Router           10.0.0.1          False tag1,tag2,tag3

DHCP Match configuration
-----
Option Number  Option Name      Option Value      Set tag
-----
3              *                10.0.0.1          tag1
*              Router           10.0.0.1          tag1

DHCP BOOTP configuration
-----
```

```

Tag           File
-----
tag1          /tmp/tftp_file
    
```

3.11.17. Showing DHCP server leases configurations

This command displays DHCP server leases configurations. The configurations contain the IP address, MAC address, lease expiry time, the client hostname, and the client id. The configurations are updated by the DHCP server after it assigns an IP address to the client.

Syntax show dhcp-server leases

Authority All users.

Examples

```

switch# show dhcp-server leases
Expiry Time           MAC Address           IP Address  Hostname and Client-id
-----
Wed Sep 23 23:07:12 2015  df:36:12:1b:54:ea  10.0.0.5    95_h1      *
Wed Sep 23 22:05:10 2015  36:d4:1b:12:ea:52  10.0.0.25   95_h2      *
    
```

3.12. TFTP server

All TFTP configurations work in the tftp-server context.

3.12.1. Changing to tftp server context

This command changes vtysh context to the tftp server and works in a config context.

Syntax tftp-server

Authority All users.

Examples

```
switch# configure terminal
switch(config)# tftp-server
switch(config-tftp-server)#
```

3.12.2. Enabling TFTP server

This command works in the tftp-server context and enables the TFTP Server.

Syntax enable

Authority All users.

Examples

```
switch# configure terminal
switch(config)# tftp-server
switch(config-tftp-server)# enable
```

3.12.3. Disabling TFTP Server

This command works in the tftp-server context and disables the TFTP Server.

Syntax disable

Authority All users.

Examples

```
switch# configure terminal
switch(config)# tftp-server
switch(config-tftp-server)# no enable
```

3.12.4. Enabling TFTP server secure mode

This command works in the tftp-server context and enables the TFTP server secure mode.

Syntax secure-mode

Authority All users.

Examples

```
switch# configure terminal
switch(config)# tftp-server
switch(config-tftp-server)# secure-mode
```

3.12.5. Disabling TFTP server secure mode

This command works in the tftp-server context and disables the TFTP server secure mode.

Syntax no secure-mode

Authority All users.

Examples

```
switch# configure terminal
switch(config)# tftp-server
switch(config-tftp-server)# no secure-mode
```

3.12.6. Setting an TFTP root

This command works in the tftp-server context and sets the tftp root path location.

Syntax path <path_name>

Authority All users.

<path> Set the tftp root path location.

Examples

```
switch# configure terminal
switch(config)# tftp-server
switch(config-tftp-server)# path /tmp/
```

3.12.7. Showing TFTP Server Configuration

This command displays TFTP server configurations.

Syntax show tftp-server

Authority All users.

Examples

```
switch# show tftp-server

TFTP server configuration
-----
TFTP server : Enabled
TFTP server secure mode : Enabled
```

```
TFTP server file path : /tmp/
```

3.13. SFTP Utility

3.13.1. SFTP Server Enable/Disable

This command enables/disables the SFTP server.

Syntax [no] sftp server enable

Authority Root user.

Examples

```
switch(config)#sftp server enable
```

```
switch(config)#no sftp server enable
```

3.13.2. Show command

This command shows the SFTP server status.

Syntax show sftp server

Authority Root user.

Examples

```
switch# show sftp server
```

```
SFTP server configuration
.....
SFTP server : Enabled
```

3.13.3. SFTP client Interactive mode

This command enters the SFTP interactive mode and can be accessed only by an admin user.

Syntax copy sftp username (<IPv4-address> | <hostname> | <IPv6-address>)

Authority Root user.

<username> specify the username of the remote device. Length must be less than 256 characters.

<IPv4-ad-
dress> IPv4 address of the remote device

<hostname> specify the hostname of the remote device. Length must be less than 256 characters.

<IPv6-ad-
dress> IPv6 address of the remote device

Examples

```
switch# copy sftp abc hostmachine
abc@hostmachine's password:
```

```
Connected to hostmachine.
sftp>
```

```
switch# copy sftp abc 10.1.1.1
The authenticity of host '10.1.1.1 (10.1.1.1)' can't be established.
ECDSA key fingerprint is SHA256:uWeyXm2j6VkDfCitlyz/P+xGgZW9YYw5GnDOsEgVHeU.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.1.1.1' (ECDSA) to the list of known hosts.
abc@10.1.1.1's password:
Connected to 10.1.1.1.
sftp>
sftp> get /users/abc/test_file
Fetching /users/abc/test_file to test_file
/users/abc/test_file          100% 212      0.2KB/s   00:00
sftp> put test_file /users/abc/
Uploading test_file to /users/abc/test_file
test_file                    100% 212      0.2KB/s   00:00
```

```
switch# copy sftp abc a::1
The authenticity of host 'a::1 (a::1)' can't be established.
ECDSA key fingerprint is SHA256:uWeyXm2j6VkDfCitlyz/P+xGgZW9YYw5GnDOsEgVHeU.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'a::1' (ECDSA) to the list of known hosts.
abc@a::1's password:
Connected to a::1.
sftp>
sftp> get /users/abc/test_file
Fetching /users/abc/test_file to test_file
/users/abc/test_file          100% 212      0.2KB/s   00:00
sftp> put test_file /users/abc/
Uploading test_file to /users/abc/test_file
test_file                    100% 212      0.2KB/s   00:00
```

3.13.4. SFTP client Non-Interactive mode

This command performs a non-interactive SFTP get and can be accessed only by an admin user.

Syntax	copy sftp username (<IPv4-address> <hostname> <IPv6-address>) Source [Destination]
Authority	Root user.
<username>	specify the username of the remote device. Length must be less than 256 characters.
<IPv4-address>	IPv4 address of the remote device
<hostname>	string specify the hostname of the remote device. Length must be less than 256 characters.
<IPv6-address>	IPv6 address of the remote device
<Source>	specify the source path of the file

<Destination> specify the detination path to store the file (Default path : */var/local/*)

Examples

```
switch# copy sftp abc hostmachine source-file
abc@hostmachine's password:
Connected to 10.1.1.1.
Fetching source-file to source-file
source-file          100%   25      0.0KB/s   00:00
switch#
```

```
switch# copy sftp abc 10.1.1.1 source-file
abc@10.1.1.1's password:
Connected to 10.1.1.1.
Fetching source-file to source-file
source-file          100%   25      0.0KB/s   00:00
switch#
```

```
switch# copy sftp abc a::1 source-file
abc@a::1's password:
Connected to a::1.
Fetching source-file to source-file
source-file          100%   25      0.0KB/s   00:00
switch#
```

```
switch# copy sftp abc hostmachine source-file destination-file
abc@hostmachine's password:
Connected to hostmachine.
Fetching source-file to destination-file
source-file          100%   25      0.0KB/s   00:00
switch#
```

```
switch# copy sftp abc 10.1.1.1 source-file destination-file
abc@10.1.1.1's password:
Connected to 10.1.1.1.
Fetching source-file to destination-file
source-file          100%   25      0.0KB/s   00:00
switch#
```

```
switch# copy sftp abc a::1 source-file destination-file
abc@a::1's password:
Connected to a::1.
Fetching source-file to destination-file
source-file          100%   25      0.0KB/s   00:00
switch#
```

3.14. sFlow Commands

3.14.1. Enable sFlow globally

This command enables sFlow globally. By default sFlow is disabled.

Syntax sflow enable

Authority All users.

Example

```
switch# configure terminal
switch(config)# sflow enable
```

3.14.2. Disable sFlow globally

This command disables sFlow globally. By default sFlow is disabled.

Syntax no sflow enable

Authority All users.

Example

```
switch# configure terminal
switch(config)# no sflow enable
```

3.14.3. Set sFlow sampling rate

This command sets the global sampling rate for sFlow. The default sampling rate is 4096, which means that one in every 4096 packets is sampled.

Syntax sflow sampling <rate>

Authority All users.

<rate> Sets the global sampling rate, 1-1000000000.

Example

```
switch# configure terminal
switch(config)# sflow sampling 1000
```

3.14.4. Remove sFlow sampling rate

This command sets the global sampling rate back to the default of 4096, which means that one in every 4096 packets is sampled.

Syntax no sflow sampling

Authority All users.

Example

```
switch# configure terminal
switch(config)# no sflow sampling
```

3.14.5. Set sFlow polling interval

This command sets the global polling interval, which by default is 30 seconds. Set the polling interval to 0 to disable polling.

Syntax sflow polling <interval>
Authority All users.
<interval> Sets the global polling interval, 0-3600.

Example

```
switch# configure terminal
switch(config)# sflow polling 10
```

3.14.6. Remove sFlow polling interval

This command resets the global polling interval to 30 seconds.

Syntax no sflow polling
Authority All users.

Example

```
switch# configure terminal
switch(config)# no sflow polling
```

3.14.7. Set sFlow collector IP address

This command sets a collector IP address (IPv4 or IPv6), with optional port and VRF (virtual routing and forwarding). The default port is 6343. VRF is the vrf on which the collector can be reached. By default, this is the data vrf. A maximum of three collectors can be configured.

Syntax sflow collector <IP> [port <port-number>] [vrf <vrf-name>]
Authority All users.
<IP> Collector IPv4 or IPv6 address.
<port-number> Port on which to reach a collector.
<vrf-name> Name of VRF on which to reach a collector.

Example

```
switch# configure terminal
switch(config)# sflow collector 10.0.0.1 port 6343 vrf vrf1
```

3.14.8. Remove sFlow collector ip address

This command removes a collector IP address (if present).

Syntax	no sflow collector <IP> [port <port-number>] [vrf <vrf-name>]
Authority	All users.
<IP>	Collector IPv4 or IPv6 address.
<port-number>	Port on which to reach a collector.
<vrf-name>	Name of VRF on which to reach a collector.

Example

```
switch# configure terminal
switch(config)# no sflow collector 10.0.0.1 port 6343 vrf vrf2
```

3.14.9. Set sFlow agent interface name and family

This command sets the name of the interface that is used for the agent IP in sFlow datagrams. If not specified, the system picks the IP address from one of the interfaces in a priority order (to be determined). It also optionally sets the family type (IPv4 or IPv6) for the agent interface, which is set to IPv4 by default.

Syntax	sflow agent-interface <interface-name> [ipv4 ipv6]
Authority	All users.
<interface-name>	System defined Name of the interface to use for agent IP address.
<ipv4>	IPv4 address family.
<ipv6>	IPv6 address family.

Example

```
switch# configure terminal
switch(config)# sflow agent-interface 1 ipv4
```

3.14.10. Remove sFlow agent interface name and family

This command removes an agent interface and family if set.

Syntax	no sflow agent-interface
Authority	All users.

Example

```
switch# configure terminal
switch(config)# no sflow agent-interface
```

3.14.11. Set sFlow header size

This command sets the sFlow header size in bytes. The default value is 128.

Syntax sflow header-size <size>
Authority All users.
<size> Sets size of the header in bytes, 64-256.

Example

```
switch# configure terminal
switch(config)# sflow header-size 64
```

3.14.12. Remove sFlow header size

This command resets the sFlow header size to the default value of 128 bytes.

Syntax no sflow header-size
Authority All users.

Example

```
switch# configure terminal
switch(config)# no sflow header-size
```

3.14.13. Set sFlow max datagram size

This command sets the maximum number of bytes that are sent in one sFlow datagram. The default value is 1400 bytes.

Syntax sflow max-datagram-size <size>
Authority All users.
<size> Sets the maximum size of an sFlow datagram, 200-9000.

Example

```
switch# configure terminal
switch(config)# sflow max-datagram-size 1000
```

3.14.14. Remove sFlow max datagram size

This command resets the number of bytes that are sent in one sFlow datagram to the default of 1400.

Syntax no sflow max-datagram-size
Authority All users.

Example

```
switch# configure terminal
switch(config)# no sflow max-datagram-size
```

3.14.15. Enable sFlow on the interface

This command enables sFlow on the interface. It is used in the interface context.

Syntax sflow enable

Authority All users.

Example

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# sflow enable
```

3.14.16. Disable sFlow on the interface

This command disables sFlow on the interface. It is used in the interface context.

Syntax no sflow enable

Authority All users.

Example

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# no sflow enable
```

3.14.17. Show sFlow configuration

This command displays global sFlow configuration settings and statistics.

Syntax show sflow

Authority All users.

Example

```
switch# show sflow
sFlow Configuration
-----
sFlow                               enabled
Collector IP/Port/Vrf               10.0.0.1/6343/vrf_default
                                      10.0.0.2/6343/vrf_default
Agent Interface                      1
Agent Address Family                 ipv4
Sampling Rate                        1024
Polling Interval                     30
Header Size                          128
Max Datagram Size                    1400
```

```
Number of Samples          0
```

3.14.18. Show sFlow configuration interface

This command displays sFlow configuration settings and statistics for an specific interface.

Syntax show sflow <interface>
Authority All users.
<interface> Name of the interface. System defined.

Example

```
switch# show sflow 1
sFlow configuration - Interface 1
-----
sFlow                enabled
Sampling Rate        1024
Number of Samples    0
```

3.15. Remote Syslog Logging Configuration Commands

3.15.1. Logging configuration commands

This command is used to add or remove remote syslog server configurations.

Syntax	[no] logging <IPv4-address> <IPv6-address> <hostname> [udp [<port>] tcp [<port>]] [severity <level>]
Authority	All users.
<IPv4-address>	IPv4 address of the remote syslog server
<IPv6-address>	IPv6 address of the remote syslog server
<hostname>	FQDN or hostname of the remote syslog server
<udp>	UDP transport protocol used to send syslog messages
<tcp>	TCP transport protocol used to send syslog messages
<port>	Port Number on which the remote syslog server runs. Default for UDP is 514 and for TCP is 1470
<severity>	Filter syslog messages using severity
<level>	Filter messages with severity higher than or equal to the specified value

Examples

```
switch(config)#logging 10.0.10.2
```

```
switch(config)#no logging
```

```
switch(config)#logging 10.0.10.6 severity info
```

```
switch(config)#no logging 10.0.10.6
```

```
switch(config)#logging 10.0.10.9 tcp 4242 severity err
```

3.16. Access Control List (ACL) Commands

3.16.1. Creation, modification, and deletion

Creates an access control list (ACL) comprised of one or more access control list entries (ACEs) that are ordered and prioritized by sequence numbers.

The **no** keyword is used to delete either an ACL or an individual ACE.

An applied ACL processes a packet sequentially against entries in the list until either the the packet matches an ACE or the last ACE in the list has been evaluated. If no ACEs are matched, the packet is denied (each ACL has an implicit default-deny ACE).



An ACL must be applied using the **apply** command (at interface context) before it has an effect on traffic. If an ACL with no user-created entries is applied, it denies all traffic on the applied interface (since only the implicit default-deny ACE is present).

Entering an existing *acl-name* value causes modification to the existing ACL, with any new *sequence-number* value creating an additional ACE, and any existing *sequence-number* value replacing an existing ACE with that same sequence number.

If no sequence number is specified, ACEs are appended to the end of the ACL with a sequence number equal to the highest ACE currently in the list plus 10.

```
[no] access-list ip <acl-name>
```

```
[no] [<sequence-number>]
    {permit|deny}
    {any|ah|gre|esp|icmp|igmp|pim|<ip-protocol-num>}
    {any|<src-ip-address>[/<prefix-length>|<subnet-mask>]}
    {any|<dst-ip-address>[/<prefix-length>|<subnet-mask>]}
    [count] [log]
```

```
[no] [<sequence-number>]
    {permit|deny}
    {sctp|tcp|udp}
    {any|<src-ip-address>[/<prefix-length>|<subnet-mask>]}
    [{eq|gt|lt|neq} <port>|range <min-port> <max-port>]
    {any|<dst-ip-address>[/<prefix-length>|<subnet-mask>]}
    [{eq|gt|lt|neq} <port>|range <min-port> <max-port>]
    [count] [log]
```

```
[no] [<sequence-number>]
    comment ...
```

Authority	Admin.
<ip>	Create or modify an IPv4 ACL.
<acl-name>	The name of the ACL.
<sequence-number>	(1-4294967295) A sequence number for the ACE.

<action>	Permit or deny traffic matching the ACE.
<comment>	Store the remaining entered text as an ACE comment.
<ip-protocol>	An IP protocol number or name.
<src-ip-address>	The source IP host, network address, or any.
<dst-ip-address>	The destination IP host, network address, or any.
<prefix-length>	The address bits to mask (CIDR subnet mask notation, 1-32).
<subnet-mask>	The address bits to mask (dotted decimal notation).
<eq>	Layer 4 port is equal to port.
<gt>	Layer 4 port is greater than port.
<lt>	Layer 4 port is less than port.
<neq>	Layer 4 port is not equal to port.
<port>	A single Layer 4 port.
<range>	Layer 4 port between min-port-max-port (inclusive).
<min-port>	The start of a Layer 4 port range.
<max-port>	The end of a Layer 4 port range.
<count>	Keep hit counts of the number of packets matching the ACE.
<log>	Keep a log of the number of packets matching the ACE.

Examples

Create an ACL with three entries:

```
switch(config)# access-list ip My_ACL
switch(config-acl)# 10 permit udp any 172.16.1.0/24
switch(config-acl)# 20 permit tcp 172.16.2.0/16 gt 1023 any
switch(config-acl)# 30 deny any any any count
switch(config-acl)# exit
```

Add a comment to an existing ACE:

```
switch(config)# access-list ip My_ACL
switch(config-acl)# 20 comment Permit all TCP ephemeral ports
switch(config-acl)# do show access-list
switch(config-acl)# exit
```

Add an ACE to an existing ACL:

```
switch(config)# access-list ip My_ACL
switch(config-acl)# 25 permit icmp 172.16.2.0/16 any
switch(config-acl)# exit
```

Replace an ACE in an existing ACL:

```
switch(config)# access-list ip My_ACL
```

```
switch(config-acl)# 25 permit icmp 172.17.1.0/16 any
switch(config-acl)# exit
```

Remove an ACE from an ACL:

```
switch(config)# access-list ip My_ACL
switch(config-acl)# no 25
switch(config-acl)# exit
```

Remove an ACL:

```
switch(config)# no access-list ip My_ACL
```

Policy-based Routing (PBR)

```
switch(config)# access-list ip pbr
switch(config)# permit any 2.2.2.2 3.3.3.3
switch(config)# exit
switch(config)# route-map ex-pbr-1 permit 1
switch(config)# match ip address access-list pbr
switch(config)# set ip next-hop 1.1.1.1
switch(config)# exit
switch(config)# interface 1
switch(config)# ip policy route-map ex-pbr-1
switch(config)# exit
```

3.16.2. Reset

Reset the configuration and application of all ACLS to match the active configuration. Active configuration means the configuration has passed platform support and capacity checks and is either programmed or pending programming in hardware.

Syntax	reset access-list all
Authority	Admin.
<all>	Operate on all ACLs.

Examples

Reset the entry configuration and application of all ACLs:

```
switch(config)# reset access-list all
```

3.16.3. Log timer

Set the log timer frequency for all ACEs with **log** configured.

The first packet that matches an entry with the *log* keyword within an ACL log timer window (configured with *access-list log-timer*) has its header contents extracted and sent to the configured logging destination (for example, console or syslog server). Each time the ACL log timer expires, a summary of all ACEs with *log* configured is sent to the logging destination.

Syntax	access-list log-timer {default <value>}
---------------	---

Authority Admin.
<default> Reset to the default value (300 seconds).
<value> Specify a value (in seconds, 30-300).

Examples

Set the ACL log timer to 120 seconds:

```
switch(config)# access-list log-timer 120
```

Reset the ACL log timer to the default value:

```
switch(config)# access-list log-timer default
```

3.16.4. Interface Application, replacement, and removal

Apply an ACL to the current interface context.

Only one direction (for example, inbound) and type (for example, IPv4) of ACL may be applied to an interface at a time, thus using the **apply** command on an interface with an already-applied ACL of the same direction and type replaces the currently-applied ACL.

Syntax [no] apply access-list ip <acl-name> {in|out}
Authority Admin.
<ip> Apply an IPv4 ACL.
<acl-name> Name of the ACL to apply.
<direction> Choose in to apply to inbound (ingress) traffic or out for outbound (egress) traffic.

Examples

Apply *My_ACL* to ingress traffic on interfaces 1 and 2

```
switch(config)# interface 1
switch(config-if)# apply access-list ip My_ACL in
switch(config-if)# exit
switch(config)# interface 2
switch(config-if)# apply access-list ip My_ACL in
switch(config-if)# exit
switch(config)#
```

Replace *My_ACL* with *My_Replacement_ACL* on interface 1 (following the above example, *My_ACL* remains applied to interface 2):

```
switch(config)# interface 1
switch(config-if)# apply access-list ip My_Replacement_ACL in
switch(config-if)# exit
switch(config)#
```

Apply no ACL on interface 1 (following the above example, *My_ACL* remains applied to interface 2):

```
switch(config)# interface 1
switch(config-if)# no apply access-list ip My_Replacement_ACL in
switch(config-if)# exit
switch(config)#
```

3.16.5. VLAN Application, replacement, and removal



Applying ACLs to VLANs is not yet supported by all OpenSwitch components. The CLI commands presented in this document are available, but the ACLs are not programmed unless all components are enhanced to support VLAN ACL apply operations.*

Apply an ACL to the current VLAN context.

Only one direction (for example, inbound) and type (for example, IPv4) of ACL may be applied to a VLAN at a time, thus using the *apply* command on a VLAN with an already-applied ACL of the same direction and type replaces the currently-applied ACL.

Syntax [no] apply access-list ip <acl-name> {in|out}
Authority Admin.
 <ip> Apply an IPv4 ACL.
 <acl-name> Name of the ACL to apply.
 <direction> Choose in to apply to inbound (ingress) traffic or out for outbound (egress) traffic.

Examples

Apply *My_ACL* to ingress traffic on VLANs 1 and 2

```
switch(config)# vlan 1
switch(config-vlan)# apply access-list ip My_ACL in
switch(config-vlan)# exit
switch(config)# vlan 2
switch(config-vlan)# apply access-list ip My_ACL in
switch(config-vlan)# exit
switch(config)#
```

Replace *My_ACL* with *My_Replacement_ACL* on VLAN 1 (following the above example, *My_ACL* remains applied to VLAN 2):

```
switch(config)# vlan 1
switch(config-vlan)# apply access-list ip My_Replacement_ACL in
switch(config-vlan)# exit
switch(config)#
```

Apply no ACL on VLAN 1 (following the above example, *My_ACL* remains applied to VLAN 2):

```
switch(config)# vlan 1
switch(config-vlan)# no apply access-list ip My_Replacement_ACL in
switch(config-vlan)# exit
switch(config)#
```

3.16.6. Global context Display

Displays configured, active ACLs and their entries.

By default, **show access-list** displays the ACL configuration active in the system. Active configuration means the configuration has passed platform support and capacity checks, and is either programmed or pending programming in hardware.

By specifying the *configuration* token, the user-specified configuration is displayed, whether or not it is active. This command displays a warning if the active and user-specified configuration do not match. In such a case, the user may wish to use the **reset access-list** command (see Section 3.16.2, "Reset").

Specifying *commands* displays active ACL entries as well as the state of any **apply** commands on interfaces.

Syntax	show access-list [{interface vlan} <id> [{in out}]] [ip] [<acl-name>] [config]
Authority	Admin.
<interface>	Display ACLs applied to a specified interface name.
<vlan>	Display ACLs applied to a specified VLAN ID.
<id>	The name or ID of the interface or VLAN.
<direction>	Choose in to limit display to ingress ACLs or out for egress ACLs.
<ip>	Limit display to IPv4 ACLs.
<acl-name>	Display the ACL matching the name.
<commands>	Display output as CLI commands.
<configuration>	Display the user-specified configuration.

Examples

Display ACLs configured in examples from previous sections:

```
switch# show access-list
Type      Name
Sequence Comment
          Action                    L3 Protocol
          Source IP Address          Source L4 Port(s)
          Destination IP Address      Destination L4 Port(s)
          Additional Parameters
-----
IPv4      My_ACL
10 permit any 172.16.1.0/24          udp
20 Permit all TCP ephemeral ports
   permit 172.16.2.0/16          tcp
   any > 1023
30 deny any
```

```
any
any
Hit-counts: enabled
```

Display ACLs configured and applied in above examples as CLI commands:

```
switch# show access-list commands
access-list ip My_ACL
 10 permit udp any 172.16.1.0/24
 20 permit tcp 172.16.2.0/16 gt 1023 any
 30 deny any any any count
interface 2
 apply access-list ip My_ACL in
```

3.16.7. Statistics (hit counts)

Display or clear hit counts for ACEs with the *count* keyword in the specified ACL.

If an entry does not have the *count* keyword enabled, it displays the - character instead of a hit count.

- Syntax** show access-list hitcounts ip <acl-name> [{interface|vlan} <id> [{in|out}]]
- Syntax** clear access-list hitcounts {all|ip <acl-name> {interface|vlan} <id> [{in|out}]}
- Authority** Admin.
- <all> Operate on all ACLs.
- <ip> Operate on an IPv4 ACL.
- <acl-name> Operate on a named ACL.
- <interface> Specify the interface to which the ACL is applied.
- <vlan> Specify the VLAN to which the ACL is applied.
- <id> The name or ID of the interface or VLAN.
- <direction> Choose in to operate on ACLs applied to ingress traffic or out for egress traffic.

Examples

Display hit counts for ACL configured in above examples:

```
switch# show access-list hitcounts ip My_ACL interface 1
Statistics for ACL My_ACL (ipv4):
Interface 1 (in):
  Hit Count  Configuration
  - 10 permit udp any 172.16.1.0/24
  - 20 permit tcp 172.16.2.0/16 gt 1023 any
  0 30 deny any any any count
```

Clear hit counts for ACL configured in above examples:

```
switch# clear access-list hitcounts ip My_ACL interface 1
```

Clear hit counts for all configured ACLs:

```
switch# clear access-list hitcounts all
```

3.16.8. Log timer

Display ACL log timer configuration. See log timer configuration for information on changing this setting.

Syntax show access-list log-timer

Authority Admin.

Examples

```
switch# show access-list log-timer
```

3.17. Show Events Command

3.17.1. Display commands

Displays events for all supported features

Runs the **show events** command for all the supported features.

Syntax	show events
Authority	All users
<event-id <ev-id>>	Displays events with supplied event ID
<severity <severity-level>>	Displays events with supplied severity
<category <category>>	Displays events of supplied category
<reverse>	Displays events in reverse order

Examples

```
switch# configure t
switch(config)# lldp enable
switch(config)# no lldp enable
switch(config)# lldp timer 100
switch(config)# lldp management-address 10.0.0.1
switch(config)# end
```

events log

```
switch# show events
2016-01-20:14:17:15.041851|ops-lldpd|1002|LOG_INFO|LLDP Disabled
2016-01-20:14:17:54.562838|ops-lldpd|1001|LOG_INFO|LLDP Enabled
2016-01-20:14:18:55.397152|ops-lldpd|1003|LOG_INFO|Configured LLDP tx-timer with 100
2016-01-20:14:20:16.715133|ops-lldpd|1007|LOG_INFO|Configured LLDP Management patter
```

show event logs

```
switch# show events event-id 1002
2016-02-19:03:55:05.391372|ops-lldpd|1002|LOG_INFO|LLDP Disabled
```

show event logs

```
switch# show events category LLDP
2016-02-19:03:55:05.391372|ops-lldpd|1002|LOG_INFO|LLDP Disabled
2016-02-19:03:57:50.249296|ops-lldpd|1003|LOG_INFO|Configured LLDP tx-timer with 9
2016-02-19:03:57:57.342332|ops-lldpd|1007|LOG_INFO|Configured LLDP Management patter
```

show event logs

```
switch# show events severity emer
```

```
No event match the filter provided
```

show event logs

```
switch# show events reverse
2016-02-19:03:57:57.342332|ops-lldpd|1007|LOG_INFO|Configured LLDP Management patter
2016-02-19:03:57:50.249296|ops-lldpd|1003|LOG_INFO|Configured LLDP tx-timer with 9
2016-02-19:03:55:05.391372|ops-lldpd|1002|LOG_INFO|LLDP Disabled
```

3.18. Audit Log

The default audit log file is located at `/var/log/audit/audit.log`. A typical raw log record appears as follows:

```
type=USYS_CONFIG msg=audit(1446776250.787:91): pid=540 uid=1002
aid=4294967295 ses=4294967295 msg='op=CLI:Set-Hostname data="newHostName"
exe="/usr/bin/vtysh" hostname=? addr=? terminal=pts/1 res=success
```

This particular record was generated by prototype code calling the `audit_log_user_message()` function in `vttysh`. Most fields are self-explanatory. Several fields match the parameters supplied in the `audit_log_user_message()` function. Explanations for some fields are as follows:

- `msg=audit(1446776250.787:91)` is the time stamp and event number. The time stamp value is 1446776250.787 and the event number is 91.
- `pid=540` is the process ID of the program that made the audit log call.
- `uid=1002` is the user ID of the program that made the audit log call.
- `aid=4294967295` is the login user ID. This specific value represents -1 for a "C" int and indicates the value is not set.
- `ses=4294967295` is the session ID, if any. In this case, it is not set.
- `op=CLI:Set-Hostname data="newHostName"` is the content of the message parameter passed to `audit_log_user_message()`.

The `ausearch` utility is used to display audit log events. Note that all audit utilities are restricted to the root user. To get easier to read output, use the `-i` or `--interpret` option. Consult the man page for more information about the many options available for this utility. If `ausearch -i -a 91` was issued to display event number 91, it would output the following:

```
type=USYS_CONFIG msg=audit(11/06/15 02:17:30.787:91) : pid=540 uid=fredf
aid=unset ses=unset msg='op=CLI:Set-Hostname
data="newHostName"exe=/usr/bin/vtysh hostname=? addr=? terminal=pts/1
res=success'
```

The other main audit utility is `aureport`, which is used to get a variety of summary reports. Read the man page for additional details. Running `aureport` without any options displays the following summary:

```
Summary Report
=====
Range of time in logs: 01/08/01 07:11:42.847 - 11/06/15 03:01:02.171
Selected time for report: 01/08/01 07:11:42 - 11/06/15 03:01:02.171
Number of changes in configuration: 2
Number of changes to accounts, groups, or roles: 5
Number of logins: 0
Number of failed logins: 0
Number of authentications: 3
Number of failed authentications: 5
Number of users: 1
```

```
Number of terminals: 5
Number of host names: 3
Number of executables: 8
Number of commands: 3
Number of files: 0
Number of AVC's: 0
Number of MAC events: 0
Number of failed syscalls: 0
Number of anomaly events: 0
Number of responses to anomaly events: 0
Number of crypto events: 0
Number of integrity events: 0
Number of virt events: 0
Number of keys: 0
Number of process IDs: 14
Number of events: 92
```

A typical report for OpenSwitch is a configuration report using "aureport -c", which displays the following:

```
Config Change Report
=====
# date time type auid success event
=====
1. 11/06/15 02:17:30 USYS_CONFIG -1 yes 91
2. 11/06/15 02:17:30 USYS_CONFIG -1 yes 93
```

3.18.1. Additional references

Linux Audit Framework web site - <http://people.redhat.com/sgrubb/audit/>

Linux Audit Quick Start - https://www.suse.com/documentation/sles11/singlehtml/audit_quickstart/audit_quickstart.html

3.19. Ping Utility

3.19.1. IPv4 address

This command is used to ping a specific IPv4 address.

Syntax ping <IPv4-address>
Authority Root user.
<IPv4-ad-
dress> IPv4 address to ping.

Examples

```
switch# ping 9.0.0.1
PING 9.0.0.1 (9.0.0.1) 100(128) bytes of data.
108 bytes from 9.0.0.1: icmp_seq=1 ttl=64 time=0.035 ms
108 bytes from 9.0.0.1: icmp_seq=2 ttl=64 time=0.034 ms
108 bytes from 9.0.0.1: icmp_seq=3 ttl=64 time=0.034 ms
108 bytes from 9.0.0.1: icmp_seq=4 ttl=64 time=0.034 ms
108 bytes from 9.0.0.1: icmp_seq=5 ttl=64 time=0.033 ms
```

```
--- 9.0.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.033/0.034/0.035/0.000 ms
```

3.19.2. Hostname

This command is used to ping a specific Hostname.

Syntax ping <hostname>
Authority Root user.
<hostname> Hostname to ping. Length must be less than 256 characters.

Examples

```
switch# ping localhost
PING localhost (127.0.0.1) 100(128) bytes of data.
108 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.060 ms
108 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.035 ms
108 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.043 ms
108 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.041 ms
108 bytes from localhost (127.0.0.1): icmp_seq=5 ttl=64 time=0.034 ms
```

```
--- localhost ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 0.034/0.042/0.060/0.011 ms
```

3.19.3. Set data-fill pattern

This command sets the hexadecimal pattern to be filled in the packet.

Syntax ping (<IPv4-address> | <hostname>) data-fill <pattern>
Authority Root user.
 <pattern> Set the hexadecimal pattern to be filled in the packet. A Maximum of 16 *pad* bytes can be specified to fill out the icmp packet.

Examples

```
switch# ping 10.0.0.2 data-fill 1234123412341234acde123456789012
PATTERN: 0x1234123412341234acde123456789012
PING 10.0.0.2 (10.0.0.2) 100(128) bytes of data.
108 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=0.207 ms
108 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.187 ms
108 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=0.225 ms
108 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=0.197 ms
108 bytes from 10.0.0.2: icmp_seq=5 ttl=64 time=0.210 ms
```

```
--- 10.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.187/0.205/0.225/0.015 ms
```

3.19.4. Set datagram-size

This command sets the size of the packet to be sent. The default value is 100 bytes.

Syntax ping (<IPv4-address> | <hostname>) datagram-size <size>
Authority Root user.
 <size> Select the datagram-size between 100 and 65399.

Examples

```
switch# ping 9.0.0.2 datagram-size 200
PING 9.0.0.2 (9.0.0.2) 200(228) bytes of data.
208 bytes from 9.0.0.2: icmp_seq=1 ttl=64 time=0.202 ms
208 bytes from 9.0.0.2: icmp_seq=2 ttl=64 time=0.194 ms
208 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.201 ms
208 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.200 ms
208 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.186 ms
```

```
--- 9.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.186/0.196/0.202/0.016 ms
```

3.19.5. Set interval

This command sets the interval seconds between sending each packet. The default value is 1 second.

Syntax ping (<IPv4-address> | <hostname>) interval <time>
Authority Root user.

<time> Select an interval in seconds between 1 and 60.

Examples

```
switch# ping 9.0.0.2 interval 2
PING 9.0.0.2 (9.0.0.2) 100(128) bytes of data.
108 bytes from 9.0.0.2: icmp_seq=1 ttl=64 time=0.199 ms
108 bytes from 9.0.0.2: icmp_seq=2 ttl=64 time=0.192 ms
108 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.208 ms
108 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.182 ms
108 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.194 ms
```

```
--- 9.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 7999ms
rtt min/avg/max/mdev = 0.182/0.195/0.208/0.008 ms
```

3.19.6. Set repetitions

This command sets the number of packets to be sent to the destination address. The default value is 5.

Syntax ping (<IPv4-address> | <hostname>) repetitions <number>

Authority Root user.

<number> Select the number of packets to send between 1 and 10000.

Examples

```
switch# ping 9.0.0.2 repetitions 10
PING 9.0.0.2 (9.0.0.2) 100(128) bytes of data.
108 bytes from 9.0.0.2: icmp_seq=1 ttl=64 time=0.213 ms
108 bytes from 9.0.0.2: icmp_seq=2 ttl=64 time=0.204 ms
108 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.201 ms
108 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.184 ms
108 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.202 ms
108 bytes from 9.0.0.2: icmp_seq=6 ttl=64 time=0.184 ms
108 bytes from 9.0.0.2: icmp_seq=7 ttl=64 time=0.193 ms
108 bytes from 9.0.0.2: icmp_seq=8 ttl=64 time=0.196 ms
108 bytes from 9.0.0.2: icmp_seq=9 ttl=64 time=0.193 ms
108 bytes from 9.0.0.2: icmp_seq=10 ttl=64 time=0.200 ms
```

```
--- 9.0.0.2 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 8999ms
rtt min/avg/max/mdev = 0.184/0.197/0.213/0.008 ms
```

3.19.7. Set timeout

This command sets the time to wait for a response in seconds from the receiver. The default value is 2 seconds.

Syntax ping (<IPv4-address> | <hostname>) timeout <time>

Authority Root user.
<time> Select timeout in seconds between 1 and 60.

Examples

```
switch# ping 9.0.0.2 timeout 3
PING 9.0.0.2 (9.0.0.2) 100(128) bytes of data.
108 bytes from 9.0.0.2: icmp_seq=1 ttl=64 time=0.175 ms
108 bytes from 9.0.0.2: icmp_seq=2 ttl=64 time=0.192 ms
108 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.190 ms
108 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.181 ms
108 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.197 ms
```

```
--- 9.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.175/0.187/0.197/0.007 ms
```

3.19.8. Set TOS

This command sets Type of Service (TOS) related bits in ICMP datagrams.

Syntax ping (<IPv4-address> | <hostname>) tos <number>
Authority Root user.
<number> Select the TOS value between 0 and 255.

Examples

```
switch# ping 9.0.0.2 tos 2
PING 9.0.0.2 (9.0.0.2) 100(128) bytes of data.
108 bytes from 9.0.0.2: icmp_seq=1 ttl=64 time=0.033 ms
108 bytes from 9.0.0.2: icmp_seq=2 ttl=64 time=0.034 ms
108 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.031 ms
108 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.034 ms
108 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.031 ms
```

```
--- 9.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.031/0.032/0.034/0.006 ms
```

3.19.9. Set ip-option

This command is used to record either the intermediate router timestamp, the intermediate router timestamp and IP address, or the intermediate router addresses.

Syntax ping (<IPv4-address> | <hostname>) ip-option (include-timestamp |include-time-stamp-and-address |record-route)
Authority Root user.

Examples

```
switch# ping 9.0.0.2 ip-option include-timestamp
```

Management And Utility Commands

```
PING 9.0.0.2 (9.0.0.2) 100(168) bytes of data.  
108 bytes from 9.0.0.2: icmp_seq=1 ttl=64 time=0.031 ms  
TS:      59909005 absolute  
        0  
        0  
        0
```

```
108 bytes from 9.0.0.2: icmp_seq=2 ttl=64 time=0.034 ms  
TS:      59910005 absolute  
        0  
        0  
        0
```

```
108 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.038 ms  
TS:      59911005 absolute  
        0  
        0  
        0
```

```
108 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.035 ms  
TS:      59912005 absolute  
        0  
        0  
        0
```

```
108 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.037 ms  
TS:      59913005 absolute  
        0  
        0  
        0
```

```
--- 9.0.0.2 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 3999ms  
rtt min/avg/max/mdev = 0.031/0.035/0.038/0.002 ms
```

```
switch# ping 9.0.0.2 ip-option include-timestamp-and-address  
PING 9.0.0.2 (9.0.0.2) 100(168) bytes of data.  
108 bytes from 9.0.0.2: icmp_seq=1 ttl=64 time=0.030 ms  
TS:      9.0.0.2 60007355 absolute  
        9.0.0.2 0  
        9.0.0.2 0  
        9.0.0.2 0
```

```
108 bytes from 9.0.0.2: icmp_seq=2 ttl=64 time=0.037 ms  
TS:      9.0.0.2 60008355 absolute  
        9.0.0.2 0  
        9.0.0.2 0  
        9.0.0.2 0
```

```
108 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.037 ms  
TS:      9.0.0.2 60009355 absolute  
        9.0.0.2 0  
        9.0.0.2 0
```

```
9.0.0.2 0

108 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.038 ms
TS: 9.0.0.2 60010355 absolute
    9.0.0.2 0
    9.0.0.2 0
    9.0.0.2 0

108 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.039 ms
TS: 9.0.0.2 60011355 absolute
    9.0.0.2 0
    9.0.0.2 0
    9.0.0.2 0

--- 9.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.030/0.036/0.039/0.005 ms

switch# ping 9.0.0.2 ip-option record-route
PING 9.0.0.2 (9.0.0.2) 100(168) bytes of data.
108 bytes from 9.0.0.2: icmp_seq=1 ttl=64 time=0.034 ms
RR: 9.0.0.2
    9.0.0.2
    9.0.0.2
    9.0.0.2

108 bytes from 9.0.0.2: icmp_seq=2 ttl=64 time=0.038 ms (same route)
108 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.036 ms (same route)
108 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.037 ms (same route)
108 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.035 ms (same route)

--- 9.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.034/0.036/0.038/0.001 ms
```

3.19.10. IPv6 address

This command is used to ping the specified IPv6 address.

- Syntax** ping6 <IPv6-address>
- Authority** Root user.
- <IPv6-address>** IPv6 address to ping.

Examples

```
switch# ping6 2020::2
PING 2020::2(2020::2) 100 data bytes
108 bytes from 2020::2: icmp_seq=1 ttl=64 time=0.386 ms
108 bytes from 2020::2: icmp_seq=2 ttl=64 time=0.235 ms
108 bytes from 2020::2: icmp_seq=3 ttl=64 time=0.249 ms
108 bytes from 2020::2: icmp_seq=4 ttl=64 time=0.240 ms
```

```
108 bytes from 2020::2: icmp_seq=5 ttl=64 time=0.252 ms
```

```
--- 2020::2 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4000ms  
rtt min/avg/max/mdev = 0.235/0.272/0.386/0.059 ms
```

3.19.11. IPv6 Hostname

This command is used to ping the specified Hostname.

Syntax ping6 <hostname>
Authority Root user.
<hostname> Hostname to ping. Length must be less than 256 characters.

Examples

```
switch# ping6 localhost  
PING localhost(localhost) 100 data bytes  
108 bytes from localhost: icmp_seq=1 ttl=64 time=0.093 ms  
108 bytes from localhost: icmp_seq=2 ttl=64 time=0.051 ms  
108 bytes from localhost: icmp_seq=3 ttl=64 time=0.055 ms  
108 bytes from localhost: icmp_seq=4 ttl=64 time=0.046 ms  
108 bytes from localhost: icmp_seq=5 ttl=64 time=0.048 ms
```

```
--- localhost ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 3998ms  
rtt min/avg/max/mdev = 0.046/0.058/0.093/0.019 ms
```

3.19.12. IPv6 Set data-fill pattern

This command sets the hexadecimal pattern to be filled in the packet.

Syntax ping6 (<IPv6-address> | <hostname>) data-fill <pattern>
Authority Root user.
<pattern> Set the hexadecimal pattern to be filled in the packet. A Maximum of 16 *pad* bytes can be specified to fill out the icmp packet.

Examples

```
switch# ping6 2020::2 data-fill ab  
PATTERN: 0xab  
PING 2020::2(2020::2) 100 data bytes  
108 bytes from 2020::2: icmp_seq=1 ttl=64 time=0.038 ms  
108 bytes from 2020::2: icmp_seq=2 ttl=64 time=0.074 ms  
108 bytes from 2020::2: icmp_seq=3 ttl=64 time=0.076 ms  
108 bytes from 2020::2: icmp_seq=4 ttl=64 time=0.075 ms  
108 bytes from 2020::2: icmp_seq=5 ttl=64 time=0.077 ms
```

```
--- 2020::2 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 3999ms  
rtt min/avg/max/mdev = 0.038/0.068/0.077/0.015 ms
```

3.19.13. IPv6 Set datagram-size

This command sets the size of the packet to be sent. The default value is 100 bytes.

Syntax ping6 (<IPv6-address> | <hostname>) datagram-size <size>
Authority Root user.
<size> Select datagram-size between 100 and 65468.

Examples

```
switch# ping6 2020::2 datagram-size 200
PING 2020::2(2020::2) 200 data bytes
208 bytes from 2020::2: icmp_seq=1 ttl=64 time=0.037 ms
208 bytes from 2020::2: icmp_seq=2 ttl=64 time=0.076 ms
208 bytes from 2020::2: icmp_seq=3 ttl=64 time=0.076 ms
208 bytes from 2020::2: icmp_seq=4 ttl=64 time=0.077 ms
208 bytes from 2020::2: icmp_seq=5 ttl=64 time=0.066 ms

--- 2020::2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.037/0.066/0.077/0.016 ms
```

3.19.14. IPv6 Set interval

This command sets the interval seconds between sending each packet. The default value is 1 second.

Syntax ping6 (<IPv6-address> | <hostname>) interval <time>
Authority Root user.
<time> Select interval in seconds between 1 and 60.

Examples

```
switch# ping6 2020::2 interval 5
PING 2020::2(2020::2) 100 data bytes
108 bytes from 2020::2: icmp_seq=1 ttl=64 time=0.043 ms
108 bytes from 2020::2: icmp_seq=2 ttl=64 time=0.075 ms
108 bytes from 2020::2: icmp_seq=3 ttl=64 time=0.074 ms
108 bytes from 2020::2: icmp_seq=4 ttl=64 time=0.075 ms
108 bytes from 2020::2: icmp_seq=5 ttl=64 time=0.075 ms

--- 2020::2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 19999ms
rtt min/avg/max/mdev = 0.043/0.068/0.075/0.014 ms
```

3.19.15. IPv6 Set repetitions

This command sets the number of packets to be sent to the destination address. The default value is 5.

Syntax ping6 (<IPv6-address> | <hostname>) repetitions <number>
Authority Root user.
<number> Select the number of packets to send between 1 and 10000.

Examples

```
switch# ping6 2020::2 repetitions 6
PING 2020::2(2020::2) 100 data bytes
108 bytes from 2020::2: icmp_seq=1 ttl=64 time=0.039 ms
108 bytes from 2020::2: icmp_seq=2 ttl=64 time=0.070 ms
108 bytes from 2020::2: icmp_seq=3 ttl=64 time=0.076 ms
108 bytes from 2020::2: icmp_seq=4 ttl=64 time=0.076 ms
108 bytes from 2020::2: icmp_seq=5 ttl=64 time=0.071 ms
108 bytes from 2020::2: icmp_seq=6 ttl=64 time=0.078 ms
```

```
--- 2020::2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4999ms
rtt min/avg/max/mdev = 0.039/0.068/0.078/0.015 ms
```

3.20. Traceroute Utility

3.20.1. IPv4 address

This command is used to traceroute the specified IPv4 address.

Syntax traceroute <IPv4-address>

Authority Root user.

<IPv4-ad-
dress> IPv4 address to traceroute.

Examples

```
switch# traceroute 10.0.10.1
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 30 hops max, 3 sec.
timeout, 3 probes
 1  10.0.40.2  0.002ms  0.002ms  0.001ms
 2  10.0.30.1  0.002ms  0.001ms  0.001ms
 3  10.0.10.1  0.001ms  0.002ms  0.002ms
```

3.20.2. Hostname

This command is used to traceroute the specified Hostname.

Syntax traceroute <hostname>

Authority Root user.

<hostname> Hostname to traceroute. Length must be less than 256 characters.

Examples

```
switch# traceroute localhost
traceroute to localhost (127.0.0.1), 1 hops min, 30 hops max, 3 sec.
timeout, 3 probes
 1  127.0.0.1  0.018ms  0.006ms  0.003ms
```

3.20.3. Set maximum TTL

This command sets the maximum number of hops used in outgoing probe packets. The default value is 30.

Syntax traceroute (<IPv4-address> | <hostname>) maxttl <number>

Authority Root user.

<IPv4-ad-
dress> IPv4 address to traceroute.

<hostname> Hostname to traceroute. Length must be less than 256 characters.

<number> Select maximum number of hops used in outgoing probe packets between 1 to 255.

Examples

```
switch# traceroute 10.0.10.1 maxttl 20
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 20 hops max, 3 sec.
timeout, 3 probes
 1  10.0.40.2  0.002ms  0.002ms  0.001ms
 2  10.0.30.1  0.002ms  0.001ms  0.001ms
 3  10.0.10.1  0.001ms  0.002ms  0.002ms
```

3.20.4. Set minimum TTL

This command sets the minimum number of hops used in outgoing probe packets. The default value is 1.

Syntax traceroute (<IPv4-address> | <hostname>) minttl <number>
Authority Root user.
 <IPv4-address> IPv4 address to traceroute.
 <hostname> Hostname to traceroute. Length must be less than 256 characters.
 <number> Select maximum number of hops used in outgoing probe packets between 1 to 255.

Examples

```
switch# traceroute 10.0.10.1 minttl 1
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 30 hops max, 3 sec.
timeout, 3 probes
 1  10.0.40.2  0.002ms  0.002ms  0.001ms
 2  10.0.30.1  0.002ms  0.001ms  0.001ms
 3  10.0.10.1  0.001ms  0.002ms  0.002ms
```

3.20.5. Set destination port

This command sets the destination port. The default value is dstport 33434.

Syntax traceroute (<IPv4-address> | <hostname>) dstport <number>
Authority Root user.
 <IPv4-address> IPv4 address to traceroute.
 <hostname> Hostname to traceroute. Length must be less than 256 characters.
 <number> Select the destination port number, 1-34000.

Examples

```
switch# traceroute 10.0.10.1 dstport 33434
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 30 hops max, 3 sec.
timeout, 3 probes
 1  10.0.40.2  0.002ms  0.002ms  0.001ms
```

```

2  10.0.30.1  0.002ms  0.001ms  0.001ms
3  10.0.10.1  0.001ms  0.002ms  0.002ms

```

3.20.6. Set probes

This command sets the number of probe queries to send out for each hop. The default value is 3.

- Syntax** tracert (<IPv4-address> | <hostname>) probes <number>
- Authority** Root user.
- <IPv4-ad-
dress> IPv4 address to tracert.
- <hostname> Hostname to tracert. Length must be less than 256 characters.
- <number> Select the number of probe queries to send out for each hop between 1 to 5.

Examples

```

switch# tracert 10.0.10.1 probes 3
tracert to 10.0.10.1 (10.0.10.1) , 1 hops min, 30 hops max, 3 sec.
timeout, 3 probes
1  10.0.40.2  0.002ms  0.002ms  0.001ms
2  10.0.30.1  0.002ms  0.001ms  0.001ms
3  10.0.10.1  0.001ms  0.002ms  0.002ms

```

3.20.7. Set timeout

This command sets the time in seconds to wait for a response to a probe. The default value is 3 seconds.

- Syntax** tracert (<IPv4-address> | <hostname>) timeout <time>
- Authority** Root user.
- <IPv4-ad-
dress> IPv4 address to tracert.
- <hostname> Hostname to tracert. Length must be less than 256 characters.
- <time> Select time in seconds to wait for a response to a probe between 1 and 60.

Examples

```

switch# tracert 10.0.10.1 timeout 5
tracert to 10.0.10.1 (10.0.10.1) , 1 hops min, 30 hops max, 5 sec.
timeout, 3 probes
1  10.0.40.2  0.002ms  0.002ms  0.001ms
2  10.0.30.1  0.002ms  0.001ms  0.001ms
3  10.0.10.1  0.001ms  0.002ms  0.002ms

```

3.20.8. Set ip-option loose source route

This command is used to set the the intermediate loose source route address.

Syntax tracert (<IPv4-address> | <hostname>) ip-option loosesourceroute <IPv4-Address>

Authority Root user.

<IPv4-ad-
dress> IPv4 address to tracert.

<hostname> Hostname to tracert. Length must be less than 256 characters.

<IPv4-ad-
dress> Loose source route address to tracert.

Examples

```
switch# tracert 10.0.10.1 ip-option loosesourceroute 10.0.40.2
tracert to 10.0.10.1 (10.0.10.1) , 1 hops min, 30 hops max, 3 sec.
timeout, 3 probes
 1  10.0.40.2  0.002ms  0.002ms  0.001ms
 2  10.0.30.1  0.002ms  0.001ms  0.001ms
 3  10.0.10.1  0.001ms  0.002ms  0.002ms
```

3.20.9. IPv6 address

This command is used to tracert the specified IPv6 address.

Syntax tracert6 <IPv6-address>

Authority Root user.

<IPv6-ad-
dress> IPv6 address to tracert.

Examples

```
switch# tracert6 0:0::0:1
tracert to 0:0::0:1 (::1) from ::1, 30 hops max, 3 sec. timeout, 3 probes,
24 byte packets
 1  localhost (::1)  0.117 ms  0.032 ms  0.021 ms
```

3.20.10. IPv6 Hostname

This command is used to tracert the specified Hostname.

Syntax tracert6 <hostname>

Authority Root user.

<hostname> Hostname to tracert. Length must be less than 256 characters.

Examples

```
switch# tracert6 localhost
tracert to localhost (::1) from ::1, 30 hops max, 3 sec. timeout, 3
probes, 24 byte packets
 1  localhost (::1)  0.189 ms  0.089 ms  0.025 ms
```

3.20.11. IPv6 Set maximum TTL

This command sets the maximum number of hops used in outgoing probe packets. The default value is 30.

Syntax	traceroute6 (<IPv6-address> <hostname>) maxttl <number>
Authority	Root user.
<IPv6-address>	IPv6 address to traceroute.
<hostname>	Hostname to traceroute. Length must be less than 256 characters.
<number>	Select maximum number of hops used in outgoing probe packets between 1 to 255.

Examples

```
switch# traceroute6 0:0::0:1 maxttl 30
traceroute to 0:0::0:1 (:::1) from :::1, 30 hops max, 3 sec. timeout, 3
probes, 24 byte packets
1 localhost (:::1) 0.117 ms 0.032 ms 0.021 ms
```

3.20.12. IPv6 Set destination port

This command sets the destination port. The default value is dstport 33434.

Syntax	traceroute6 (<IPv6-address> <hostname>) dstport <number>
Authority	Root user.
<IPv6-address>	IPv6 address to traceroute.
<hostname>	Hostname to traceroute. Length must be less than 256 characters.
<number>	Select the destination port number, 1-34000.

Examples

```
switch# traceroute6 0:0::0:1 dstport 33434
traceroute to 0:0::0:1 (:::1) from :::1, 30 hops max, 3 sec. timeout, 3
probes, 24 byte packets
1 localhost (:::1) 0.117 ms 0.032 ms 0.021 ms
```

3.20.13. IPv6 Set probes

This command sets the number of probe queries to send out for each hop. The default value is 3.

Syntax	traceroute6 (<IPv6-address> <hostname>) probes <number>
Authority	Root user.
<IPv6-address>	IPv6 address to traceroute.
<hostname>	Hostname to traceroute. Length must be less than 256 characters.

<number> Select the number of probe queries to send out for each hop between 1 to 5.

Examples

```
switch# traceroute6 0:0::0:1 probes 3
traceroute to 0:0::0:1 (::1) from ::1, 30 hops max, 3 sec. timeout, 3
probes, 24 byte packets
1 localhost (::1) 0.117 ms 0.032 ms 0.021 ms
```

3.20.14. IPv6 Set timeout

This command sets the time in seconds to wait for a response to a probe. The default value is 3 seconds.

Syntax traceroute6 (<IPv6-address> | <hostname>) timeout <time>

Authority Root user.

<IPv6-ad-
dress> IPv6 address to traceroute.

<hostname> Hostname to traceroute. Length must be less than 256 characters.

<time> Select time in seconds to wait for a response to a probe between 1 and 60.

Examples

```
switch# traceroute6 0:0::0:1 timeout 3
traceroute to 0:0::0:1 (::1) from ::1, 30 hops max, 3 sec. timeout, 3
probes, 24 byte packets
1 localhost (::1) 0.117 ms 0.032 ms 0.021 ms
```

3.21. Diagnostic Dump Commands

3.21.1. Show supported feature list

This command displays the list of features supported by the diag-dump CLI.

Syntax diag-dump list

Authority All users

Examples

```
switch# diag-dump list
Diagnostic Dump Supported Features List
-----
Feature                               Description
-----
sys                                    System Daemon and Mgmt Info
lldp                                   Link Layer Discovery Protocol
lacp                                   Link Aggregation Control Protocol
l3port                                 Layer 3 Port
bgp                                    Border Gateway Protocol
subinterface                           Layer 3 sub-interface
loopback                               Loopback interface
rest                                    REST interface
ntp                                     Network Time Protocol
mstp                                    Multiple Spanning Tree Protocol
...
switch#
```

3.21.2. Show basic diagnostic

This command displays the basic diagnostic information of the feature. Check for supported features by using the **diag-dump list** command.

Syntax diag-dump <feature> basic

Authority All users

Examples

```
switch# diag-dump ?
FEATURE_NAME  Feature name
list          Show supported features with description
```

```
switch# diag-dump list
Diagnostic Dump Supported Features List
lldp                                   Link Layer Discovery Protocol
```

```
switch# diag-dump lldp
basic  Basic information
```

```
switch# diag-dump lldp basic
LLDP : DISABLED
```

intf name	OVSDB interface	LLDPD Interface	LLDP Status	Link State
bridge_normal	Yes	Yes	rctx	down
51-3	Yes	No		
53	Yes	No		
49-4	Yes	No		
51-1	Yes	No		
35	Yes	No		
39	Yes	No		
4	Yes	No		
6	Yes	No		
50-1	Yes	No		
53-3	Yes	No		
....				

```
Diagnostic dump captured for feature lldp
```

3.21.3. Capture basic diagnostic to file

This command captures the diagnostic information in a given file.

Syntax diag-dump basic [FILE]

Authority All users

Examples

```
switch# diag-dump lldp basic lldp.txt
```

3.22. Core Dump CLI Guide

3.22.1. Copy an instance of daemon coredump to tftp

This command copies only one instance of the coredump daemon file to the destination tftp server. The destination filename is an optional parameter. If the destination file name (optional) is not provided, the source file name is used as the destination file name.

Syntax copy core-dump <DAEMONNAME> instance-id <INSTANCE ID> tftp <TFTP SERVER IPV4 ADDRESS /HOST NAME> [FILENAME]

Authority The root and netop users can copy corefiles to any external tftp or sftp server from the switch.

<daemon name> Daemon name

<instance id> Instance id of core file, 1-65535

<tftp server address> Host name of TFTP server

<file name> Destination file name

Examples

```
switch# show core-dump
=====
Daemon Name          | Instance ID | Crash Reason          | Timestamp
=====
ops-vland            439          Aborted               2016-04-26 18:05:28
ops-vland            410          Aborted               2016-04-26 18:08:59
=====
Total number of core dumps : 2
=====
switch#
switch# copy core-dump ops-vland instance-id 439 tftp 10.0.12.161 ops-vland.xz
copying ...
Sent 109188 bytes in 0.1 seconds
switch#
```

If there are no core dumps present with a given instance, then the following information appears:
No coredump found for daemon <daemon name>

```
switch# copy core-dump ops-vland instance-id 567 tftp 10.0.12.161 ops-vland.xz
No coredump found for daemon ops-vland with instance 567
switch#
```

3.22.2. Copy all instances of a corefile for a daemon

This command copies all of the corefile instances for a daemon to the destination tftp server.

Syntax copy core-dump <DAEMONNAME> tftp <TFTP SERVER IPV4 ADDRESS / HOSTNAME >

Authority The root and netop users can copy corefiles to any external tftp or sftp server from the switch.

<daemon name> Daemon name

<tftp server address> Host name of TFTP server

Examples

```
switch# show core-dump
=====
Daemon Name          | Instance ID | Crash Reason          | Timestamp
=====
ops-vland            | 439         | Aborted              | 2016-04-26 18:05:28
ops-vland            | 410         | Aborted              | 2016-04-26 18:08:59
=====
Total number of core dumps : 2
=====
switch#
switch# copy core-dump ops-vland tftp 10.0.12.161
copying ...
Sent 109188 bytes in 0.1 seconds
copying ...
Sent 109044 bytes in 0.0 seconds
switch#
```

If there are no core dumps files present, then the following information appears:

```
switch# copy core-dump ops-lldpd tftp 10.0.12.161
No coredump found for daemon ops-lldpd
switch#
```

3.22.3. Copy kernel corefile to tftp server

This command copies the daemon coredump to the destination sftp server. You can specify the destination filename by specifying in the command.

Syntax copy core-dump kernel tftp <TFTP SERVER IPV4 ADDRESS / HOST NAME > [FILENAME]

Authority The root and netop users can copy corefiles to any external tftp or sftp server from the switch.

<tftp server address> Host name of TFTP server

<file name> Destination file name

Examples

```
switch# show core-dump
=====
Daemon Name          | Instance ID | Crash Reason          | Timestamp
=====
```

```
=====
ops-vland          439          Aborted          2016-04-26 18:05:28
ops-vland          410          Aborted          2016-04-26 18:08:59
kernel             2016-04-26 18:04:20
=====
Total number of core dumps : 3
=====
```

```
switch#
switch#
switch# copy core-dump kernel
sftp tftp
switch# copy core-dump kernel
sftp Copy coredump to sftp server
tftp Copy coredump to tftp server
switch# copy core-dump kernel tftp
A.B.C.D Specify server IP
WORD Specify server name
switch# copy core-dump kernel tftp 10.0.12.161
<cr>
[FILENAME] Specify destination file name
```

```
switch# copy core-dump kernel tftp 10.0.12.161
copying ...
Sent 30955484 bytes in 19.6 seconds
switch#
```

If there are no kernel corefiles, then the following information appears: No coredump found for kernel

```
switch# copy core-dump kernel tftp 10.0.12.161
No coredump found for kernel
switch#
```

3.22.4. Copy one instance of daemon corefile to sftp server

This command copies the daemon coredump to the destination sftp server. You can specify the destination filename. The destination filename is optional parameter. If you have not specified the file name, then it saves as a source file name.

Syntax copy core-dump <DAEMONNAME> instance-id <INSTANCE ID> sftp <USER-NAME> <SFTP SERVER IPV4/HOST NAME> [FILENAME]

Authority The root and netop users can copy corefiles to any external tftp or sftp server from the switch.

<daemon name> Daemon name

<instance id> Instance id of core file, 1-65535

<sftp server address> Host name of SFTP server

<user name> User name
<file name> Destination file name

Examples

```
switch#copy core-dump ops-vland instance-id 410 sftp naiksat 10.0.12.161
ops-vland.xz
copying ...
naiksat@10.0.12.161's password:
Connected to 10.0.12.161.
sftp> put /var/diagnostics/coredump/core.ops-vland.0.a6f6c4b58aa5467ba57d
7f9492afa10f.410.1461694139000000.xz ops-vland.xz
Uploading /var/diagnostics/coredump/core.ops-vland.0.a6f6c4b58aa5467ba57d7
f9492afa10f.410.1461694139000000.xz to /users/naiksat/ops-vland.xz
/var/diagnostics/coredump/core.ops-vland.0.a6 100% 106KB 106.5KB/s 00:00
switch#
```

If there are no core dumps to present, the following information appears:

```
copy core-dump ops-vland instance-id 410 sftp naiksat 10.0.12.161 ops-vland.xz
No coredump found for daemon ops-vland with instance 410
```

3.22.5. Copy all corefile instances for a daemon to a sftp server

This command copies all instance of a daemon coredump to the destination sftp server. You can specify the destination file name. If you have not specified the file name then it saves as a source file name.

Syntax	copy core-dump < DAEMON NAME> sftp <USERNAME> <SFTP SERVER ADDRESS> [DESTINATION FILE NAME]
Authority	The root and netop users can copy corefiles to any external tftp or sftp server from the switch.
<daemon name>	Daemon name
<instance id>	Instance id of core file, 1-65535
<sftp server address>	Host name of SFTP server
<file name>	Destination file name

Examples

```
switch# copy core-dump ops-switchd sftp naiksat 10.0.12.161
copying ...
The authenticity of host '10.0.12.161 (10.0.12.161)' can't be established.
ECDSA key fingerprint is SHA256:uWeyXm2j6VkJDfCitlyz/P+xGgZW9YYw5GnDOsEgVHeU.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.12.161' (ECDSA) to the list of known hosts.
```

```

naiksatsat@10.0.12.161's password:
Connected to 10.0.12.161.
sftp> put /var/diagnostics/coredump/core.ops-switchd.0.1bddabce7ee5468884cc
012b1d7c2ab0.361.1461694266000000.xz core.ops-switchd.0.1bddabce7ee5468884c
c012b1d7c2ab0.361.1461694266000000.xz
Uploading /var/diagnostics/coredump/core.ops-switchd.0.1bddabce7ee5468884cc
012b1d7c2ab0.361.1461694266000000.xz to /users/naiksatsat/core.ops-switchd.0.1
bddabce7ee5468884cc012b1d7c2ab0.361.1461694266000000.xz
/var/diagnostics/coredump/core.ops-switchd.0. 100% 4531KB 4.4MB/s 00:00
switch#

```

If there are no core dumps to present, the following information appears:

```

switch# copy core-dump ops-fand sftp naiksatsat 10.0.12.161
No coredump found for daemon ops-fand
switch#

```

3.22.6. Copy kernel corefile to sftp srver

This command copies the kernel corefile to the destination sftp server. You can specify the destination file name. If you have not specified a file name then it saves as a source file name.

Syntax copy core-dump kernel sftp <USERNAME> <SFTP SERVER IP> [DESTINATION FILE NAME]

Authority The root and netop users can copy corefiles to any external tftp or sftp server from the switch.

<sftp server address> Host name of SFTP server

<user name> User name

<file name> Destination file name

Examples

```

switch# copy core-dump kernel sftp naiksatsat 10.0.12.161 kernelcore.tar.gz
copying ...
naiksatsat@10.0.12.161's password:
Connected to 10.0.12.161.
sftp> put /var/diagnostics/coredump/kernel-core/vmcore.20160426.180420.tar.gz
kernelcore.tar.gz
Uploading /var/diagnostics/coredump/kernel-core/vmcore.20160426.180420.tar.gz
to /users/naiksatsat/kernelcore.tar.gz
/var/diagnostics/coredump/kernel-core/vmcore. 100% 44MB 43.5MB/s 00:01
switch#

```

If there are no core dumps to present, the following information appears: No coredump found for kernel

```

switch# copy core-dump kernel sftp naiksatsat 10.0.12.161 kernelcore.tar.gz
No coredump found for kernel
switch#

```

3.22.7. Copy coredump help string

```
switch# copy
  core-dump      Copy daemon or kernel coredump
  running-config Copy from current system running configuration
  sftp           Copy data from an SFTP server
  startup-config Copy from startup configuration
switch# copy core-dump
  DAEMON_NAME Specify daemon-name
  kernel       Copy kernel coredump
switch# copy core-dump ops-fand
  instance-id  Coredump instance ID
  sftp         Copy coredump to sftp server
  tftp         Copy coredump to tftp server
switch# copy core-dump ops-fand instance-id
  INSTANCE_ID Specify coredump instance ID
switch# copy core-dump ops-fand instance-id 123
  sftp Copy coredump to sftp server
  tftp Copy coredump to tftp server
switch# copy core-dump ops-fand instance-id 123 tftp
  A.B.C.D Specify server IP
  WORD     Specify server name
switch# copy core-dump ops-fand instance-id 123 tftp 1.2.3.4
  <cr>
  [FILE_NAME] Specify destination file name
switch# copy core-dump ops-fand instance-id 123 tftp 1.2.3.4 abc.xz
  <cr>
switch# copy core-dump ops-fand instance-id 123 tftp 1.2.3.4 ops-fand.xz
  <cr>
switch# copy core-dump ops-fand
  instance-id  Coredump instance ID
  sftp         Copy coredump to sftp server
  tftp         Copy coredump to tftp server
switch# copy core-dump ops-fand tftp
  A.B.C.D Specify server IP
  WORD     Specify server name
switch# copy core-dump ops-fand tftp 1.2.3.4
  <cr>
switch# copy core-dump kernel
  sftp Copy coredump to sftp server
  tftp Copy coredump to tftp server
switch# copy core-dump kernel tftp
  A.B.C.D Specify server IP
  WORD     Specify server name
switch# copy core-dump kernel tftp 1.2.3.4
  <cr>
  [FILENAME] Specify destination file name
switch# copy core-dump kernel tftp 1.2.3.4 kernel.tar.gz
  <cr>
switch# copy core-dump ops-fand
  instance-id  Coredump instance ID
```

```
sftp          Copy coredump to sftp server
tftp          Copy coredump to tftp server
switch# copy core-dump ops-fand instance-id 123
sftp          Copy coredump to sftp server
tftp          Copy coredump to tftp server
switch# copy core-dump ops-fand instance-id 123 sftp
USERNAME     Specify user name of sshd server
switch# copy core-dump ops-fand instance-id 123 sftp naiksat
A.B.C.D      Specify server IP
WORD         Specify server name
switch#
switch# copy core-dump ops-fand instance-id 123 sftp naiksat 1.2.3.4
<cr>
[FILE_NAME]  Specify destination file name
switch# copy core-dump ops-fand instance-id 123 sftp naiksat 1.2.3.4 ops-fand.tar.gz
```

```
switch# copy core-dump ops-fand
instance-id  Coredump instance ID
sftp          Copy coredump to sftp server
tftp          Copy coredump to tftp server
switch# copy core-dump ops-fand
instance-id  Coredump instance ID
sftp          Copy coredump to sftp server
tftp          Copy coredump to tftp server
switch# copy core-dump ops-fand
instance-id  Coredump instance ID
sftp          Copy coredump to sftp server
tftp          Copy coredump to tftp server
switch# copy core-dump ops-fand sftp
USERNAME     Specify user name of sshd server
switch# copy core-dump ops-fand sftp naiksat
A.B.C.D      Specify server IP
WORD         Specify server name
switch# copy core-dump ops-fand sftp naiksat 1.2.3.4
<cr>
switch# copy core-dump
DAEMON_NAME  Specify daemon-name
kernel       Copy kernel coredump
switch# copy core-dump kernel
sftp          Copy coredump to sftp server
tftp          Copy coredump to tftp server
switch# copy core-dump kernel sftp
USERNAME     Specify user name of sshd server
switch# copy core-dump kernel sftp naiksat
A.B.C.D      Specify server IP
WORD         Specify server name
switch# copy core-dump kernel sftp naiksat 1.2.3.4
<cr>
[FILENAME]  Specify destination file name
switch# copy core-dump kernel sftp naiksat 1.2.3.4 kernel.tar.gz
<cr>
```

3.22.8. show core dump

This command lists all the core dumps in the switch. Each entry in the listing displays the daemon name that crashed and the timestamp of the crash event.

Syntax show core-dump

Authority All users

Examples

```
switch# show core-dump
=====
TimeStamp          | Daemon Name
=====
2016-10-09 09:08:22  ops-lldpd
2015-09-12 10:34:56  kernel
=====
Total number of core dumps : 1
=====
```

If there are no core dumps to present, the following information appears:

```
switch# show core-dump
No core dumps are present
```

3.23. NTP Commands Reference

3.23.1. ntp server

Forms an association with an NTP server.

Syntax ntp server <name|ipv4-address> [key key-id] [prefer] [version version-number]

Syntax [no] ntp server <name|ipv4-address>

Authority Admin user.

<name> The name or IPV4 address of the server.

<key-id> The key used while communicating with the server, 1-65534.

<prefer> Request to make this the preferred NTP server.

<version-no> NTP version 3 or 4.

<no> Destroys a previously configured server. |

Examples

```
s1(config)#ntp server time.apple.com key 10 version 4
s1(config)#no ntp server 192.0.1.1
```

3.23.2. ntp authentication

Enables/disables the NTP authentication feature.

Syntax [no] ntp authentication enable

Authority Admin user.

<no> Disables the NTP authentication feature.

Examples

```
s1(config)#ntp authentication enable
s1(config)#no ntp authentication enable
```

3.23.3. ntp authentication-key

Defines the authentication key.

Syntax ntp authentication-key <key-id> md5 <password>

Syntax [no] ntp authentication-key <key-id>

Authority Admin user.

<key-id> The key used while communicating with the server, 1-65534.

<password> The MD5 password, 8-16 chars.

<no> Destroys the previously created NTP authentication key.

Examples

```
s1(config)#ntp authentication-key 10 md5 myPassword
s1(config)#no ntp authentication-key 10
```

3.23.4. ntp trusted-key

Marks a previously defined authentication key as trusted. If NTP authentication is enabled, the device synchronizes with a time source only if the server carries one of the authentication keys specified as a trusted key.

Syntax [no] ntp trusted-key <key-id>
Authority Admin user.
 <key-id> The key used while communicating with the server, 1-65534.
 <no> Destroys the previously created NTP authentication key.

Examples

```
s1(config)#ntp trusted-key 10
s1(config)#no ntp trusted-key 10
```

3.23.5. show ntp associations

Displays the status of connections to NTP servers.

Syntax show ntp associations
Authority Admin user.

Examples

```
s1(config)#show ntp associations
```

```
-----
  ID           NAME           REMOTE  VER  KEYID
  -----
  1           192.0.1.1       192.0.1.1  3    -
  * 2    time.apple.com  17.253.2.253  4    10
  -----
```

```
-----
REF-ID  ST  T  LAST  POLL  REACH  DELAY  OFFSET  JITTER
  -----
.INIT.  -  -  -     -     -     -     -     -
.GPSs.  2  U  10    64    0  0.121  0.994  0.001
  -----
```

Key

```
code      : Tally code (Explained later)
ID        : Server number
NAME      : NTP server FQDN/IPV4 address (only the first 15 characters
of the name are displayed)
REMOTE    : Remote server IP address
```

```
VER          : NTP version (3 or 4)
KEYID       : Key used to communicate with this server
REF_ID      : Reference ID for the remote server (Can be an IP address)
Stratum (ST) : Number of hops between the client and the reference clock.
TYPE (T)    : Transmission Type - U Unicast/manycast; B Broadcast; M
Multicast; L Local; b bcast/mcast; S Symm_peer; m manycast
LAST        : Poll interval since the last packet was received (seconds
unless unit is provided).
POLL        : Interval (in seconds) between NTP poll packets. Maximum
(1024) reached as server and client syncs.
REACH       : Octal number that displays status of last eight NTP messages
(377 - all messages received).
DELAY       : Round trip delay (in milliseconds) of packets to the selected
reference clock.
OFFSET      : Provides Root Mean Square time (in milliseconds) between this
local host and the remote peer or server.
JITTER      : Maximum error (in milliseconds) of local clock relative to the
reference clock.
```

Key for the Tally code

This field displays the current selection status.

```
 : Discarded as not valid
x : Discarded by intersection algorithm
. : Discarded by table overflow (not used)
- : Discarded by the cluster algorithm
+ : Included by the combine algorithm
# : Backup (more than tos maxclock sources)
* : System peer
o : PPS peer (when the prefer peer is valid)
```

3.23.6. show ntp status

SyntaDisplays the status of NTP on the switch; whether NTP is enabled/disabled and if it has been synchronized with a server.x

Syntax show ntp status

Authority Admin user.

Examples

When the system has not been synced:

```
s1(config)#show ntp status
NTP is enabled.
NTP authentication is enabled.
```

When the system has been synced to a NTP server:

```
s1(config)#show ntp status
NTP is enabled.
```

```
NTP authentication is enabled.  
Uptime: 200 seconds  
Synchronized to NTP Server 17.253.2.253 at stratum 2.  
Poll interval = 1024 seconds.  
Time accuracy is within 0.994 seconds  
Reference time: Thu Jan 28 2016 0:57:06.647 (UTC)
```

3.23.7. show ntp authentication-keys

Displays the NTP authentication keys.

Syntax show ntp authentication-keys

Authority Admin user.

Examples

```
s1(config)#show ntp authentication-keys  
-----  
Auth key          MD5 password  
-----  
10                MyPassword
```

3.23.8. show ntp trusted-keys

Displays the NTP trusted keys.

Syntax show ntp trusted-keys

Authority Admin user.

Examples

```
s1(config)#show ntp trusted-keys  
-----  
Trusted keys  
-----  
10  
50  
-----
```

3.23.9. show ntp statistics

Displays the global NTP statistics.

Syntax show ntp statistics

Authority Admin user.

Examples

```
s1(config)#show ntp statistics  
Rx-pkts          100
```

```
Rx cur ver      80
Rx old ver      20
Err-pkts        2
Auth-failed-pkts 1
Declined-pkts   0
Restricted-pkts 0
Rate-limited-pkts 0
KoD-pkts        0
```

Legend:

Rx-pkts: Total NTP packets received.
Cur Ver Rx-pkts: Number of NTP packets that match the current NTP version.
Old Ver Rx-pkts: Number of NTP packets that match the previous NTP version.
Error pkts: Packets dropped due to all other error reasons.
Auth-failed pkts: Packets dropped due to authentication failure.
Declined pkts: Packets denied access for any reason.
Restricted pkts: Packets dropped due to NTP access control.
Rate-limited pkts: Number of packets discarded due to rate limitation.
KOD pkts: Number of Kiss of Death packets sent.

For general NTP debugging information, see <http://doc.ntp.org/4.2.6p5/debug.html>. <http://doc.ntp.org/4.2.8p8/monopt.html>.



Because ntpq sends query messages to ntpd for fetching status information. Rx-pkts field may show a non-zero packet count, even when ntp association is not configured on the switch.

3.24. Mirror Commands

Overview

The port mirroring feature enables traffic on one or more switch interfaces to be replicated on another interface.

Mirror session

A mirror session defines the settings for the replication of data between one or more source interfaces and a destination interface.

A maximum of four mirror sessions can be active at the same time on the switch. There is no limit on the number of inactive sessions that can be defined in the configuration.

Each mirror session has a single output, or *destination* interface, and zero or more input, or *source* interfaces. The destination interface is the recipient of all mirrored traffic, and must be able to support the combined data rate of all source interfaces. Source interfaces can be configured to mirror received traffic, transmitted traffic, or all traffic.

Source and destination interfaces do not need to reside in the same subnet, VLAN or VRF.

A LAG can be specified as either a source or destination interface. The switch internally handles the mirroring of the traffic appropriately across all the LAG member interfaces.

Mirroring is VRF agnostic. That is, a network administrator may choose to specify source interfaces from different VRFs in the same mirror session and have a single destination for the mirrored traffic.

Mirror rules

The following rules apply when creating a mirror session:

1. An interface cannot be both a source and destination in the same mirror session.
2. The destination interface in an **active** mirror session cannot be the source or destination in another **active** mirror session.
3. The source interface in an **active** mirror session cannot be the destination in another **active** mirror session.
4. The destination interface cannot be a member of a VLAN nor have an IP address configured.
5. The destination interface cannot have the spanning tree protocol enabled on it.



If you try to activate a mirror session that violates rules 2 or 3 it will remain shutdown.



The same interface can be the source in more than one mirror session as long as it does not violate rule 1 or 3.

3.24.1. mirror session

Changes to mirror session mode for the specified session name. If the session name does not exist, it is created.

Use the no form of this command to remove a mirror session.

Syntax	[no] mirror session <name>
Command mode	Configuration mode (config).
Authority	All users.
<name>	Name of a session. Up to 64 letters, numbers, underscores, dashes, or periods.

Example

Creating a new mirror session named Mirror_3

```
switch(config)# mirror session Mirror_3
switch(config-mirror)#
```

3.24.2. destination

The **destination interface** command assigns the specified Ethernet interface or LAG where all mirror traffic for this session will be transmitted. Only one destination interface is allowed per session.

The interface must already be an interface defined in the switch configuration. Interface activation is not necessary for addition to a mirror session.

Entering another destination interface will cause all mirror traffic to use the interface. This may cause a temporary suspension of mirror traffic from the source(s) during the reconfiguration.

The **no destination interface** command will cease the use of the interface and deactivate (shut-down) the session.

Special requirements for destination interfaces

To be qualified as a mirror session destination, the interface:

- Must not already be a source or destination in any other active mirror session
- Must not be participating in any form of Spanning Tree protocol
- Must not be a member of a VLAN nor have an IP address configured.



An interface will be automatically removed from a mirror session in these two circumstances:

- the interface becomes a member of a LAG
- the interface route mode is changed (i.e. 'routing' or 'no routing')

If the interface removed is a mirror destination, then the mirror session is automatically de-activated (i.e. 'no shutdown').

The interface/LAG must then be re-added to the mirror session and the session reactivated.

Syntax [no] destination interface <interface>
Command mode Mirror session mode (config-mirror).
Authority All users.
<interface> Name of a an interface.

Example

Setting interface 10 as the destination for the session Mirror_3

```
switch(config)# mirror session Mirror_3  
switch(config-mirror)# destination interface 10
```

Removing interface 10 as the destination for the session Mirror_3

```
switch(config)# mirror session Mirror_3  
switch(config-mirror)# no destination interface
```

3.24.3. shutdown

Deactivates a mirror session. By default, mirror sessions are inactive.

Use the **no** form of this command to activate a mirror session.

Syntax [no] shutdown
Command mode Mirror session mode (config-mirror).
Authority All users.

Examples

Activating mirror session Mirror_3

```
switch(config)# mirror session Mirror_3  
switch(config-mirror)# no shutdown
```

3.24.4. source

The **source interface** command adds, modifies, or removes the specified Ethernet interface or LAG as a mirror source. When adding or modifying a source port, the mirror traffic direction must be specified:

- both - traffic received and transmitted
- rx only received traffic
- tx only transmitted traffic

A source interface must already be an interface defined in the switch configuration. Interface activation is not necessary for addition to a mirror session.

More than one source interface can be configured in a mirror session, each with their own direction.

To change the direction of a source interface, re-enter the **source interface** command again with the new direction.

There may be a temporary suspension of mirrored traffic when adding sources or changing source directions.

The **no source** command will cease mirroring traffic from the source interface.

Special requirements for mirror source interfaces

To be qualified as a mirror session source, the interface must:

- Not already be a destination in any mirror session



An interface will be automatically removed from a mirror session in these two circumstances:

- the interface becomes a member of a LAG
- the interface route mode is changed (i.e. 'routing' or 'no routing')

The interface/LAG must then be re-added to the mirror session.

Syntax source interface <INTERFACE> {both|rx|tx}

Syntax no source interface <INTERFACE>

Command mode Mirror session mode (config-mirror).

Authority All users.

<INTER-
FACE> Ethernet interface or LAG

Examples

```
switch# configure terminal
switch(config)# mirror session Mirror_3
switch(config-mirror)# source interface 5 both
```

3.24.5. show mirror

The **show mirror** command will display the list of all configured mirror sessions and their status.

With a **NAME** parameter, this command will display the details of the single named mirror session.

Syntax show mirror [<NAME>]

Authority All users.
<NAME> Display the details of that mirror session

Examples

```
switch# show mirror
name                                     status
-----
My_Session_1                             active
Other-Session-2                           shutdown
```

```
switch# show mirror My_Session_1
Mirror Session: My_Session_1
Status: active
Source: interface 2 both
Source: interface 3 rx
Destination: interface 1
Output Packets: 123456789
Output Bytes: 8912345678
```

3.25. CLI support for Autoprovisioning

The feature is enabled by default and cannot be turned off through CLI. To disable the autoprovisioning feature, configure the DHCP server to NOT send option 239 in the DHCP reply/ack messages.

3.25.1. autoprovisioning

This command forces manual autoprovisioning.

Syntax autoprovisioning manual
Authority Admin

3.25.2. show autoprovisioning

This command displays the autoprovision status. If autoprovision has been performed, the script URL is displayed. See the following examples for expected output.

Syntax show autoprovisioning
Authority Admin

Examples

If autoprovision is performed

```
switch # show autoprovisioning
Performed : Yes
URL : http://192.168.1.1/autoprovision.sh
```

If autoprovision is not performed

```
switch # show autoprovisioning
Performed : No
```

3.26. System commands

3.26.1. Setting the fan speed

This command globally sets the fan speed to the value indicated by the command parameter. This command overrides the fan speed set internally by the platform. The fan speed value set by the user takes affect depending on platform cooling requirements.

By default fans operate at normal speed.

Syntax	[no] fan-speed < normal medium fast maximum >
Authority	All users.
<no>	Removes the configured fan speed, and sets it to the default speed.
<normal>	Normal is 40% of maximum speed.
<medium>	Medium is 65% of maximum speed.
<fast>	Fast is 80% of maximum speed.
<max>	Fan speed is at maximum speed.

Examples

```
switch(config)#fan-speed slow
```

3.26.2. Setting an LED state

This command sets the LED state to on, off, or flashing. By default, the LED state is off.

Syntax	[no] led < led-name > < on flashing off >
Authority	All users.
<no>	Turns off the LED.
<led-name>	LED name of whose state is to be set
<off>	Select this to switch off LED
<on>	Select this to switch on LED
<flashing>	Select this to blink/flash the LED

Examples

```
switch(config)#led base-loc on
```

3.26.3. Showing version information

This command shows the current switch version information. The format of the show version output:

```
<name> <version> (Build: <platform>-ops-<X.Y.Z-string>-<branch-name>
[-<build-time>][-<meta-string>]
```

Syntax	show version
---------------	--------------

Authority All users.

Field Name	Explanation
name	Name of the project.
version	Version of the software.
platform	Platform for which the image is built.
ops	Abbreviation for OpenSwitch.
X.Y.Z-string	The release version tag.
branch-name	Branch where the image is built.
build-time	For periodic builds, the build time-stamp in YYYYMMDDNN format. For developer builds, the build time-stamp in YYYYMMDDHHmmss format.
meta-string	“dev” is appended to image names when a developer builds an image using “make”.

Examples

```
switch# show version
FOXOSS 2.0.0 (Build: foxoss-ops-2.0.0-Poblano-20180308014408-dev)
```

3.26.4. Showing package information

This command lists every package present in the switch image under the PACKAGE column. The VERSION column displays the git hash value if the SOURCE URL is a git repository. If not, the VERSION column displays the version string of the package. SOURCE TYPE displays the type of source pointed to by SOURCE URL. SOURCE URL displays the download location for the source-code of the corresponding package in the SOURCE URI column. If version information and/or Source URL is not available during build-time, show version detail displays NA (Not Available).

Syntax show version detail [ops]

Authority All users.

<ops> Displays git-hashes for OpenSwitch repos (ops-*) alone.

Examples

```
switch# show version detail
PACKAGE      : libz1
VERSION      : NA
SOURCE TYPE  : other
SOURCE URL   : NA
```

```
PACKAGE      : libjemalloc-dbg
VERSION      : NA
SOURCE TYPE  : other
SOURCE URL   : NA
```

```
PACKAGE      : lttng-tools
VERSION      : d522c1f14285e2e8b10b7c0cd011847696ffe779
```

```
SOURCE TYPE : git
SOURCE URL  : https://git.lttng.org/lttng-tools.git;branch=stable-2.6
```

```
PACKAGE      : libe2p2
VERSION      : NA
SOURCE TYPE  : other
SOURCE URL   : NA
```

```
PACKAGE      : busybox
VERSION      : 1.23.2
SOURCE TYPE  : http
SOURCE URL   : http://www.busybox.net/downloads/busybox-1.23.2.tar.bz2
```

3.26.5. Setting timezone on the switch

This command sets the time zone on the switch. By default the time zone is set to UTC (Coordinated Universal Time).

Syntax [no] timezone set **TIMEZONE**

Authority All users.

<no> Removes the configured time zone, and sets it to the default UTC time zone.

<TIME-ZONE> The parameter should follow values as per the POSIX timezone database.

Examples

```
switch(config)# timezone set us/alaska
switch(config)#no timezone set us/alaska
```

3.26.6. Showing system information

Using no parameters, this command shows the overall system details, including information about physical components such as the fan, temperature sensor, LED, and power supply. Using a parameter, this command gives detailed information of various physical components.

Syntax show system [< fan | temperature [detail] | led | power-supply >]

Authority All users.

<fan> Displays fan information.

<temperature> Displays temperature-sensor information.

<led> Displays LED information.

<power-supply> Displays power-supply information.

<detail> Displays detailed temperature-sensor information.

Examples

```
switch# show system
OpenSwitch Version : 2.0.0 (Build: foxoss-ops-2.0.0-Poblano-20180308014408)
```

Management And Utility Commands

```
-dev)
Product Name       : Aurora 720

Vendor            : Netberg
Platform          : x86_64-huracan_rangeley-r0
Manufacturer      : Netberg
Manufacturer Date  : 04/11/2016 14:35:24

Serial Number     : 2M3AR000129          Label Revision      :

ONIE Version      : 2015.11             DIAG Version        : DIAG_HURACAN
_1.3.7
Base MAC Address  : 70:b3:d5:cc:f0:47    Number of MACs      : 1067
Interface Count   : 160                 Max Interface Speed : 100000Mbps
```

Fan details:

Name	Speed	Status
base-1B	normal	ok
base-1F	normal	ok
base-2B	normal	ok
base-2F	normal	ok
base-3B	normal	ok
base-3F	normal	ok
base-4B	normal	ok
base-4F	normal	ok

LED details:

Name	State	Status
base-psu1	on	ok
base-psu2	flashing	ok
base-stat	on	ok
base-fan	on	ok

Power supply details:

Name	Status
base-psu1	OK
base-psu2	Input Fault

Temperature Sensors:

Location	Name	Reading(celsius)
CPU core 0	base-4	30.00
CPU core 3	base-7	31.00
Embedded Switch Chip Sensors	base-3	50.00
Close to the front of MAC	base-1	34.04
CPU core 2	base-6	31.00
Close to the rear of MAC	base-2	37.00

CPU core 1 base-5 30.00

3.26.7. System fan information

This command displays detailed fan information.

Syntax show system fan

Authority All users

Example

```
switch#show system fan
Fan information
-----
Name           Speed  Direction      Status      RPM
-----
base-3F        normal front-to-back  ok          5400
base-1F        normal front-to-back  ok          5273
base-4F        normal front-to-back  ok          5335
base-2F        normal front-to-back  ok          5357
base-2B        normal front-to-back  ok          4368
base-3B        normal front-to-back  ok          4500
base-4B        normal front-to-back  ok          4383
base-1B        normal front-to-back  ok          4470
-----
Fan speed override is set to : normal
-----
```

3.26.8. Showing system temperature information

This command displays detailed temperature sensor information. If a parameter is not used, the command displays minimal temperature information.

Syntax show system temperature [detail]

Authority All users

<detail> Displays detailed temperature-sensor information.

Example

```
switch# show system temperature
Temperature information
-----
Name           Current      Status      Fan state
temperature    (in C)
-----
base-4         32.00        normal      normal
base-7         31.00        normal      normal
base-3         50.00        normal      normal
base-1         34.04        normal      normal
```

```
base-6    32.00      normal      normal
base-2    37.00      normal      normal
base-5    32.00      normal      normal
```

```
switch# show system temperature detail
Detailed temperature information
```

```
-----
Name                :base-4
Location             :CPU core 0
Status               :normal
Fan-state            :normal
Current temperature(in C) :30.00
Minimum temperature(in C) :25.00
Maximum temperature(in C) :34.00
```

```
Name                :base-7
Location             :CPU core 3
Status               :normal
Fan-state            :normal
Current temperature(in C) :31.00
Minimum temperature(in C) :26.00
Maximum temperature(in C) :35.00
```

```
Name                :base-3
Location             :Embedded Switch Chip Sensors
Status               :normal
Fan-state            :normal
Current temperature(in C) :50.00
Minimum temperature(in C) :0.00
Maximum temperature(in C) :51.00
```

3.26.9. Showing system LED information

This command displays detailed LED information.

Syntax show system led

Authority All users

Example

```
switch# show system led
Name          State      Status
-----
base-psu1     on        ok
base-psu2     flashing  ok
base-stat     on        ok
base-fan      on        ok
```

3.26.10. Showing system power-supply information

This command displays detailed power-supply information.

Syntax show system power-supply
Authority All users

Example

```
switch#show system power-supply
Name           Status
-----
base-psu1      OK
base-psu2      Input Fault
```

3.26.11. Showing system date information

This command displays system date information. It shows system time in <Day> <Mon> <Date> <hh:mm:ss> <timezone> <year> format.

Syntax show date
Authority All users

Example

```
switch# show date
Wed Jun 22 18:39:48 UTC 2016
switch#
```

3.26.12. Showing system CPU information using top

This command displays detailed CPU information sorted by CPU usage.

Syntax top cpu
Authority All users

Example

```
switch# top cpu
top - 11:30:07 up 4:52, 1 user, load average: 0.04, 0.08, 0.12
Tasks: 141 total, 1 running, 139 sleeping, 0 stopped, 1 zombie
%Cpu(s): 1.2 us, 0.5 sy, 0.0 ni, 98.3 id, 0.0 wa, 0.0 hi, 0.1 si, 0.0 st
KiB Mem : 8016188 total, 6724796 free, 1096244 used, 195148 buff/cache
KiB Swap: 0 total, 0 free, 0 used. 6725144 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
1	root	20	0	29996	4644	3488	S	0.0	0.0	0:00.19	/sbin/init
16	root	20	0	23352	5796	5524	S	0.0	0.1	0:00.34	/lib/systemd/systeme
65	root	20	0	32452	2924	2492	S	0.0	0.0	0:00.02	/lib/systemd/systeme
138	systemd+	20	0	18276	2688	2484	S	0.0	0.0	0:00.00	/lib/systemd/systeme
142	root	20	0	259676	2936	2588	S	0.0	0.0	0:00.06	/usr/sbin/rsyslogd
150	message+	20	0	13180	2496	2272	S	0.0	0.0	0:00.00	/usr/bin/dbus-daem
151	root	20	0	13108	2352	2144	S	0.0	0.0	0:00.00	/lib/systemd/systeme
153	root	20	0	15712	2216	1652	S	0.0	0.0	0:00.00	/usr/sbin/crond -n

3.26.13. Showing system memory information using top

This command displays detailed memory information sorted by memory usage.

Syntax top memory

Authority All users

Example

```
switch# top memory
top - 11:31:28 up 4:53, 1 user, load average: 0.28, 0.15, 0.14
Tasks: 141 total, 1 running, 139 sleeping, 0 stopped, 1 zombie
%Cpu(s): 1.2 us, 0.5 sy, 0.0 ni, 98.3 id, 0.0 wa, 0.0 hi, 0.1 si, 0.0 st
KiB Mem : 8016188 total, 6724432 free, 1096560 used, 195196 buff/cache
KiB Swap: 0 total, 0 free, 0 used. 6724784 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
321	root	20	0	161984	38516	8848	S	0.0	0.4	0:02.75	python /usr/bin/re
236	root	20	0	182212	18520	7176	S	0.0	0.2	0:00.81	python /usr/bin/op
253	root	20	0	101828	18052	7108	S	0.0	0.2	0:00.29	python /usr/bin/op
312	root	20	0	112496	17312	3992	S	0.0	0.2	0:00.07	python /usr/bin/op
405	root	20	0	109908	16208	3344	S	0.0	0.2	0:00.66	python /usr/bin/op
313	root	20	0	101564	14008	3244	S	0.0	0.1	0:00.00	python /usr/bin/op
188	root	20	0	40288	13300	4636	S	0.0	0.1	0:00.35	/usr/sbin/ovsdb-se

3.26.14. Showing time zone information

This command displays detailed information for the time zone configured on the system.

Syntax show system timezone

Authority All users

Example

By default the time zone configured is UTC:

```
switch# show system timezone
System is configured for timezone : UTC
DST active: n/a
```

If the time zone is configured for "US/Alaska", then it may be verified using the show system time-zone command:

```
switch# show system timezone
System is configured for timezone : US/Alaska
DST active: yes
Last DST change: DST began at
Sun 2016-03-13 01:59:59 AKST
Sun 2016-03-13 03:00:00 AKDT
```

Management And Utility Commands

```
Next DST change: DST ends (the clock jumps one hour backwards) at
Sun 2016-11-06 01:59:59 AKDT
Sun 2016-11-06 01:00:00 AKST
```

3.27. Secure Shell Commands

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

3.27.1. password-authentication

Enable password authentication method.

The no form disables password authentication method.

Syntax [no] ssh password-authentication

Authority Admin

3.27.2. public-key-authentication

Enable publickey authentication method

The no form disables publickey authentication method.

Syntax [no] ssh public-key-authentication

Authority Admin

3.28. Control Plane Policing

Control plane policing (CoPP) in OpenSwitch is used to prioritize traffic handling by the CPU, and to protect the switch from DoS attacks.

NOTE:

- If a packet class is not supported on the switch, then all status and statistics values for that class will be empty.
- Statistics that are not supported for a packet class will be empty.

3.28.1. show copp statistics

Displays control plane policing (CoPP) statistics for all protocols, or a specific protocol.

Syntax show copp statistics [<protocol-name>]

Authority Operator.

<proto- Name of a protocol for which to retrieve CoPP statistics. To see a list of all supported-
col-name> ed protocol names, use the command: show copp statistics ?

Example

```
switch# sh copp statistics acl-logging
Control Plane Packet: ACL LOGGING packets
```

```
rate (pps):          5
burst size (pkts):   5
local_priority:      0
```

```
packets_passed:      5          bytes_passed:      320
packets_dropped:     5          bytes_dropped:     320
```

```
switch# sh copp statistics
Control Plane Packets Total Statistics
```

```
total_packets_passed: 5500    total_bytes_passed: 352000
total_packets_dropped: 5500    total_bytes_dropped: 352000
```

```
Control Plane Packet: BGP packets
```

```
rate (pps):          5000
burst size (pkts):   5000
local_priority:      9
```

```
packets_passed:      5000    bytes_passed:      320000
packets_dropped:     5000    bytes_dropped:     320000
```

```
Control Plane Packet: LLDP packets
```

```
rate (pps):          500
burst size (pkts):   500
```

Management And Utility Commands

local_priority:	8		
packets_passed:	500	bytes_passed:	32000
packets_dropped:	500	bytes_dropped:	32000

3.29. CLI support for Config Persistence

3.29.1. Copy startup configuration to running configuration

The **copy startup-config running-config** command is used to save the configuration in the persistent database to the current configuration of the switch. This can be used as a rollback to the original configuration, if the modified configurations have to be discarded.

Syntax copy startup-config running-config

Authority Admin

Examples

```
switch # copy startup-config running-config
```

3.29.2. Copy running configuration to startup configuration

The **copy running-config startup-config** command is used to save the current configuration of the switch to the persistent configuration database. The saved configuration is used as the startup configuration on the next boot up.

Syntax copy running-config startup-config

Authority Admin

Examples

```
switch # copy running-config startup-config
```

3.29.3. Show startup configuration

This command displays the saved startup configuration in CLI command format

Syntax show startup-config

Authority Admin

Examples

```
switch # show startup-config
Startup configuration:
!
radius-server host 1.2.3.4 key testRadius
radius-server host 1.2.3.4 auth_port 2015
radius-server retries 5
radius-server timeout 10
!
```

3.30. Logrotate Commands

3.30.1. logrotate period

This command configures the rotation of log files based on time. The possible values are hourly, weekly or monthly. When the time difference between the last rotation of a log file and current time exceeds the configured value, the log rotation is triggered for that particular file. To reset the log rotation to the default value of daily, use the no form of the command (no logrotate period (hourly | weekly | monthly)).

If no parameter is specified, the default value of daily is used.

Syntax	logrotate period (hourly weekly monthly)
Authority	All users
<hourly>	Rotates log files every hour.
<monthly>	Rotates log files every month.
<weekly>	Rotates log files every week.

Examples

```
switch(config)# logrotate period weekly
```

3.30.2. logrotate maxsize

This command configures the log rotation based on log file size. The log file size is checked hourly. When the size of the log file exceeds the configured value, the rotation is triggered for that particular log file. To reset the default value of 10 MB, use the no form of the command (no logrotate maxsize **filesize**).

Syntax	logrotate maxsize <filesize>
Authority	All users
<filesize>	File size in Mega Bytes (MB), 1-200. Default value is 10MB

Examples

```
switch(config)# logrotate maxsize 20
```

3.30.3. logrotate target

This command sends the rotated log files to a specified remote host Universal Resource Identifier (URI) by using the tftp protocol. If no URI is specified, the rotated and compressed log files are stored locally in the /var/log/ path. To prevent rotated logs from being sent to a remote host, use the no form of the command (no logrotate target **URI**).

This parameter specifies the URI of the remote host. The possible values are tftp://A.B.C.D' or 'tftp://X:X::X:X. Both IPv4 and IPv6 addresses are supported.

Syntax	logrotate target <URI>
---------------	------------------------

Authority All users
<URI> URI of the remote host.

Examples

```
switch(config)# logrotate target tftp://192.168.1.132  
switch(config)# logrotate target tftp://2001:db8:0:1::128
```

3.30.4. show logrotate

This command displays configuration parameters for the logrotate commands.

Syntax show logrotate
Authority All users

Examples

```
h1# show logrotate  
Logrotate configurations :  
Period : weekly  
Maxsize : 20MB  
Target : tftp://2001:db8:0:1::128
```

3.31. Show Tech Commands

3.31.1. show tech

Displays detailed information about the switch by automatically running the collection of show commands associated with switch features. The show commands associated with a feature are defined in the show tech configuration file (ops-supportability/conf/ops_showtech.yaml).

Syntax show tech

Authority All users

Examples

This example shows a truncated version of the information returned by the show tech command. The system feature results in the running of three show commands: show version, show system, and show vlan.

```
switch# show tech
=====
Show Tech executed on Wed Mar 14 06:56:56 2018
=====
[Begin] Feature basic
=====
*****
Command : show version
*****
FOXOSS 2.0.0 (Build: foxoss-ops-2.0.0-Poblano-20180308014408-dev)

*****
Command : show system
*****
OpenSwitch Version : 2.0.0 (Build: foxoss-ops-2.0.0-Poblano-20180308014408-dev)
Product Name       : Aurora 720

Vendor             : Netberg
Platform           : x86_64-huracan_rangeley-r0
Manufacturer       : Netberg
Manufacturer Date  : 04/11/2016 14:35:24

Serial Number      : 2M3AR000129          Label Revision      :

ONIE Version       : 2015.11             DIAG Version         : DIAG_HURACAN_1.3.7
Base MAC Address   : 70:b3:d5:cc:f0:47       Number of MACs       : 4
Interface Count    : 160                 Max Interface Speed  : 100000Mbps

Fan details:

Name              Speed      Status
-----
base-1B           normal    ok
```

```
base-1F      normal    ok
base-2B      normal    ok
base-2F      normal    ok
base-3B      normal    ok
base-3F      normal    ok
base-4B      normal    ok
base-4F      normal    ok
```

LED details:

```
Name        State      Status
-----
base-psu1   on         ok
base-fan    on         ok
base-psu2   flashing   ok
base-stat   on         ok
```

Power supply details:

```
Name        Status
-----
base-psu1    OK
base-psu2    Input Fault
```

3.31.2. show tech list

Lists all features that are supported by the show tech command.

Syntax show tech list

Authority All users

Examples

```
switch# show tech list
Show Tech Supported Features List
-----
Feature                               Desc
-----
basic                                  Show Tech Basic
ntp                                    Network Time Protocol
lldp                                   Link Layer Discovery Protocol
lag                                    Link Aggregation Protocol
qos                                    Quality of Service
acl                                    Access Control Lists
ecmp                                   IP ECMP Load Balancing
mstp                                   Multiple Spanning Tree Protocol
sflow                                  sFlow
version                                Image versioning scheme
ospfv2                                 Open Shortest Path First version 2 Protocol
ucast-routing                          Unicast Routing Information
copp                                    Control Plane Policing
dhcp-server                             Dynamic Host Configuration Protocol Server
tftp-server                             Trivial File Transfer Protocol Server
```

snmp	SNMP
sftp-server	SSH File Transfer Protocol Server
source-interface-selection	Source Interface Selection
loopback	Loopback Interface
aaa	Authentication Authorization and Accounting
vlan	Virtual Local Area Network
ztp	Zero Touch Provisioning

3.31.3. show tech feature

Runs all show commands that are defined for the specified feature.

- Syntax** show tech <feature>
Authority All users
<feature> Feature name as displayed by the show tech list command.

Examples

```
switch# show tech sflow
=====
Show Tech executed on Wed Mar 14 07:02:16 2018
=====
[Begin] Feature sflow
=====
*****
Command : show sflow
*****
sFlow not yet configured.
=====
[End] Feature sflow
=====

=====
Show Tech commands executed successfully
=====
```

3.31.4. Show tech to file

Saves the output of the show tech command to a file.

- Syntax** show tech [<feature>] localfile <filename> [force]
Authority All users
<feature> Feature name as displayed by the show tech list command.
<filename> Name of the file where output of the command is saved. If the specified file already exists, it is not overwritten.
<force> If the specified output file exists, it is overwritten.

Examples

```
switch# show tech basic localfile stbasic.sta  
Show Tech output stored in file /tmp/stbasic.sta
```

```
switch# show tech basic localfile stbasic.sta  
/tmp/stbasic.sta already exists, please give different name or use force  
option to overwrite existing file
```

```
switch# show tech basic localfile stbasic.sta force  
Show Tech output stored in file /tmp/stbasic.sta
```

3.32. Show Vlog Commands

Command	Usage
show vlog	Displays vlog messages of ops daemons.
show vlog daemon (daemon_name)	Displays the vlog messages of the corresponding ops-daemon only.
show vlog severity (severity_level)	Displays the vlog messages of the corresponding severity level and above.
show vlog config list	Displays a list of supported features and descriptions.
show vlog config feature (feature_Name)	Displays the feature configuration log level of syslog and file destinations.
show vlog config daemon (daemon_Name)	Displays the daemon configuration log level of syslog and file destinations.
show vlog config	Displays a list of supported features' corresponding daemons logging levels of file and console destinations.
show vlog daemon (daemon_name) severity (severity_level)	Displays vlogs for the specified ops-daemon with the specified severity level and above.
show vlog severity (severity_level) daemon (daemon_name)	Displays vlogs for the specified severity level and above with ops-daemon only.

3.32.1. Show vlog

Displays vlog messages of ops daemons.

Syntax show vlog

Authority All users

3.32.2. Show vlog daemon

Displays only the corresponding ops daemon vlog messages.

Syntax show vlog daemon <daemon_name>

Authority All users

<daemon_name> Name of the ops daemon.

3.32.3. Show vlog severity

Displays corresponding severity level and above vlog messages.

Syntax show vlog severity <emer/err/warn/info/debug>

Authority All users

<emer>	Emergency logs only.
<err>	Error and above severity logs.
<warn>	Warning and above severity logs.
<info>	Information and above severity logs.
<debug>	All logs.

3.32.4. Show vlog config list

Lists all vlog supported features and descriptions.

Syntax	show vlog config list
Authority	All users

3.32.5. Show vlog config feature

Displays the feature configuration log levels of file and syslog destinations.

Syntax	show vlog config feature <feature_name>
Authority	All users
<feature_name>	Name of the feature.

3.32.6. Show vlog config daemon

Displays the ops-daemon configuration log levels of file and syslog destinations.

Syntax	show vlog config daemon <daemon_name>
Authority	All users
<daemon_name>	Name of the ops daemon.

3.32.7. Show vlog config

Lists all supported features and corresponding daemons logging levels of file and syslog destinations.

Syntax	show vlog config
Authority	All users

3.32.8. Show vlog daemon (daemon_name) severity (severity_level)

Displays vlogs for the specified ops-daemon only with specified severity level and above.

Syntax	show vlog daemon <daemon_name> severity <severity_level>
---------------	--

Authority All users

<daemon_name> Name of the ops daemon.

<severity_level> Severity log level (emer/err/warn/info/dbg).

Examples

```
switch# show vlog
```

```
show vlog
```

```
-----
ovsdb-server          | ovs | 00001 | ovsdb_server | INFO | ovsdb-server (Open vSwitch) 2.5
ops-arpmgrd           | ovs | 00001 | arpmgrd     | INFO | ops-arpmgrd (OpenSwitch arpmgrd) 2.5
ops-arpmgrd           | ovs | 00002 | reconnect   | INFO | unix:/var/run/openvswitch/db.sock:
ops-arpmgrd           | ovs | 00003 | reconnect   | INFO | unix:/var/run/openvswitch/db.sock:
ops-arpmgrd           | ovs | 00004 | ovsdb_idl   | INFO | DEBUG first row is missing from ta
ops-intfd             | ovs | 00001 | ops_intfd   | INFO | ops-intfd (OpenSwitch Interface Da
.....
```

```
switch# show vlog daemon ops-lldpd
```

```
show vlog
```

```
ovs|00001|lldpd_ovsdb_if|INFO|ops-lldpd (OPENSWITCH LLDPD Daemon) started
```

```
switch# show vlog severity warn
```

```
show vlog
```

```
-----
ops-sysd              | ovs | 00005 | ovsdb_if    | ERR  | Failed to commit the transaction. rc = 7
ops-pmd               | ovs | 00007 | timeval     | WARN | Unreasonably long 2802ms poll interval (
ops-pmd               | ovs | 00008 | timeval     | WARN | faults: 590 minor, 0 major
ops-pmd               | ovs | 00009 | timeval     | WARN | context switches: 637 voluntary, 70 invo
ops-sysd              | ovs | 00006 | ovsdb_if    | ERR  | Failed to commit the transaction. rc = 7
ops-intfd             | ovs | 00007 | intfd_ovsdb_if|WARN| value for speeds not set in h/w d
.....
```

```
switch# show vlog config list
```

```
=====
Features          Description
=====
lldp              Link Layer Discovery Protocol
lacp              Link Aggregation Control Protocol
fan               System Fan
```

```
switch# show vlog config feature lldp
```

```
=====
Feature          Syslog      File
=====
lldp             DBG         WARN
```

```
switch# show vlog config daemon ops-fand
```

```
=====
Daemon          Syslog      File
=====
ops-fand        DBG        WARN
```

```
switch# show vlog config
=====
Feature          Daemon          Syslog      File
=====
lldp             ops-lldpd      DBG        DBG
                 ops-portd      INFO       INFO
lacp             ops-lacpd      OFF        OFF
                 ops-ledd       DBG        EMER
fan              ops-fand       INFO       INFO
```

```
switch# configure
switch(config)# vlog feature lacp syslog dbg
switch(config)# vlog daemon ops-lldpd file warn
switch(config)# end
switch# show vlog feature lacp
```

```
=====
Feature          Syslog      File
=====
lacp             DBG        INFO
```

```
switch# show vlog daemon ops-lldpd
=====
Daemon          Syslog      File
=====
ops-lldpd       DBG        WARN
```

```
switch# configure t
switch(config)# vlog feature lacp file dbg
switch(config)# vlog daemon ops-lldpd syslog info
switch(config)# vlog feature fand all dbg
switch(config)# end
```

```
switch# show vlog config feature lacp
=====
Feature          Syslog      File
=====
lacp             OFF        DBG
```

```
switch# show vlog config daemon ops-lldpd
=====
Daemon          Syslog      File
=====
ops-lldpd       INFO       DBG
```

```
switch# show vlog config feature fan
=====
Feature          Syslog      File
=====
```

```
fan                DBG          DBG
switch# show vlog severity debug daemon ops-pmd
-----
show vlog
-----
ovs|00006|ops_pmd|INFO|ops-pmd (OpenSwitch pmd) 0.02
```

3.33. BroadView Commands

Broadview support depends on the OpenNSL library.

3.33.1. broadview client ip port

Sets the IP address of the remote device on which the application that retrieves BroadView statistics is located.

Syntax `broadview client ip <ipv4-address> port <port-num>`

Authority Admin

`<ipv4-address>` IPv4 address of the remote device.

`<port-num>` Port number the application is using on the remote device.

Example

Setting up communications with a application on device 10.10.47.50 on port 8080

```
switch(config)# broadview client ip 10.10.47.50 port 8080
```

3.33.2. broadview agent-port

Sets the port number the BroadView agent on the switch will use to communicate with the application on the remote device.

Syntax `broadview agent-port <port-num>`

Authority Admin.

`<port-num>` Port number the BroadView agent will use to communicate.

Examples

Setting the agent port to 8080

```
switch(config)# broadview agent-port 8080
```

3.33.3. show broadview

Display configuration settings.

Syntax `show broadview`

Authority Admin.

Example

```
switch# show broadview
BroadView client IP is 10.130.168.30
BroadView client port is 9054
BroadView agent port is 8080
```

3.34. Rebooting the switch.

3.34.1. reboot

Rebooting the switch.

Syntax reboot

Authority Admin.

3.34.2. reboot fast

Fast reboot the switch without waiting for the whole BIOS boot process to finish.

Syntax reboot fast

Authority Admin.

3.34.3. reboot os

Reboot switch and reinstall OS from a media.

Syntax reboot fast

Authority Admin.

3.34.4. reboot primary

Reboot switch to use primary image.

Syntax reboot fast

Authority Admin.

3.34.5. reboot secondary

Reboot switch to use secondary image.

Syntax reboot fast

Authority Admin.

3.34.6. reboot warm

Warm reboot the switch without interruption to the data plane.

Syntax reboot fast

Authority Admin.

Chapter 4. Layer 2 features

Section 4.1, "Interface Commands"

Section 4.2, "MAC Address Table"

Section 4.3, "LACP commands"

Section 4.4, "VLAN commands"

Section 4.5, "MSTP commands"

Section 4.6, "LLDP Commands"

Section 4.7, "Error Disable / Recovery"

Section 4.8, "Unidirectional Link Detection Commands"

Section 4.9, "Storm-Control Commands"

Section 4.10, "FEC"

4.1. Interface Commands

In vtysh every command belongs to a particular context. All interface configuration commands, except interface, work in the interface context.

4.1.1. Change to interface context

This command changes the vtysh context to interface. This command works in the config context.

Syntax	interface
Authority	All users
<A.B>	Subinterface name as physical_interface.subinterface name <1-4294967293>
<IFNAME>	Interface's name
<lag>	Configure link-aggregation parameters
<loopback>	Configure loopback interface
<mgmt>	Configure management interface
<range>	Configure interface range
<tunnel>	Tunnel Configuration
<vlan>	VLAN configuration

Examples

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)#
```

4.1.2. Configure a range of interfaces

Syntax	interface range
Authority	All users
<intf>	Physical interface
<lag>	Link-aggregation interface
<vlan>	VLAN interface

4.1.3. Enable an interface

This command enables an interface.

Syntax	no shutdown
Authority	All users

Examples

```
switch# configure terminal
switch(config)# interface 1
```

```
switch(config-if)# no shutdown
```

4.1.4. Disable an interface

This command disables an interface.

Syntax shutdown

Authority All users

Examples

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# shutdown
```

4.1.5. Enable routing on an interface

This command enables routing on an interface.

Syntax routing

Authority All users

Examples

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# routing
```

4.1.6. Disable routing on an interface

This command disables routing on an interface.

Syntax no routing

Authority All users

Examples

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# no routing
```

4.1.7. Set interface speed

This command sets the operating speed of an interface.

Syntax speed (auto|1000|10000|100000|250000|40000)

Authority All users

<auto> Speed set to auto mode.

<1000>	Speed set to 1 Gbps.
<10000>	Speed set to 10 Gbps.
<100000>	Speed set to 100 Gbps.
<25000>	Speed set to 25 Gbps.
<40000>	Speed set to 40 Gbps.

Examples

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# speed 10000
```

4.1.8. Set interface speed to default

This command sets the operating speed of an interface to default. The default setting is auto.

Syntax	no speed
Authority	All users

Examples

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# no speed
```

4.1.9. Set interface MTU

This command sets the MTU (maximum transmission unit) of an interface.

Syntax	mtu (auto <value>)
Authority	All users
<auto>	MTU set to auto mode.
<value>	MTU value between 576 and 9192 bytes.

Examples

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# mtu auto
switch(config-if)# mtu 580
```

4.1.10. Set interface MTU to default

This command sets the MTU (maximum transmission unit) of an interface to default. The default setting is auto.

Syntax	no mtu
---------------	--------

Authority All users

Examples

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# no mtu
```

4.1.11. Set interface duplexity

This command sets the duplexity of an interface to either half duplex or full duplex.

Syntax duplex (half|full)

Authority All users

<half> Set mode as half duplex.

<full> Set mode as full duplex.

Examples

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# duplex half
```

4.1.12. Set interface duplexity to default

This command sets the duplexity of an interface to default. The default mode is full.

Syntax no duplex

Authority All users

Examples

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# no duplex
```

4.1.13. Enable flow control

This command enables flow control for sending and receiving pause frames.

Syntax flowcontrol (receive|send) (off|on)

Authority All users

<receive> Select the status for receiving pause frames.

<send> Select the status for sending pause frames.

<off> Switches flow control off for the above parameter.

<on> Switches flow control on for the above parameter.

Examples

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# flowcontrol receive on
switch(config-if)# flowcontrol send on
```

4.1.14. Set flowcontrol to default

This command sets the flow control to default. The default is off.

Syntax no flowcontrol (receive|send)
Authority All users
<receive> Select the status for receiving pause frames.
<send> Select the status for sending pause frames.

Examples

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# no flowcontrol receive
switch(config-if)# no flowcontrol send
```

4.1.15. Set autonegotiation state

This command sets the autonegotiation state of the interface.

Syntax autonegotiation (on|off)
Authority All users
<off> Switch off auto negotiation.
<on> Switch on auto negotiation.

Examples

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# autonegotiation on
```

4.1.16. Set autonegotiation to default

This command sets the autonegotiation state to default. The default is off.

Syntax no autonegotiation
Authority All users

Examples

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# no autonegotiation
```

4.1.17. Set an IPv4 address for an interface

This command sets an IPv4 address for an interface. This command only works when the interface is configured as L3.

Syntax ip address <ipv4_address/mask> [secondary]

Authority All users

<ipv4_address> IPv4 address with mask for the interface.
mask>

<secondary> Select this if the IPv4 address is a secondary address.

Examples

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# ip address 10.0.0.2/24
switch(config-if)# ip address 10.0.0.3/24 secondary
```

4.1.18. Remove the IPv4 address for an interface

This command removes the IPv4 address associated with an interface. This command works only when the interface is configured as L3.

Syntax no ip address <ipv4_address/mask> [secondary]

Authority All users

<ipv4_address> IPv4 address with mask for the interface.
mask>

<secondary> Select this if the IPv4 address is a secondary address.

Examples

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# no ip address 10.0.0.2/24
switch(config-if)# no ip address 10.0.0.3/24 secondary
```

4.1.19. Set an IPv6 address for an interface

This command sets an IPv6 address for an interface. This command only works when the interface is configured as L3.

Syntax ipv6 address <ipv6_address/mask> [secondary]

Authority All users

<ipv6_address> IPv6 address with mask for the interface.
mask>

<secondary> Select this if the IPv6 address is a secondary address.

Examples

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# ipv6 address 2001:0db8:85a3:0000:0000:8a2e:0370:7334/24
switch(config-if)# ipv6 address 2001:0db8:85a3:0000:0000:8a2e:0370:733/24
secondary
```

4.1.20. Remove the IPv6 address for an interface

This command removes the IPv6 address associated with an interface. This command only works when the interface is configured as L3.

Syntax no ipv6 address <ipv6_address/mask> [secondary]

Authority All users

<ipv6_address/IPv6 address with mask for the interface.
mask>

<secondary> Select this if the IPv6 address is a secondary address.

Examples

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# no ipv6 address 2001:0db8:85a3:0000:0000:8a2e:0370:7334/24
switch(config-if)# no ipv6 address 2001:0db8:85a3:0000:0000:8a2e:0370:733/24
secondary
```

4.1.21. Split a QSPF interface

The **split** command, splits a QSPF interface to work as four 10Gb/25Gb interfaces. The QSPF interface must support splitter cables in order to split the interface.

The **no split** command combines the split QSPF interface to work as one 40Gb/100Gb interface.

The split interface names are appended with -1,-2,-3 and -4. For example, if the QSPF interface name is 54 then the split interface names are 54-1, 54-2, 54-3 and 54-4.

Syntax [no] split

Authority All users

Examples

```
switch# configure terminal
switch(config)# interface 54
switch(config)# split
```

```
switch# configure terminal
switch(config)# interface 54
switch(config)# no split
```

4.1.22. Show all interfaces

This command displays various switch interfaces with their configurations and statuses.

Syntax show interface [brief]
Authority All users
<brief> Select this to display the output in tabular format.

Examples

```
switch# show interface
Interface 1 is down (Administratively down)
Admin state is down
State information: admin_down
Hardware: Ethernet, MAC Address: 70:72:cf:fd:e7:b4
MTU 9192
Half-duplex
Speed 0 Mb/s
Auto-Negotiation is turned on
Input flow-control is on, output flow-control is on
RX
 0 input packets 0 bytes
 0 input error   0 dropped
 0 CRC/FCS
TX
 0 output packets 0 bytes
 0 input error    4 dropped
 0 collision
```

```
Interface 10 is down (Administratively down)
Admin state is down
State information: admin_down
Hardware: Ethernet, MAC Address: 70:72:cf:fd:e7:b4
MTU 9192
Half-duplex
Speed 0 Mb/s
Auto-Negotiation is turned on
Input flow-control is on, output flow-control is on
RX
 0 input packets 0 bytes
 0 input error   0 dropped
 0 CRC/FCS
TX
 0 output packets 0 bytes
 0 input error    4 dropped
 0 collision
```

.....


```
switch# show interface brief
```

Ethernet Interface	VLAN	Type	Mode	Status	Reason	Speed (Mb/s)	Port Ch#
1	..	eth	..	down	Administratively down		auto
10	..	eth	..	down	Administratively down		auto

```
11          ..          eth          ..          down          Administratively down          auto
```

4.1.23. Show the interface configuration

This command displays the configuration and status of an interface.

- Syntax** show interface <interface> [brief]
- Authority** All users
- <brief> Select this to display the output in tabular format.

Examples

```
switch# show interface 1
Interface 1 is up
Admin state is up
Hardware: Ethernet, MAC Address: 70:72:cf:fd:e7:b4
MTU 1500
Full-duplex
Speed 1000 Mb/s
Auto-Negotiation is turned on
Input flow-control is off, output flow-control is off
RX
    0 input packets      0 bytes
    0 input error        0 dropped
    0 CRC/FCS
TX
    0 output packets    0 bytes
    0 input error        0 dropped
    0 collision
switch# show interface 1 brief
Ethernet      VLAN      Type      Mode      Status      Reason      Speed      Port
Interface                                           (Mb/s)     Ch#
.....
1             ..          eth       ..        down        Administratively down  auto
```

4.1.24. Show transceiver information for all interfaces

This command displays information about pluggable modules or fixed interfaces present in the switch.

- Syntax** show interface transceiver [brief]
- Authority** All users
- <brief> Select this to display the output in tabular format.

Examples

```
switch# show interface transceiver
Interface 1:
Connector: SFP+
Transceiver module: SFP_RJ45
```

```
Connector status: supported
Vendor name: AVAGO
Part number: ABCU-5710RZ-HP8
Part revision:
Serial number: MY36G2C52D
Supported speeds: 1000
```

```
Interface 10:
Connector: SFP+
Transceiver module: not present
```

```
Interface 11:
Connector: SFP+
Transceiver module: not present
```

```
-----
-----
switch# show interface transceiver brief
```

```
-----
Ethernet      Connector      Module      Module
Interface      Type          Status
-----
1              SFP+          SFP_RJ45    supported
10             SFP+          --          --
11             SFP+          --          --
12             SFP+          --          --
13             SFP+          --          --
```

4.1.25. Show transceiver information for an interface

This command displays transceiver information about a particular switch interface.

- Syntax** show interface <interface> transceiver [brief]
- Authority** All users
- <interface> Name of the interface.
- <brief> Select this to display the output in tabular format.

Examples

```
switch# show interface 1 transceiver
Interface 1:
Connector: SFP+
Transceiver module: SFP_RJ45
Connector status: supported
Vendor name: AVAGO
Part number: ABCU-5710RZ-HP8
Part revision:
Serial number: MY36G2C52D
Supported speeds: 1000
```

```
switch# show interface 1 transceiver brief
```

Ethernet Interface	Connector	Module Type	Module Status
1	SFP+	SFP_RJ45	supported

4.1.26. Show the running configuration for all interfaces

This command displays active configurations of various switch interfaces.

Syntax show running-config interface

Authority All users

Examples

```
switch# show running-config interface
Interface 2
  no shutdown
  speed 40000
  autonegotiation on
  exit
Interface 1
  no shutdown
  exit
.....
.....
```

```
switch# show running-config interface
interface bridge_normal
  no shutdown
  no routing
  exit
interface 2
  no shutdown
  lag 100
  exit
interface lag 100
  no routing
  lacp mode active
```

4.1.27. Show the running configuration for an interface

This command displays active configurations of a particular switch interface.

Syntax show running-config interface <interface>

Authority All users

<interface> Name of the interface.

Examples

```
switch# show running-config interface 2
Interface 2
  no shutdown
  speed 40000
  autonegotiation on
  exit
```

```
switch# do show running-config interface lag100
interface lag 100
  no routing
  lacp mode active
```

4.1.28. Show transceiver DOM information for all interfaces

This command displays diagnostics information, and alarm and warning flags of optical transceivers (SFP, SFP+, QSFP+), on all interfaces. This information is known as DOM (Digital Optical Monitoring).

DOM information also consists of vendor determined thresholds which trigger high/low alarm and warning flags.

Syntax show interface dom

Authority All users

Examples

```
switch# sh int 1 dom
Interface 1:
Connector: SFP+
Transceiver module: SFP_SR
  Temperature: 18.00C
  Temperature high alarm: Off
  Temperature low alarm: Off
  Temperature high warning: Off
  Temperature low warning: Off
  Temperature high alarm threshold: 73.00C
  Temperature low alarm threshold: -3.00C
  Temperature high warning threshold: 70.00C
  Temperature low warning threshold: 0.00C
  Voltage: 3.41V
  Voltage high alarm: Off
  Voltage high alarm: Off
  Voltage high alarm: Off
  Voltage low warning: Off
  Voltage high alarm threshold: 3.80V
  Voltage low alarm threshold: 2.81V
  Voltage high warning threshold: 3.46V
  Voltage low warning threshold: 3.13V
  Bias current: 0.16mA
  Bias current high alarm: Off
```

Layer 2 features

```
Bias current low alarm: On
Bias current high warning: Off
Bias current low warning: On
Bias current high alarm threshold: 13.20mA
Bias current low alarm threshold: 1.00mA
Bias current high warning threshold: 12.60mA
Bias current low warning threshold: 1.00mA
Rx power: 0.00mW
Rx power high alarm: Off
Rx power low alarm: On
Rx power high warning: Off
Rx power low warning: On
Rx power high alarm threshold: 1.26mW
Rx power low alarm threshold: 0.11mW
Rx power high warning threshold: 0.79mW
Rx power low warning threshold: 0.18mW
Tx power: 0.01mW
Tx power high alarm: Off
Tx power low alarm: On
Tx power high warning: Off
Tx power low warning: On
Tx power high alarm threshold: 1.00mW
Tx power low alarm threshold: 0.09mW
Tx power high warning threshold: 0.79mW
Tx power low warning threshold: 0.19mW
```

```
Interface 3:
Connector: SFP+
Transceiver module: SFP_DAC
% No DOM information available
```

```
Interface 4:
Connector: SFP+
Transceiver module: SFP_DAC
% No DOM information available
```

```
Interface 5:
Connector: SFP+
Transceiver module: not present
```

```
Interface 6:
Connector: SFP+
Transceiver module: not present
```

```
switch# sh int 49 dom
Interface 49:
Connector: QSFP (splittable)
Transceiver module: QSFP_SR4
  Temperature: 24.00C
  Voltage: 3.37V
```

```
Lane 1:
  Bias current: 0.00mA
```

```
Bias current high alarm: Off
Bias current low alarm: Off
Bias current high warning: Off
Bias current low warning: Off
Rx power: 0.00mW
Rx power high alarm: Off
Rx power low alarm: Off
Rx power high warning: Off
Rx power low warning: Off
```

Lane 2:

```
Bias current: 0.00mA
Bias current high alarm: Off
Bias current low alarm: Off
Bias current high warning: Off
Bias current low warning: Off
Rx power: 0.00mW
Rx power high alarm: Off
Rx power low alarm: Off
Rx power high warning: Off
Rx power low warning: Off
```

Lane 3:

```
Bias current: 0.00mA
Bias current high alarm: Off
Bias current low alarm: Off
Bias current high warning: Off
Bias current low warning: Off
Rx power: 0.00mW
Rx power high alarm: Off
Rx power low alarm: Off
Rx power high warning: Off
Rx power low warning: Off
```

Lane 4:

```
Bias current: 0.00mA
Bias current high alarm: Off
Bias current low alarm: Off
Bias current high warning: Off
Bias current low warning: Off
Rx power: 0.00mW
Rx power high alarm: Off
Rx power low alarm: Off
Rx power high warning: Off
Rx power low warning: Off
```

Interface 50:

```
Connector: QSFP (splittable)
Transceiver module: QSFP_CR4
% No DOM information available
```

Interface 50-1:

```
Connector: QSFP
```

```
Interface 50-2:
Connector: QSFP
```

```
Interface 50-3:
Connector: QSFP
```

```
Interface 50-4:
Connector: QSFP
```

```
Interface 51:
Connector: QSFP (splittable)
Transceiver module: not present
```

4.1.29. Show transceiver DOM information for an interface

This command displays diagnostics information, and alarm and warning flags of optical transceivers (SFP, SFP+, QSFP+), on a particular interface.

Syntax show interface <interface> dom

Authority All users

<interface> Name of the interface.

Examples

```
switch# sh int 1 dom
Interface 1:
Connector: SFP+
Transceiver module: SFP_SR
Temperature: 18.00C
Temperature high alarm: Off
Temperature low alarm: Off
Temperature high warning: Off
Temperature low warning: Off
Temperature high alarm threshold: 73.00C
Temperature low alarm threshold: -3.00C
Temperature high warning threshold: 70.00C
Temperature low warning threshold: 0.00C
Voltage: 3.41V
Voltage high alarm: Off
Voltage high alarm: Off
Voltage high alarm: Off
Voltage low warning: Off
Voltage high alarm threshold: 3.80V
Voltage low alarm threshold: 2.81V
Voltage high warning threshold: 3.46V
Voltage low warning threshold: 3.13V
Bias current: 0.16mA
Bias current high alarm: Off
Bias current low alarm: On
Bias current high warning: Off
```

Layer 2 features

```
Bias current low warning: On
Bias current high alarm threshold: 13.20mA
Bias current low alarm threshold: 1.00mA
Bias current high warning threshold: 12.60mA
Bias current low warning threshold: 1.00mA
Rx power: 0.00mW
Rx power high alarm: Off
Rx power low alarm: On
Rx power high warning: Off
Rx power low warning: On
Rx power high alarm threshold: 1.26mW
Rx power low alarm threshold: 0.11mW
Rx power high warning threshold: 0.79mW
Rx power low warning threshold: 0.18mW
Tx power: 0.01mW
Tx power high alarm: Off
Tx power low alarm: On
Tx power high warning: Off
Tx power low warning: On
Tx power high alarm threshold: 1.00mW
Tx power low alarm threshold: 0.09mW
Tx power high warning threshold: 0.79mW
Tx power low warning threshold: 0.19mW
```

```
switch# sh int 50 dom
Interface 50:
Connector: QSFP (splittable)
Transceiver module: QSFP_SR4
  Temperature: 24.00C
  Voltage: 3.37V
```

```
Lane 1:
Bias current: 0.00mA
Bias current high alarm: Off
Bias current low alarm: Off
Bias current high warning: Off
Bias current low warning: Off
Rx power: 0.00mW
Rx power high alarm: Off
Rx power low alarm: Off
Rx power high warning: Off
Rx power low warning: Off
```

```
Lane 2:
Bias current: 0.00mA
Bias current high alarm: Off
Bias current low alarm: Off
Bias current high warning: Off
Bias current low warning: Off
Rx power: 0.00mW
Rx power high alarm: Off
Rx power low alarm: Off
```

Rx power high warning: Off
Rx power low warning: Off

Lane 3:

Bias current: 0.00mA
Bias current high alarm: Off
Bias current low alarm: Off
Bias current high warning: Off
Bias current low warning: Off
Rx power: 0.00mW
Rx power high alarm: Off
Rx power low alarm: Off
Rx power high warning: Off
Rx power low warning: Off

Lane 4:

Bias current: 0.00mA
Bias current high alarm: Off
Bias current low alarm: Off
Bias current high warning: Off
Bias current low warning: Off
Rx power: 0.00mW
Rx power high alarm: Off
Rx power low alarm: Off
Rx power high warning: Off
Rx power low warning: Off

4.2. MAC Address Table

4.2.1. mac-address-table

This command works with the learnt MAC addresses.

- Syntax** mac-address-table [aging-time] [reserved] [static]
- Authority** Admin user.
- <aging-time> ageing time in seconds, 0-1000000.
- <reserved> *forward* The packets with configured MAC address to be forwarded.
- <static> MAC address in the form xx:xx:xx:xx:xx:xx

Examples

```
switch(config)# mac-address-table reserved ?
forward                The packets with configured MAC address to be
                        forwarded
switch(config)# mac-address-table static ?
MAC                    MAC address in the form xx:xx:xx:xx:xx:xx
switch(config)# mac-address-table aging-time ?
<0-1000000>
```

4.2.2. show mac-address-table

This command displays all of the learnt MAC addresses in the device with following information:

- MAC address
- VLAN Information
- Learnt from ASIC
- Port name

- Syntax** show mac-address-table [dynamic] [port <ports> | vlan <VLAN_ID>] [address <A:B:C:D:E:F>]
- Authority** Admin user.

Examples

```
switch# show mac-address-table
MAC age-time          : 300 seconds
Number of MAC addresses : 3
MAC Address           VLAN      Type      Port
-----
00:01:01:01:01:02    2        dynamic   2
00:01:01:01:01:03    1        dynamic   3
switch#
```

4.2.3. show mac-address-table [dynamic]

This command displays details of all MAC addresses learnt on specified ports.

Syntax show mac-address-table [dynamic] [port < 2 | 1-2 >]
Authority Admin user.
 < 1 or 1-2 or 1,lag1 > Show all learnt MAC addresses on specified ports.

Examples

```
switch# show mac-address-table dynamic port 1
MAC age-time          : 300 seconds
Number of MAC addresses : 1
MAC Address           VLAN      Type      Port
-----
00:01:01:01:01:03    1        dynamic   1
```

```
switch# show mac-address-table dynamic port 1-2
MAC age-time          : 300 seconds
Number of MAC addresses : 2
MAC Address           VLAN      Type      Port
-----
00:01:01:01:01:02    2        dynamic   2
00:01:01:01:01:03    1        dynamic   1
```

This command displays details of all MAC addresses learnt on specified VLANs.

Syntax show mac-address-table [dynamic] [vlan < 2 | 1-2 >]
Authority Admin user.
 < 1 or 1-2 or 1,lag1 > Show all MAC addresses learnt on specified VLANs.

Examples

```
switch# show mac-address-table dynamic vlan 1
MAC age-time          : 300 seconds
Number of MAC addresses : 1
MAC Address           VLAN      Type      Port
-----
00:01:01:01:01:03    1        dynamic   1
```

```
switch# show mac-address-table dynamic vlan 2-3
MAC age-time          : 300 seconds
Number of MAC addresses : 2
MAC Address           VLAN      Type      Port
-----
00:01:01:01:01:02    2        dynamic   2
00:01:01:01:0c:02    3        dynamic   2
```

4.2.4. show mac-address-table address < mac-address >

This command displays details of specified learnt MAC address.

Syntax show mac-address-table address <A:B:C:D:E:F>

Authority Admin user.

<A:B:C:D:E:F> Show details of the learnt MAC address.

Examples

```
switch# show mac-address-table address 00:01:01:01:01:03
MAC age-time           : 300 seconds
Number of MAC addresses : 1
MAC Address            VLAN      Type      Port
-----
00:01:01:01:01:03    1        dynamic   1
```

4.3. LACP commands

4.3.1. Creation of LAG interface

This command creates a Link Aggregation Group (LAG) interface represented by an ID.

Syntax interface lag ID

Authority All users

<ID> This command takes an ID as a parameter which represents a LAG interface. The LAG interface ID can be in the range of 1 to 2000.

Examples

```
switch(config)# interface lag 100
switch(config-lag-if)#
```

4.3.2. Deletion of LAG interface

This command deletes a LAG interface represented by an ID.

Syntax no interface lag ID

Authority All users

<ID> This command takes an ID as a parameter which represents a LAG interface. The LAG interface ID can be in the range of 1 to 2000.

Examples

```
switch(config)# no interface lag 100
```

4.3.3. Configuring LACP system priority

This command sets a Link Aggregation Control Protocol (LACP) system priority.

Syntax lacp system-priority <0-65535>

Authority All users

<0-65535> This command takes a system priority value in the of range 0 to 65535.

Examples

```
switch(config)# lacp system-priority 100
```

4.3.4. Configuring default LACP system priority

This command sets an LACP system priority to a default(65534).

Syntax no lacp system-priority

Authority All users

Examples

```
switch(config)# no lacp system-priority
```

4.3.5. Assigning interface to LAG

This command adds an interface to a LAG interface specified by an ID.

Syntax lag ID
Authority All users
<ID> This command takes an ID as a parameter which represents a LAG interface. The LAG interface ID can be in the range of 1 to 2000.

Examples

```
switch(config)# interface 1  
switch(config-if)# lag 100
```

4.3.6. Removing interface from LAG

This command removes an interface from a LAG interface specified by an ID.

Syntax no lag ID
Authority All users
<ID> This command takes an ID as a parameter which represents a LAG interface. The LAG interface ID can be in the range of 1 to 2000.

Examples

```
switch(config)# interface 1  
switch(config-if)# no lag 100
```

4.3.7. Configuring LACP port-id

This command sets an LACP port-id value of the interface.

Syntax lacp port-id <1-65535>
Authority All users
<1-65535> This command takes a port-id value in the range of 1 to 65535.

Examples

```
switch(config-if)# lacp port-id 10
```

4.3.8. Configuring LACP port-priority

This command sets an LACP port-priority value for the interface.

Syntax lacp port-priority <1-65535>

Authority All users
<1-65535> This command takes a port-priority value in the range of 1 to 65535.

Examples

```
switch(config-if)# lacp port-priority 10
```

4.3.9. Entering into LAG context

This command enters into the LAG context of the specified LAG ID. If the specified LAG interface is not present, this command creates a LAG interface and enters it into the LAG context.

Syntax interface lag ID
Authority All users
<ID> This command takes an ID as a parameter which represents a LAG interface. The LAG interface ID can be in the range of 1 to 2000.

Examples

```
switch(config)# interface 1  
switch(config-if)# lag 100
```

4.3.10. Configuring LACP mode

This command sets an LACP mode to active or passive. The no form of the command sets the LACP mode to off.

Syntax [no] lacp mode {active/passive}
Authority All users
<active/passive> This command takes an active or passive keyword as an argument to set an LACP mode.

Examples

```
switch(config)# interface lag 1  
switch(config-lag-if)# lacp mode active  
switch(config-lag-if)# no lacp mode active
```

4.3.11. Configuring hash type

This command sets an LACP hash type to l2-src-dst, l3-src-dst or l4-src-dst. The default is l3-src-dst.

Syntax hash {l2-src-dst/l3-src-dst/l4-src-dst}
Authority All users

Examples

```
switch(config)# interface lag 1  
switch(config-lag-if)# hash l2-src-dst
```

4.3.12. Configuring LACP fallback

This command enables LACP fallback. The no form of the command disables LACP fallback.

Syntax [no] lacp fallback
Authority All users

Examples

```
switch(config)# interface lag 1
switch(config-lag-if)# lacp fallback
switch(config-lag-if)# no lacp fallback
```

4.3.13. Configuring LACP fallback mode

This command sets LACP fallback mode to priority or all_active. The no form of the command takes only all_active mode and sets LACP fallback mode to priority.

Syntax lacp fallback mode priority|all_active
Syntax no lacp fallback mode all_active
Authority All users
<mode> Keyword to set LACP fallback mode.

Examples

```
switch(config)# interface lag 1
switch(config-lag-if)# lacp fallback mode all_active
switch(config-lag-if)# no lacp fallback mode all_active
```

4.3.14. Configuring LACP fallback timeout

This command sets LACP fallback timeout value. The no form of the command sets LACP fallback timeout to 0.

Syntax [no] lacp fallback timeout <1-900>
Authority All users
<timeout> Value in seconds to set LACP fallback timeout.

Examples

```
switch(config)# interface lag 1
switch(config-lag-if)# lacp fallback timeout 150
switch(config-lag-if)# no lacp fallback timeout 150
```

4.3.15. Configuring LACP rate

This command sets an LACP heartbeat request time to fast. The default is slow, which is once every 30 seconds. The no form of the command sets an LACP rate to slow.

Syntax lacp rate fast

Authority All users

Examples

```
switch(config)# interface lag 1
switch(config-lag-if)# lacp rate fast
```

4.3.16. Configuring no shutdown

This command sets every interface in LAG to no shutdown.

Syntax no shutdown

Authority All users

Examples

```
switch(config)# interface lag 1
switch(config-lag-if)# no shutdown
```

4.3.17. Configuring shutdown

This command sets every interface in LAG to shutdown.

Syntax shutdown

Authority All users

Examples

```
switch(config)# interface lag 1
switch(config-lag-if)# shutdown
```

4.3.18. Display global LACP configuration

This command displays global a LACP configuration.

Syntax show lacp configuration

Authority All users

Examples

```
switch# show lacp configuration
System-id      : 70:72:cf:ef:fc:d9
System-priority : 65534
```

4.3.19. Display LACP aggregates

This command displays all LACP aggregate information if no parameter is passed. If a LAG name is passed as an argument, it shows information of the specified LAG.

Syntax show lacp aggregates [lag-name]
Authority All users
 <lag-name> This command takes a LAG name as an optional parameter.

Examples

```
switch# show lacp aggregates lag100
Aggregate-name       : lag100
Aggregated-interfaces : 1
Heartbeat rate      : slow
Fallback            : false
Fallback mode       : priority
Fallback timeout    : 0
Hash                : 13-src-dst
Aggregate mode      : active
```

```
switch# show lacp aggregates
Aggregate-name       : lag100
Aggregated-interfaces : 1
Heartbeat rate      : slow
Fallback            : false
Fallback mode       : priority
Fallback timeout    : 0
Hash                : 13-src-dst
Aggregate mode      : active
```

```
Aggregate-name       : lag200
Aggregated-interfaces : 3 2
Heartbeat rate      : slow
Fallback            : false
Fallback mode       : all_active
Fallback timeout    : 100
Hash                : 13-src-dst
Aggregate mode      : active
switch#
```

4.3.20. Display LACP interface configuration

This command displays an LACP configuration of the physical interfaces. If an interface name is passed as argument, it only displays an LACP configuration of a specified interface.

Syntax show lacp interfaces [IFNAME]
Authority All users
 <IFNAME> This command takes an interface name as an optional parameter.

Examples

```
switch# show lacp interfaces
State abbreviations
A - Active            P - Passive            F - Aggregable I - Individual
```

```
S - Short-timeout L - Long-timeout N - InSync      O - OutofSync
C - Collecting    D - Distributing
X - State m/c expired      E - Default neighbor state
```

Actor details of all interfaces

```
\-----
Intf Aggregate Port      Port      Key  State  System-id      System  Aggr
   name      id      Priority
\-----
1   lag100    16       1       1     ALFNCDE 70:72:cf:59:97:06 65534  100
3   lag200    70       1       2     ALFOCX  70:72:cf:59:97:06 65534  200
2   lag200    13       1       2     ALFNCDE 70:72:cf:59:97:06 65534  200
.
```

Partner details of all interfaces

```
\-----
Intf Aggregate Partner Port      Key  State  System-id      System  Aggr
   name      Port-id Priority
\-----
1   lag100    0       0       0     PLFNCD 00:00:00:00:00:00 0       100
3   lag200    0       0       0     PSFO   00:00:00:00:00:00 0       200
2   lag200    0       0       0     PLFNCD 00:00:00:00:00:00 0       200
```

```
switch# show lacp interfaces lag100
```

State abbreviations

```
A - Active          P - Passive          F - Aggregable I - Individual
S - Short-timeout L - Long-timeout N - InSync      O - OutofSync
C - Collecting     D - Distributing
X - State m/c expired      E - Default neighbor state
```

Aggregate-name :

```
\-----
                        Actor          Partner
\-----
Port-id                |              |
Port-priority          |              |
Key                    |              |
State                  |              |
System-id              |              |
System-priority        |              |
switch#
```

4.3.21. LAG show running-config

This command displays the complete switch configuration, when the switch has LAGs configured it should display all the configuration specific to those interfaces.

Syntax show running-config

Authority All users

Examples

```
switch# show running-config
```

```

Current configuration:
!
!
!
!
!
vlan 1
    no shutdown
interface lag 2
    no shutdown
    ip address 10.2.2.2/24
    ipv6 address 2001::1/64
interface lag 3
    no shutdown
    lacp mode passive
interface lag 1
    no shutdown
    lacp mode active
    ip address 10.1.1.1/24
    ipv6 address 2001:db8:a0b:12f0::1/64

```

4.3.22. LAG diag-dump basic

This command displays diagnostic information about the system LAGs. If a file is specified, it captures the information to it. The information includes the configured, eligible and participant interface members of all the LAGs in the system. It also includes the amount of PDUs and marker PDUs sent and received by each interface configured as member of one dynamic LAG, and the LACP state machine state for each dynamic LAG in the system. It also includes the configuration files for the Linux bonding driver for each LAG in the system.

Syntax diag-dump lacp basic [file]
Authority All users
<file> File to capture the command output.

Examples

```

switch# diag-dump lacp basic
=====
[Start] Feature lacp Time : Wed Apr 6 01:54:44 2016
=====
[Start] Daemon ops-lacpd
-----
System Ports:
===== Ports =====
Port lag2:
    lacp                   : active
    lag_member_speed       : 1000
    configured_members     : 5 4
    eligible_members       : 5 4
    participant_members    : 5 4

```

Layer 2 features

```
interface_count      : 2
Port 1:
  lacp                : off
  lag_member_speed    : 1000
  configured_members  : 1
  eligible_members    : 1
  participant_members :
  interface_count     : 0
Port bridge_normal:
  lacp                : off
  lag_member_speed    : 0
  configured_members  : bridge_normal
  eligible_members    :
  participant_members :
  interface_count     : 0
```

```
LAG interfaces:
Port lag2:
  configured_members  : 5 4
  eligible_members    : 5 4
  participant_members : 5 4
```

```
LACP PDUs counters:
LAG lag2:
Configured interfaces:
Interface: 5
  lacp_pdus_sent: 10
  marker_response_pdus_sent: 0
  lacp_pdus_received: 7
  marker_pdus_received: 0
Interface: 4
  lacp_pdus_sent: 10
  marker_response_pdus_sent: 0
  lacp_pdus_received: 8
  marker_pdus_received: 0
```

```
LACP state:
LAG lag2:
Configured interfaces:
Interface: 5
  actor_oper_port_state
    lacp_activity:1 time_out:0 aggregation:1 sync:1 collecting:1
    distributing:1 defaulted:0 expired:0
  partner_oper_port_state
    lacp_activity:1 time_out:0 aggregation:1 sync:1 collecting:1
    distributing:1 defaulted:0 expired:0
  lacp_control
    begin:0 actor_churn:0 partner_churn:0 ready_n:1 selected:1
    port_moved:0 ntt:0 port_enabled:1
Interface: 4
  actor_oper_port_state
    lacp_activity:1 time_out:0 aggregation:1 sync:1 collecting:1
```

Layer 2 features

```
        distributing:1 defaulted:0 expired:0
partner_oper_port_state
    lacp_activity:1 time_out:0 aggregation:1 sync:1 collecting:1
        distributing:1 defaulted:0 expired:0
lacp_control
    begin:0 actor_churn:0 partner_churn:0 ready_n:1 selected:1
        port_moved:0 ntt:0 port_enabled:1
```

```
-----
[End] Daemon ops-lacpd
-----
```

```
-----
[Start] Daemon ops-portd
-----
```

```
Configuration file for lag2:
Ethernet Channel Bonding Driver: v3.7.1 (April 27, 2011)
```

```
Bonding Mode: load balancing (xor)
Transmit Hash Policy: layer2 (0)
MII Status: up
MII Polling Interval (ms): 0
Up Delay (ms): 0
Down Delay (ms): 0
```

```
Slave Interface: 5
MII Status: up
Speed: 10000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 70:72:cf:3a:b6:b6
Slave queue ID: 0
```

```
Slave Interface: 4
MII Status: up
Speed: 10000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 70:72:cf:3a:b6:b6
Slave queue ID: 0
```

```
-----
[End] Daemon ops-portd
-----
```

```
=====
[End] Feature lacp
=====
```

```
Diagnostic dump captured for feature lacp
```

4.4. VLAN commands

4.4.1. Assigning an interface to access mode VLAN

This command assigns the interface to an existing access VLAN represented by the ID in the command. If the VLAN does not exist already, this command displays an error.

Syntax vlan access <vlanid>
Authority All users
<vlanid> Represents VLAN and takes values from 1 to 4094

Examples

The following commands assign interface 2 to access mode VLAN 20.

```
switch(config)# interface 2
switch(config-if)#no routing
switch(config-if)#vlan access 20
```

4.4.2. Removing an interface from access mode VLAN

This command removes the interface from an access VLAN represented by an ID.

Syntax no vlan access [<vlanid>]
Authority All users
<vlanid> Represents VLAN and takes values from 1 to 4094

Examples

```
switch(config)#interface 2
switch(config-if)# no VLAN access
```

OR

```
switch(config-if)# no VLAN access 20
```

4.4.3. Assigning a trunk native VLAN to an interface

This command assigns a trunk native VLAN represented by an ID to an interface or a LAG interface. The interface or LAG interface should have routing disabled for this command to work correctly.

Syntax vlan trunk native <vlanid>
Authority All users
<vlanid> Represents VLAN and takes values from 1 to 4094

Examples

```
switch(config)# interface 2
```

```
switch(config-if)#no routing
switch(config-if)#vlan trunk native 20
```

```
switch(config)# interface lag 2
switch(config-lag-if)#no routing
switch(config-lag-if)#vlan trunk native 20
```

4.4.4. Removing a trunk native VLAN from an interface

This command removes the trunk native VLAN from an interface/LAG interface.

Syntax no vlan trunk native [<vlanid>]
Authority All users
<vlanid> Represents VLAN and takes values from 1 to 4094

Examples

```
switch(config)# interface 2
switch(config-if)#no vlan trunk native
```

```
switch(config)# interface lag 2
switch(config-lag-if)#no vlan trunk native
```

4.4.5. Assigning tagging on a native VLAN to an interface

This command enables tagging on a native VLAN to an interface or a LAG interface.

Syntax vlan trunk native tag
Authority All users

Examples

```
switch(config)# interface 2
switch(config-if)#no routing
switch(config-if)#vlan trunk native tag
```

```
switch(config)# interface lag 2
switch(config-if)#no routing
switch(config-lag-if)#vlan trunk native tag
```

4.4.6. Removing tagging on a native VLAN from an interface

This command disables tagging on a native VLAN on an interface/LAG interface.

Syntax no vlan trunk native tag
Authority All users

Examples

The following commands remove interface 2 from tagged trunk native VLAN.

```
switch(config)# interface 2
switch(config-if)# no vlan trunk native tag
```

The following commands remove interface LAG 2 to trunk native VLAN 20 which is already created.

```
switch(config)# interface lag 2
switch(config-lag-if)# no vlan trunk native tag
```

4.4.7. Assigning a VLAN to a trunk on the interface

This command assigns the VLAN represented by an ID to a trunk on the interface / LAG interface. This command expects the interface / LAG interface to be already configured as part of the trunk VLAN.



vlanid can accept input in the form of range, comma and both.

For example :

1. vlan trunk allowed 2
2. vlan trunk allowed 2-6
3. vlan trunk allowed 2,5,8,10
4. vlan trunk allowed 2-5,6

Syntax vlan trunk allowed <vlanid>
Authority All users
 <vlanid> Represents VLAN and takes values from 1 to 4094

Examples

```
switch(config)# interface 2
switch(config-if)#no routing
switch(config-if)#vlan trunk native 1
switch(config-if)#vlan trunk allowed 2
```

```
switch(config)# interface lag 2
switch(config-if)#no routing
switch(config-lag-if)#vlan trunk native 1
switch(config-lag-if)#vlan trunk allowed 2
```

```
switch(config)# interface 3
switch(config-if)# no routing
switch(config-if)# vlan trunk native 1
```

```
switch(config-if)# vlan trunk allowed 2-5,10,17
```

4.4.8. Removing a VLAN from a trunk on the interface

This command removes the VLAN represented by an ID from a trunk on the interface/LAG interface.

Syntax no vlan trunk allowed [<vlanid>]
Authority All users
<vlanid> Represents VLAN and takes values from 1 to 4094

Examples

```
switch(config)# interface 2  
switch(config-if)#no vlan trunk allowed 2
```

```
switch(config)# interface lag 2  
switch(config-lag-if)#no vlan trunk allowed 2
```

4.4.9. Turning on a VLAN

This command powers the VLAN up.

Syntax no shutdown
Authority All users

Examples

```
switch(config)# vlan 3  
switch(config-vlan)# no shutdown
```

4.4.10. Turning off a VLAN

This command shuts the VLAN down.

Syntax shutdown
Authority All users

Examples

```
switch(config)# vlan 3  
switch(config-vlan)# shutdown
```

4.4.11. Creating a VLAN

This command creates a VLAN with a given ID and sets the admin state of the VLAN to the default of down.

Syntax vlan <vlanid>

Authority All users
 <vlanid> Represents VLAN and takes values from 1 to 4094

Examples

```
switch(config)# vlan 3
switch(config-vlan)#
```

4.4.12. Deleting a VLAN

This command deletes the VLAN with a given ID. The value ranges from 1 to 4094.

Syntax no vlan < vlanid >
Authority All users
 <vlanid> Represents VLAN and takes values from 1 to 4094

Examples

```
switch(config-vlan)# no vlan 3
switch(config)#
```

4.4.13. Displaying a VLAN summary

This command displays a summary of a VLAN configuration.

Syntax show vlan summary
Authority All users

Examples

```
switch#show vlan summary
```

```
Number of existing VLANs : 2
```

4.4.14. Displaying a VLAN detail

This command displays VLAN configuration information of all existing VLANs in the switch.

Syntax show vlan [< vlanid >]
Authority All users
 <vlanid> Represents VLAN and takes values from 1 to 4094

Examples

```
switch#show vlan
```

VLAN	Name	Status	Reason	Reserved	Interfaces
1	DEFAULT_VLAN_1	down	no_member_port		

Layer 2 features

```
33      VLAN33      up      ok      13port      1
```

```
switch#show vlan 33
```

```
-----  
VLAN    Name           Status  Reason           Reserved    Interfaces  
-----  
33      VLAN33        up      ok               13port
```

4.5. MSTP commands

4.5.1. Enable MSTP protocol

This command enables MSTP feature for all the instances.

Syntax spanning-tree

Authority All users

Examples

```
switch# configure terminal
switch# spanning-tree
```

4.5.2. Disable MSTP protocol

This command disables MSTP feature for all the instances.

Syntax no spanning-tree

Authority All users

Examples

```
switch# configure terminal
switch# no spanning-tree
```

4.5.3. Set MSTP config name

This command sets config name for MSTP.

Syntax spanning-tree config-name <configuration-name>

Authority All users

<configuration-name> Specifies the MSTP configuration name(maximum 32 characters)

Examples

```
switch# configure terminal
switch# spanning-tree config-name MST0
```

4.5.4. Set default MSTP config name

This command sets the default config name for all the instances, default is system MAC-Address.

Syntax no spanning-tree config-name [<configuration-name>]

Authority All users

<con-fig-name> Specifies the MSTP configuration name

Examples

```
switch# configure terminal
switch# no spanning-tree config-name
```

4.5.5. Set MSTP config revision number

This command sets config revision number for the all the instances.

Syntax spanning-tree config-revision <revision-number>

Authority All users

<revision-number> Specifies the MSTP configuration revision number value, 1-65535.

Examples

```
switch# configure terminal
switch# spanning-tree config-revision 40
```

4.5.6. Set default MSTP config revision number

This command sets default config revision number for the all the instances, default value is 0.

Syntax no spanning-tree config-revision [<revision-number>]

Authority All users

<revision-number> Specifies the MSTP configuration revision number value, 1-65535.

Examples

```
switch# configure terminal
switch# no spanning-tree config-revision
```

4.5.7. VLAN to an instance

This command maps the VLAN-ID to corresponding instance.

Syntax spanning-tree instance <instance-id> vlan <VLAN-ID>

Authority All users

<instance-id> Specifies the MSTP instance number, 1-64.

<VLAN-ID> Specifies the VLAN-ID number, 1-4094

Examples

```
switch# configure terminal
switch# spanning-tree instance 1 vlan 1
switch# spanning-tree instance 1 vlan 2
```

4.5.8. Remove VLAN from instance

This command removes the VLAN-ID from the MSTP instance.

Syntax no spanning-tree instance <instance-id> vlan <VLAN-ID>

Authority All users

<instance-id> Specifies the MSTP instance number, 1-64.

<VLAN-ID> Specifies the VLAN-ID number, 1-4094

Examples

```
switch# configure terminal
switch# no spanning-tree instance 1 vlan 1
switch# no spanning-tree instance 1 vlan 2
```

4.5.9. Set forward delay

This command sets the forward-delay for the bridge.

Syntax spanning-tree forward-delay <delay-in-secs>

Authority All users

<delay-in-secs> Specifies the forward delay in seconds, 4-30

Examples

```
switch# configure terminal
switch# spanning-tree forward-delay 6
```

4.5.10. Set default forward delay

This command sets the default forward-delay for the bridge, default value is 15 seconds.

Syntax no spanning-tree forward-delay [<delay-in-secs>]

Authority All users

<delay-in-secs> Specifies the forward delay in seconds, 4-30

Examples

```
switch# configure terminal
switch# no spanning-tree forward-delay
```

4.5.11. Set hello time

This command sets the hello interval for all the MSTP instances.

Syntax spanning-tree hello-time <hello-in-secs>

Authority All users

<hello-in-secs> Specifies the hello interval in seconds, 2-10

Examples

```
switch# configure terminal
switch# spanning-tree hello-time 6
```

4.5.12. Set default hello time

This command sets the default hello interval for all the MSTP instances, default value is 2 seconds.

Syntax no spanning-tree hello-time [<hello-in-secs>]

Authority All users

<hello-in-secs> Specifies the hello interval in seconds, 2-10

Examples

```
switch# configure terminal
switch# no spanning-tree hello-time
```

4.5.13. Set MSTP priority

This command sets the priority for all the MSTP instances. The priority value will be derived by multiplying with value of 4096.

Syntax spanning-tree priority <0-15>

Authority All users

<priority> Specifies the priority

Examples

```
switch# configure terminal
switch# spanning-tree priority 12
```

4.5.14. Set default MSTP priority

This command sets the priority to its default value of 8 for all the MSTP instances. The priority value will be derived by multiplying with value of 4096.

Syntax no spanning-tree priority [<0-15>]

Authority All users

<priority> Specifies the priority

Examples

```
switch# configure terminal
switch# spanning-tree priority 12
```

4.5.15. Set transmit hold count

This command sets the txHoldCount for all the MSTP instances. Used by protocol to limit the maximum transmission rate of MST BPDUs within the hello interval.

Syntax spanning-tree transmit-hold-count <0-10>
Authority All users
<transmit-hold-count> Specifies the txHoldCount in pps

Examples

```
switch# configure terminal
switch# spanning-tree transmit-hold-count 5
```

4.5.16. Set default transmit hold count

This command sets the txHoldCount to its default value of 6 pps for all MST instances.

Syntax no spanning-tree transmit-hold-count [<0-10>]
Authority All users
<transmit-hold-count> Specifies the txHoldCount in pps

Examples

```
switch# configure terminal
switch# spanning-tree transmit-hold-count 5
```

4.5.17. Set max age

This command sets the maximum age for all the MSTP instances.

Syntax spanning-tree max-age <age-in-secs>
Authority All users
<age-in-secs> Specifies the maximum age in seconds, 6-30

Examples

```
switch# configure terminal
switch# spanning-tree max-age 10
```

4.5.18. Set default max age

This command sets the default max age for all the MSTP instances, default value is 20 seconds.

Syntax no spanning-tree max-age [<age-in-secs>]
Authority All users
<age-in-secs> Specifies the maximum age in seconds, 6-30

Examples

```
switch# configure terminal
switch# no spanning-tree max-age
```

4.5.19. Set max hops

This command sets the hop count for all the MSTP instances.

Syntax spanning-tree max-hops <hop-count>
Authority All users
<hop-count> Specifies the maximum number of hops, 1-40.

Examples

```
switch# configure terminal
switch# spanning-tree max-hops 10
```

4.5.20. Set default max hops

This command sets the default hop count for all the MSTP instances, default value is 20.

Syntax no spanning-tree max-hops [<hop-count>]
Authority All users
<hop-count> Specifies the maximum number of hops, 1-40.

Examples

```
switch# configure terminal
switch# no spanning-tree max-hops
```

4.5.21. Set instance priority

This command sets the priority value for that particular instance.

Syntax spanning-tree instance <1-64> priority <0-15>
Authority All users
<instance-id> Specifies the instance-id
<priority-value> Specifies the priority value

Examples

```
switch# configure terminal
switch# spanning-tree instance 1 priority 5
```

4.5.22. Set default instance priority

This command sets the default priority value for that particular instance.

Syntax no spanning-tree instance <1-64> priority [<0-15>]

Authority All users

<instance-id> Specifies the instance-id

<priority-value> Specifies the priority value

Examples

```
switch# configure terminal
switch# no spanning-tree instance 1 priority
```

4.5.23. Set port type

This command sets the port-type for all the MSTP instances.

Syntax spanning-tree port-type (admin-edge | admin-network)

Authority All users

<admin-edge> Specifies the port as admin-edge

<admin-network> Specifies the port as admin-network

Examples

```
switch# configure terminal
switch# interface 1
switch# spanning-tree port-type admin-edge
switch# spanning-tree port-type admin-network
```

4.5.24. Set default port type

This command sets the port-type to its default value of admin-network for all the MSTP instances.

Syntax no spanning-tree port-type [admin-edge | admin-network]

Authority All users

<admin-edge> Specifies the port as admin-edge

<admin-network> Specifies the port as admin-network

Examples

```
switch# configure terminal
switch# interface 1
switch# no spanning-tree port-type
```

4.5.25. Enable bpdu guard

This command enable the bpdu guard on the interfaces.

Syntax spanning-tree bpdu-guard [enable | disable]
Authority All users
<bp-du-guard> Specifies the bpdu-guard
<enable> Specifies the status parameter
<disable> Specifies the status parameter

Examples

```
switch# configure terminal
switch# interface 1
switch# spanning-tree bpdu-guard enable
```

4.5.26. Set default bpdu guard

This command sets the bpdu guard status to its default value of disable on the interface.

Syntax no spanning-tree bpdu-guard [enable | disable]
Authority All users
<bp-du-guard> Specifies the bpdu-guard
<enable> Specifies the status parameter
<disable> Specifies the status parameter

Examples

```
switch# configure terminal
switch# interface 1
switch# spanning-tree bpdu-guard
```

4.5.27. Enable root guard

This command enable the root guard on the interface.

Syntax spanning-tree root-guard [enable | disable]
Authority All users
<root-guard> Specifies the root-guard
<enable> Specifies the status parameter
<disable> Specifies the status parameter

Examples

```
switch# configure terminal
switch# interface 1
switch# spanning-tree root-guard enable
```

4.5.28. Set default root guard

This command sets the root guard status to its default value of disable on the interface.

Syntax no spanning-tree root-guard [enable | disable]
Authority All users
<root-guard> Specifies the root-guard
<enable> Specifies the status parameter
<disable> Specifies the status parameter

Examples

```
switch# configure terminal
switch# interface 1
switch# spanning-tree root-guard
```

4.5.29. Enable loop guard

This command enable the loop guard in the interface.

Syntax spanning-tree loop-guard [enable | disable]
Authority All users
<loop-guard> Specifies the loop-guard
<enable> Specifies the status parameter
<disable> Specifies the status parameter

Examples

```
switch# configure terminal
switch# interface 1
switch# spanning-tree loop-guard enable
```

4.5.30. Set default loop guard

This command sets the loop guard status to its default value of disable on the interface.

Syntax no spanning-tree loop-guard [enable | disable]
Authority All users
<loop-guard> Specifies the loop-guard
<enable> Specifies the status parameter
<disable> Specifies the status parameter

Examples

```
switch# configure terminal
switch# interface 1
switch# spanning-tree loop-guard
```

4.5.31. Enable bpdu filter

This command enable the bpdu filter in the interface.

Syntax spanning-tree bpdu-filter [enable | disable]
Authority All users
<bpdu-filter> Specifies the bpdu-filter
<enable> Specifies the status parameter
<disable> Specifies the status parameter

Examples

```
switch# configure terminal
switch# interface 1
switch# spanning-tree bpdu-guard enable
switch# spanning-tree root-guard disable
```

4.5.32. Set default bpdu filter

This command sets the bpdu filter status to its default value of disable on the interface.

Syntax no spanning-tree bpdu-filter [enable | disable]
Authority All users
<bpdu-filter> Specifies the bpdu-filter
<enable> Specifies the status parameter
<disable> Specifies the status parameter

Examples

```
switch# configure terminal
switch# interface 1
switch# spanning-tree bpdu-guard enable
switch# spanning-tree root-guard disable
```

4.5.33. Set instance cost

This command sets MSTP cost value for that particular instance.

Syntax spanning-tree instance <1-64> cost <1-200000000>
Authority All users
<instance-id> Specifies the instance-id

<cost-value> Specifies the cost value

Examples

```
switch# configure terminal
switch# interface 1
switch# spanning-tree instance 1 cost 2000
```

4.5.34. Set instance default cost

This command sets the default MSTP cost value for the instance to 20000.

Syntax no spanning-tree instance <1-64> cost [<1-200000000>]

Authority All users

<instance-id> Specifies the instance-id

<cost-value> Specifies the cost value

Examples

```
switch# configure terminal
switch# interface 1
switch# no spanning-tree instance 1 cost
```

4.5.35. Set instance port priority

This command sets MSTP port-priority value for that particular instance. The priority value will be derived by multiplying with value of 16.

Syntax spanning-tree instance <1-64> port-priority <1-15>

Authority All users

<instance-id> Specifies the instance-id

<port-priority-value> Specifies the port-priority value

Examples

```
switch# configure terminal
switch# interface 1
switch# spanning-tree instance 1 port-priority 8
```

4.5.36. Set instance default port priority

This command sets the port-priority to its default value of 8 for that MSTP instance. The priority value will be derived by multiplying with value of 16.

Syntax no spanning-tree instance <1-64> port-priority [<1-15>]

Authority All users

<instance-id> Specifies the instance-id

<port-priority-value> Specifies the port-priority value

Examples

```
switch# configure terminal
switch# interface 1
switch# no spanning-tree instance 1 port-priority
```

4.5.37. Show spanning tree global configuration

This command shows priority, address, Hello-time, Max-age, Forward-delay for bridge and root node.

Syntax show spanning-tree

Authority All users

Examples

```
MST0
Spanning tree status: Enabled
Root ID      Priority      : 32768
             MAC-Address : 70:72:cf:e1:b9:16
             This bridge is the root
             Hello time(in seconds): 2  Max Age(in seconds): 20  Forward
             Delay(in seconds): 15
```

```
Bridge ID    Priority      : 32768
             MAC-Address : 70:72:cf:e1:b9:16
             Hello time(in seconds): 2  Max Age(in seconds): 20  Forward
             Delay(in seconds): 15
```

Port	Role	State	Cost	Priority	Type
1	disabled_port	Blocking	0	128	point_to_point
2	disabled_port	Blocking	0	128	point_to_point

4.5.38. Show spanning tree detail configuration

This command shows detail information regarding CIST and corresponding port details.

Syntax show spanning-tree detail

Authority All users

Examples

```
MST0 is executing the mstp compatible Spanning Tree protocol
Bridge Identifier has priority 12, address: 70:72:cf:55:33:cd
Configured Hello time(in seconds): 5  Forward delay(in seconds): 5
Max-age(in seconds):10  txHoldCount(in pps): 5
We are the root of the spanning tree
```

```
Topology change flag not set
Number of topology changes 0, last change occurred 48 seconds ago
```

```
Times: Hold          5 Topology chnage      0
        Hello        5 max age          10, forward delay    5
Timers: Hello expiry 0 forward delay expiry 0
```

```
Port 1 of MST0 is disabled_port
Port path cost 0, Port priority 8
Designated root has priority 4, address 70:72:cf:e1:b9:16
Designated bridge has priority 4, address 70:72:cf:e1:b9:16
Designated port has priority 4, address 70:72:cf:e1:b9:16
Number of transitions to forwarding state: 0
Link type is point_to_point by default, Internal
Bpdus sent 0, received 0
```

```
Port 2 of MST0 is disabled_port
Port path cost 0, Port priority 8
Designated root has priority 4, address 70:72:cf:e1:b9:16
Designated bridge has priority 4, address 70:72:cf:e1:b9:16
Designated port has priority 4, address 70:72:cf:e1:b9:16
Number of transitions to forwarding state: 0
Link type is point_to_point by default, Internal
Bpdus sent 0, received 0
```

4.5.39. Show MSTP global configuration

This command shows MSTP instance and corresponding VLANs.

Syntax show spanning-tree mst-config

Authority All users

Examples

```
MST configuration information
MST config ID          : MST0
MST config revision    : 33
MST config digest      : 0x9bbda9c70d91f633e1e145fbcbf8d321
Number of instances    : 2
```

Instance ID	Member VLANs
1	1,2
3	3

4.5.40. Show MSTP configuration

This command shows global MSTP configuration.

Syntax show spanning-tree mst

Authority All users

Examples

```
switch# show spanning-tree mst
MST0
Vlans mapped:
Bridge      Address:70:72:cf:84:d1:56    priority:8
Root
Regional Root
Operational Hello time(in seconds): 2 Forward delay(in seconds):15
Max-age(in seconds):20 txHoldCount(in pps): 6
Configured  Hello time(in seconds): 2 Forward delay(in seconds):15
Max-age(in seconds):20 txHoldCount(in pps): 6
```

Port	Role	State	Cost	Priority	Type
1	Disabled	Blocking	0	8	point_to_point
2	Disabled	Blocking	0	8	point_to_point

```
MST1
Vlans mapped: 1
Bridge      Address:70:72:cf:84:d1:56    Priority:8
Root        Address:                    Priority:8
            Port:0, Cost:20000, Rem Hops:0
```

Port	Role	State	Cost	Priority	Type
1	Disabled	Blocking	0	8	Point_to_point
2	Disabled	Blocking	0	8	Point_to_point

4.5.41. Show MSTP detail configuration

This command shows detail MSTP CIST and all instance related information with port detail.

Syntax show spanning-tree mst detail

Authority All users

Examples

```
switch# show spanning-tree mst detail
MST0
Vlans mapped:
Bridge      Address:70:72:cf:84:d1:56    priority:8
Root
Regional Root
Operational Hello time(in seconds): 2 Forward delay(in seconds):15
Max-age(in seconds):20 txHoldCount(in pps): 6
Configured  Hello time(in seconds): 2 Forward delay(in seconds):15
Max-age(in seconds):20 txHoldCount(in pps): 6
```

Port	Role	State	Cost	Priority	Type
1	Disabled	Blocking	0	8	point_to_point

Layer 2 features

```
2          Disabled          Blocking  0          8          point_to_point
```

MST1

```
Vlans mapped: 1
Bridge        Address:70:72:cf:84:d1:56   Priority:8
Root         Address:70:72:cf:05:02:b3   Priority:8
            Port:0, Cost:20000, Rem Hops:0
```

Port	Role	State	Cost	Priority	Type
1	Disabled	Blocking	0	8	Point_to_point
2	Disabled	Blocking	0	8	Point_to_point

Port 1

```
Designated root address      : 70:72:cf:05:02:b3
Designated regional root address : 70:72:cf:05:02:b3
Designated bridge address     : 70:72:cf:05:02:b3
Timers:      Message expires in 0 sec, Forward delay expiry:0, Forward transitions:0
Bpdus sent 0, received 0
```

Port 2

```
Designated root address      : 70:72:cf:05:02:b3
Designated regional root address : 70:72:cf:05:02:b3
Designated bridge address     : 70:72:cf:05:02:b3
Timers:      Message expires in 0 sec, Forward delay expiry:0, Forward transitions:0
Bpdus sent 0, received 0
```

4.5.42. Show MSTP instance configuration

This command shows MSTP configurations for the given instance ID.

Syntax show spanning-tree mst <1-64>

Authority All users

Examples

```
switch# sh spanning-tree mst 1
```

```
MST1
Vlans mapped: 1
Bridge        Address:70:72:cf:84:d1:56   Priority:8
Root         Address:                    Priority:8
            Port:0, Cost:20000, Rem Hops:0
```

Port	Role	State	Cost	Priority	Type
1	Disabled	Blocking	0	8	Point_to_point
2	Disabled	Blocking	0	8	Point_to_point

4.5.43. Show MSTP instance configuration

This command shows MSTP configurations for the given instance ID with corresponding port details.

Syntax show spanning-tree mst <1-64> detail

Authority All users

Examples

```
switch# show spanning-tree mst 1 detail
MST1
Vlans mapped: 1
Bridge Address:70:72:cf:84:d1:56 Priority:8
Root Address: Priority:8
Port:0, Cost:20000, Rem Hops:0
```

Port	Role	State	Cost	Priority	Type
1	Disabled	Blocking	0	8	Point_to_point
2	Disabled	Blocking	0	8	Point_to_point

```
Port 1
Designated root address : 70:72:cf:55:33:cd
Designated regional root address : 70:72:cf:55:33:cd
Designated bridge address : 70:72:cf:55:33:cd
Timers: Message expires in 0 sec, Forward delay expiry:0, Forward transitions:0
Bpdus sent 0, received 0
```

```
Port 2
Designated root address : 70:72:cf:55:33:cd
Designated regional root address : 70:72:cf:55:33:cd
Designated bridge address : 70:72:cf:55:33:cd
Timers: Message expires in 0 sec, Forward delay expiry:0, Forward transitions:0
Bpdus sent 0, received 0
```

4.5.44. Show MSTP running configuration

This command shows configured commands for MSTP.

Syntax show running-config spanning-tree

Authority All users

Examples

```
switch# show running-config spanning-tree
!
spanning-tree
spanning-tree config-name MST0
spanning-tree config-revision 3
spanning-tree instance 1 vlan 2
spanning-tree instance 1 vlan 1
spanning-tree priority 12
spanning-tree hello-time 5
spanning-tree forward-delay 5
spanning-tree max-age 10
```

Layer 2 features

```
spanning-tree max-hops 10
spanning-tree transmit-hold-count 5
spanning-tree instance 1 priority 12
interface 2
    spanning-tree instance 1 cost 2000000
interface 1
    spanning-tree instance 1 port-priority 12
    spanning-tree instance 1 cost 200000
```

4.6. LLDP Commands

All LLDP configuration commands except lldp transmission and lldp reception work in config context.

4.6.1. Enable LLDP

This command enables the LLDP (Link Layer Discovery Protocol) feature in the device. By default, LLDP is enabled on the device.

Syntax lldp enable

Authority All users

Examples

```
switch# configure terminal
switch(config)# lldp enable
```

4.6.2. Disable LLDP

This command disables the LLDP (Link Layer Discovery Protocol) feature in the device.

Syntax no lldp enable

Authority All users

Examples

```
switch# configure terminal
switch(config)# no lldp enable
```

4.6.3. Clear LLDP counters

This command clears LLDP neighbor counters.

Syntax lldp clear counters

Authority All users

Examples

```
switch# configure terminal
switch(config)# lldp clear counters
```

4.6.4. Clear LLDP neighbor details

This command clears LLDP neighbor details.

Syntax lldp clear neighbors

Authority All users

Examples

```
switch# configure terminal
switch(config)# lldp clear neighbors
```

4.6.5. Set LLDP holdtime

This command sets the amount of time (in seconds), a receiving device holds the information sent before discarding it.

Syntax lldp holdtime <time>
Authority All users
<time> Select hold time between 2 and 10 seconds.

Examples

```
switch# configure terminal
switch(config)# lldp holdtime 5
```

4.6.6. Set LLDP holdtime to default

This command sets default values for the amount of time a receiving device should hold the information sent before discarding it. The default value is 4 seconds.

Syntax no lldp holdtime
Authority All users

Examples

```
switch# configure terminal
switch(config)# no lldp holdtime
```

4.6.7. Set LLDP reinit delay

This command sets the amount of time (in seconds) to wait before performing LLDP initialization on any interface.

Syntax lldp reinit <time>
Authority All users
<time> Select reinit delay between 1 and 10 seconds.

Examples

```
switch# configure terminal
switch(config)# lldp reinit 5
```

4.6.8. Set LLDP reinit delay to default

This command resets to default value the amount of time to wait before performing LLDP initialization on any interface. The default value is 2 seconds.

Syntax no lldp reinit
Authority All users

Examples

```
switch# configure terminal
switch(config)# no lldp reinit
```

4.6.9. Set management IP address

This command sets the Management IP Address to be sent using LLDP TLV.

Syntax lldp management-address (<ipv4_address> | <ipv6_address>)
Authority All users

<ipv4_address> Set IPV4 address as LLDP management address.

<ipv6_address> Set IPV6 address as LLDP management address.

Examples

```
switch# configure terminal
switch(config)# lldp management-address 16.93.49.9
switch(config)# lldp management-address 2001:db8:85a3::8a2e:370:7334
```

4.6.10. Remove management IP address

This command removes the Management IP Address to be sent using LLDP TLV.

Syntax no lldp management-address
Authority All users

Examples

```
switch# configure terminal
switch(config)# no lldp management-address
```

4.6.11. Select TLVs

This command selects the TLVs to be sent and received in LLDP packets.

Syntax lldp select-tlv (management-address | port-description | port-vlan-id | port-vlan-name | port-protocol-vlan-id | port-protocol-id | system-capabilities | system-description | system-name)

Authority All users

<management-address> Select management-address TLV.

<port-description> Select port-description TLV.

<port-vlan-id>	Select port-vlan-id TLV.
<port-vlan-name>	Select port-vlan-name TLV.
<port-protocol-vlan-id>	Select port-protocol-vlan-id TLV.
<port-protocol-id>	Select port-protocol-id TLV.
<system-capabilities>	Select system-capabilities TLV.
<system-description>	Select system-description TLV.
<system-name>	Select system-name TLV.

Examples

```
switch# configure terminal
switch(config)# lldp select-tlv management-address
switch(config)# lldp select-tlv port-description
switch(config)# lldp select-tlv port-vlan-id
switch(config)# lldp select-tlv port-vlan-name
switch(config)# lldp select-tlv port-protocol-vlan-id
switch(config)# lldp select-tlv port-protocol-id
switch(config)# lldp select-tlv system-capabilities
switch(config)# lldp select-tlv system-description
switch(config)# lldp select-tlv system-name
```

4.6.12. Remove TLVs

This command removes the TLVs from being sent and received in LLDP packets.

Syntax	no lldp select-tlv (management-address port-description port-vlan-id port-vlan-name port-protocol-vlan-id port-protocol-id system-capabilities system-description system-name)
Authority	All users
<management-address>	Select management-address TLV.
<port-description>	Select port-description TLV.
<port-vlan-id>	Select port-vlan-id TLV.
<port-vlan-name>	Select port-vlan-name TLV.
<port-protocol-vlan-id>	Select port-protocol-vlan-id TLV.

<port-protocol-id> Select port-protocol-id TLV.

<system-capabilities> Select system-capabilities TLV.

<system-description> Select system-description TLV.

<system-name> Select system-name TLV.

Examples

```
switch# configure terminal
switch(config)# no lldp select-tlv management-address
switch(config)# no lldp select-tlv port-description
switch(config)# no lldp select-tlv port-vlan-id
switch(config)# no lldp select-tlv port-vlan-name
switch(config)# no lldp select-tlv port-protocol-vlan-id
switch(config)# no lldp select-tlv port-protocol-id
switch(config)# no lldp select-tlv system-capabilities
switch(config)# no lldp select-tlv system-description
switch(config)# no lldp select-tlv system-name
```

4.6.13. Set LLDP timer

This command sets the LLDP status update interval in seconds which are transmitted to neighbors.

Syntax lldp timer <time>

Authority All users

<time> Select timer between 5 and 32768 seconds

Examples

```
switch# configure terminal
switch(config)# lldp timer 7
```

4.6.14. Set LLDP timer to default

This command sets the default time interval for transmitting LLDP status updates to neighbors. The default value is 30 seconds.

Syntax no lldp timer

Authority All users

Examples

```
switch# configure terminal
switch(config)# no lldp timer
```

4.6.15. Enable LLDP transmission

This command enables LLDP transmission (TX) for a particular interface. This command only works in interface context.

Syntax lldp transmit

Authority All users

Examples

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# lldp transmit
```

4.6.16. Disable LLDP transmission

This command disables LLDP transmission (TX) for a particular interface. This command only works in interface context.

Syntax no lldp transmit

Authority All users

Examples

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# no lldp transmit
```

4.6.17. Enable LLDP reception

This command enables LLDP reception (RX) for a particular interface. This command only works in interface context.

Syntax lldp receive

Authority All users

Examples

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# lldp receive
```

4.6.18. Disable LLDP reception

This command disables LLDP reception (RX) for a particular interface. This command only works in interface context.

Syntax no lldp receive

Authority All users

Examples

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# no lldp receive
```

4.6.19. Show LLDP configuration

This command displays various switch LLDP configurations. The configuration includes the LLDP timer, transmission status, reception status, selected TLVs and so on.

Syntax show lldp configuration

Authority All users

Examples

```
switch# show lldp configuration
LLDP Global Configuration:
LLDP Enabled :No
LLDP Transmit Interval :30
LLDP Hold time Multiplier :4
```

```
TLVs advertised:
Management Address
Port description
Port VLAN-ID
Port Protocol VLAN-ID
Port VLAN Name
Port Protocol-ID
System capabilities
System description
System name
```

```
LLDP Port Configuration:
Port  Transmission-enabled  Receive-enabled
1      Yes                   Yes
10     Yes                   Yes
11     Yes                   Yes
12     Yes                   Yes
13     Yes                   Yes
```

4.6.20. Show LLDP TLV

This command displays TLVs that will be sent and received in LLDP packets.

Syntax show lldp tlv

Authority All users

Examples

```
switch# show lldp tlv
TLVs advertised:
```

```

Management Address
Port description
Port VLAN-ID
Port Protocol VLAN-ID
Port VLAN Name
Port Protocol-ID
System capabilities
System description
System name
    
```

4.6.21. Show LLDP neighbor information

This command displays information about the switch's neighbors.

Syntax show lldp neighbor-info
Authority All users

Examples

```

switch# show lldp neighbor-info
Total neighbor entries : 1
Total neighbor entries deleted : 0
Total neighbor entries dropped : 0
Total neighbor entries aged-out : 0
    
```

Local Port	Neighbor Chassis-ID	Neighbor Port-ID	TTL
1	10:60:4b:39:3e:80	1	120
2			

4.6.22. Show LLDP neighbor information for the interface

This command displays detailed information about a particular neighbor connected to a particular interface.

Syntax show lldp neighbor-info <interface>
Authority All users
 <interface> Name of the interface. System defined.

Examples

```

switch# show lldp neighbor-info 1
Port : 1
Neighbor entries : 1
Neighbor entries deleted : 0
Neighbor entries dropped : 0
Neighbor entries age-out : 0
Neighbor Chassis-Name : HP-3800-24G-PoEP-2XG
Neighbor Chassis-Description : HP J9587A 3800-24G-PoE+-2XG Switch
Neighbor Chassis-ID : 10:60:4b:39:3e:80
    
```

```
Neighbor Management-Address : 192.168.1.1
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled : Bridge
Neighbor Port-ID : 1
TTL : 120
```

4.6.23. Show LLDP statistics

This command displays global LLDP statistics such as packet counts, unknown TLV received and so on.

Syntax show lldp statistics

Authority All users

Examples

```
switch# show lldp statistics
LLDP Global statistics:
```

```
Total Packets transmitted : 9
Total Packets received : 12
Total Packet received and discarded : 0
Total TLVs unrecognized : 0
```

LLDP Port Statistics:

Port-ID	Tx-Packets	Rx-packets	Rx-discarded	TLVs-Unknown
1	9	12	0	0
10	0	0	0	0

4.6.24. Show LLDP statistics for the interface

This command displays LLDP statistics for a particular interface such as packet counts, unknown TLV received and so on.

Syntax show lldp statistics <interface>

Authority All users

<interface> Name of the interface. System defined.

Examples

```
switch# show lldp statistics 1
LLDP statistics:
Port Name: 1
Packets transmitted :20
Packets received :23
Packets received and discarded :0
Packets received and unrecognized :0
```

4.6.25. Show LLDP local device information

This command displays information advertised by the switch if LLDP feature is enabled by user.

Syntax show lldp local-device

Authority All users

Examples

If all ports are administratively down and link state is down, only global info will be displayed.

```
switch# show lldp local-device
Global Data
-----
Chassis-id           : 48:0f:cf:af:50:c9
System Name         : switch
System Description   : OpenSwitch 0.1.0 (basil) Linux 3.9.11 #1 SMP Fri
Management Address   : 120.92.155.52
Capabilities Available : Bridge, Router
Capabilities Enabled  : Bridge, Router
TTL                  : 120
```

If port 1 is administratively down and the link state is up, global info and only active port details are displayed.

```
Global Data
-----
Chassis-id           : 48:0f:cf:af:50:c9
System Name         : switch
System Description   : OpenSwitch 0.1.0 (basil) Linux 3.9.11 #1 SMP Fri
Management Address   : 120.92.155.52
Capabilities Available : Bridge, Router
Capabilities Enabled  : Bridge, Router
TTL                  : 120
```

```
Port Based Data:
-----
Port-ID              : 1
Port-Description     : "1"
```

If the VLANs are configured on the active ports, the VLAN-Id and VLAN name are displayed along with port details.

The VLAN is configured in access mode (vlan access 100).

```
Global Data
-----
Chassis-id           : 48:0f:cf:af:50:c9
System Name         : switch
System Description   : OpenSwitch 0.1.0 (basil) Linux 3.9.11 #1 SMP Fri
Management Address   : 120.92.155.52
Capabilities Available : Bridge, Router
Capabilities Enabled  : Bridge, Router
TTL                  : 120
```

```
Port Based Data:
-----
```

Layer 2 features

```
Port-ID          : 1
Port-Description : "1"
Port VLAN Id     : 100
VLAN-Ids         : 100
VLAN Name       : VLAN100
```

The VLAN is configured in trunk mode (vlan trunk 200 300).

Global Data

```
-----
Chassis-id      : 48:0f:cf:af:50:c9
System Name     : switch
System Description : OpenSwitch 0.1.0 (basil) Linux 3.9.11 #1 SMP Fri
Management Address : 120.92.155.52
Capabilities Available : Bridge, Router
Capabilities Enabled  : Bridge, Router
TTL             : 120
```

Port Based Data:

```
-----
Port-ID          : 1
Port-Description : "1"
Port VLAN Id     :
VLAN-Ids         : 200, 300
VLAN Name       : VLAN200, VLAN300
```

The VLAN is configured in native tagged or untagged mode (vlan native 100, vlan trunk 200 300).

Global Data

```
-----
Chassis-id      : 48:0f:cf:af:50:c9
System Name     : switch
System Description : OpenSwitch 0.1.0 (basil) Linux 3.9.11 #1 SMP Fri
Management Address : 120.92.155.52
Capabilities Available : Bridge, Router
Capabilities Enabled  : Bridge, Router
TTL             : 120
```

Port Based Data:

```
-----
Port-ID          : 1
Port-Description : "1"
Port VLAN Id     : 100
VLAN-Ids         : 100, 200, 300
VLAN Name       : VLAN100, VLAN200, VLAN300
```

4.7. Error Disable / 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.

This feature works in the global config mode.

4.7.1. errdisable detect

This command detects a specified cause or all causes.

The no form of this command disables the detection. When disabled, auto recovery will not occur for interfaces in a diag-disable state due to that cause.

Syntax	[no] errdisable detect cause <all> <link-flap> <mac-flap> <storm-control> <udld>
Authority	Admin
<all>	Enable error detection on all causes
<link-flap>	Enable error detection on link flap
<mac-flap>	Enable error detection on mac flapping
<storm-control>	Enable error detection on storm control
<udld>	Enable error detection on udld

4.7.2. errdisable flap-setting

Set error disable flap parameters for application.

The no form of this command removes flap parameters.

Syntax	[no] errdisable flap-setting cause link-flap max-flaps <1-100>
Authority	Admin
<1-100>	Flap count

4.7.3. 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.

The no form of this command disables auto recovery for a specific cause or all causes. When disabled, auto recovery will not occur for interfaces in a diag-disable state due to that cause.

Syntax [no] errdisable recovery cause <all> <link-flap> <mac-flap> <storm-control> <udld>
Authority Admin
 <all> Enable error recovery on all causes
 <bpduguard> Enable error recovery on bpduguard
 <link-flap> Enable error recovery on link flap
 <mac-flap> Enable error recovery on mac flapping
 <storm-control> Enable error recovery on storm control
 <udld> Enable error recovery on udld

4.7.4. errdisable recovery interval

Use this command to configure the auto recovery time interval. The auto recovery time interval is common for all causes. The time can be any value from 30 to 86400 seconds. When the recovery interval expires, the system attempts to bring interfaces in the diag-disable state back into service (link up).

The no form of this command resets the auto recovery interval to the factory default value of 300.

Syntax errdisable recovery interval <30-86400>
Authority Admin
 <30-86400> timer-interval(sec)

4.7.5. show errdisable detect

Show errdisable detect configuration

Syntax show errdisable detect
Authority Admin

Examples

```
switch# show errdisable detect
```

ErrDisable Reason	Detection Status
mac-flap	Enable
storm-control	Enable
link-flap	Enable
bpduguard	Enable
udld	Enable

4.7.6. show errdisable flap-values

Show flap values for error disable detection

Syntax show errdisable flap-values

Authority Admin

Examples

```
switch# show errdisable flap-values
```

ErrDisable Reason	Flaps	Time(sec)
-----	-----	-----
mac-flap	5	10
link-flap	5	10

4.7.7. show errdisable recovery

Show errdisable recovery configuration

Syntax show errdisable recovery

Authority Admin

Examples

```
switch# show errdisable recovery
```

ErrDisable Reason	Recovery Status
-----	-----
mac-flap	Disable
storm-control	Disable
link-flap	Disable
bpduguard	Disable
udld	Disable

```
Timer Interval: 300 seconds
```

Interface	Errdisable Reason	Time left(sec)
-----	-----	-----

4.8. Unidirectional Link Detection Commands

The Unidirectional Link Detection (UDLD) feature detects unidirectional links'physical ports. UDLD must be enabled on both sides of the link to detect a unidirectional link. The UDLD protocol operates by exchanging packets containing information about neighboring devices.

The purpose of the UDLD feature is to detect and avoid unidirectional links. A unidirectional link is a forwarding anomaly in a Layer 2 communication channel in which a bi-directional link stops passing traffic in one direction.

4.8.1. udd enable (Global Config)

Use the udd enable command in Global Config mode to enable UDLD globally on the switch.

Default	disable
Syntax	udd enable
Authority	Admin

4.8.2. no udd enable (Global Config)

Use the no udd enable command in Global Config mode to disable UDLD globally on the switch.

Syntax	no udd enable
Authority	Admin

4.8.3. udd message time

Use the udd message time command in Global Config mode to configure the interval between UDLD probe messages on ports that are in the advertisement phase. The interval range is from 7 to 90 seconds.

Default	15
Syntax	udd message time interval
Authority	Admin

4.8.4. udd timeout interval

Use the udd timeout interval command in Global Config mode to configure the time interval after which the UDLD link is considered to be unidirectional. The interval range is from 5 to 60 seconds.

Default	Default 5
Syntax	udd timeout interval interval
Authority	Admin

4.8.5. udd debug

Use the udd enable debug command in Global Config mode to enable UDLD debug globally on the switch.

Use the `no udd enable debug` command in Global Config mode to disable UDLD debug globally on the switch.

Default Disabled
Syntax [no] udd debug enable
Authority Admin

4.8.6. udd enable (Interface Config)

Use the `udd enable` command in Interface Config mode to enable UDLD on the specified interface.

Default Disabled
Syntax udd enable
Authority Admin

4.8.7. no udd enable (Interface Config)

Use the `no udd enable` command in Interface Config mode to disable UDLD on the specified interface.

Syntax no udd enable
Authority Admin

4.8.8. udd port

Use the `udd port` command in Interface Config mode to select the UDLD mode operating on this interface. If the keyword `aggressive` is not entered, the port operates in normal mode.

Default normal
Syntax udd port [aggressive]
Authority Admin

4.8.9. show udd

Use the `show udd` command to display the global settings of UDLD.

Syntax show udd
Authority Admin

Parameter	Definition
Admin Mode	The global administrative mode of UDLD.
Message Interval	The time period (in seconds) between the transmission of UDLD probe packets.

Parameter	Definition
Timeout Interval	The time period (in seconds) before making the decision that the link is unidirectional.

Example:

```
switch# show udd
```

```
UDLD Admin. Mode: Disable
Message Interval: 15 seconds
Timeout Interval: 5 seconds
UDLD Debug: Disable
```

4.8.10. show udd interface

Use the show udd interface command to display the UDLD settings for the specified interface.

Syntax show udd {interface | all}

Authority Admin

Parameter	Definition
interface	The identifying interface 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: <ul style="list-style-type: none"> • Undetermined – UDLD has not collected enough information to determine the state of the link • Not applicable – UDLD is disabled, either globally or on the port. • Shutdown – UDLD has detected a unidirectional link and shutdown the port. That is, the port is in an errDisabled state. • Bidirectional – UDLD has detected a bidirectional link. Undetermined (Link Down) – The port would transition into this state when the port link physically goes down due to any reasons other than the port has been put into D-Disable mode by the UDLD protocol on the switch.

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

```
switch# show udd interface 1
```

```
Interface      UDLD Admin Mode  UDLD Mode  UDLD Status  UDLD Debug
-----
1              Disable          Normal     Not-Applicable
```

4.9. Storm-Control Commands

This section describes commands you use to configure storm-control and view storm-control configuration information. A traffic storm is a condition that occurs when incoming packets flood the LAN, which creates performance degradation in the network. The Storm-Control feature protects against this condition.

OpenSwitch provides broadcast and unicast storm recovery for individual interfaces. Unicast Storm-Control protects against traffic whose MAC addresses are not known by the system. For broadcast and unicast storm-control, if the rate of traffic ingressing on an interface increases beyond the configured threshold for that type, the traffic is dropped.

To configure storm-control, you will enable the feature for all interfaces or for individual interfaces, and you will set the threshold (storm-control level) beyond which the broadcast or unicast traffic will be dropped. The Storm-Control feature allows you to limit the rate of specific types of packets through the switch on a per-port, per-type, basis.

Configuring a storm-control level also enables that form of storm-control. Disabling a storm-control level using the *no* form of storm-control maintains the configured level (to be active the next time that form of storm-control is enabled).



The actual rate of ingress traffic required to activate storm-control is based on the size of incoming packets and the hard-coded average packet size of 512 bytes - used to calculate a packet-per-second (pps) rate - as the forwarding-plane requires pps versus an absolute rate kbps. For example, if the configured limit is 10%, this is converted to ~25000 pps, and this pps limit is set in forwarding plane (hardware). You get the approximate desired output when 512bytes packets are used.

4.9.1. storm-control action

This command disable an interface if a storm occurs.

Default	enabled
Syntax	storm-control action shutdown
Authority	Admin

4.9.2. storm-control broadcast

Use this command to enable broadcast storm recovery mode for one or more interfaces (Interface Config mode). If the mode is enabled, broadcast storm recovery is active and, if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.

Default	enabled
Syntax	storm-control broadcast {level rate}
Authority	Admin
<level>	Set storm suppression level on this interface
<rate>	Set storm rate limitation on this interface

4.9.2.1. no storm-control broadcast

Use this command to disable broadcast storm recovery mode for a specific interface or range of interfaces.

Syntax no storm-control broadcast
Authority Admin

4.9.3. storm-control multicast

This command enables multicast storm recovery mode for an interface or range of interfaces. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default disabled
Syntax storm-control multicast {level | rate}
Authority Admin
<level> Set storm suppression level on this interface
<rate> Set storm rate limitation on this interface

4.9.3.1. no storm-control multicast

This command disables multicast storm recovery mode for an interface.

Syntax no storm-control multicast
Authority Admin

4.9.4. storm-control unicast

This command enables unicast storm recovery mode for an interface or range of interfaces. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

Default disabled
Syntax storm-control unicast {level | rate}
Authority Admin
<level> Set storm suppression level on this interface
<rate> Set storm rate limitation on this interface

4.9.4.1. no storm-control unicast

This command disables unicast storm recovery mode for an interface.

Syntax no storm-control unicast

Authority Admin

4.9.5. show storm-control interface

This command displays switch configuration information. Specify the *interface* to display information about a specific interface.

Syntax show storm-control interface

Authority Admin

Parameter	Definition
Bcast Mode	Shows whether the broadcast storm control mode is enabled or disabled. The factory default is disabled.
Bcast Level	The broadcast storm control level.
Mcast Mode	Shows whether the multicast storm control mode is enabled or disabled.
Mcast Level	The multicast storm control level.
Ucast Mode	Shows whether the Unknown Unicast or DLF (Destination Lookup Failure) storm control mode is enabled or disabled.
Ucast Level	The Unknown Unicast or DLF (Destination Lookup Failure) storm control level.

Example:

```
switch# show storm-control interface 1
```

Intf	Bcast Mode	Bcast Limit	Mcast Mode	Mcast Limit	Ucast Mode	Ucast Limit	Action
1	Disable	256pps	Disable	256pps	Disable	256pps	

4.10. FEC

4.10.1. fec

Enable/disable the RS-FEC mode for the interface.

Syntax [no] fec

Authority Admin

Chapter 5. Layer 3 features

Section 5.1, “L3 Interfaces”

Section 5.2, “Loopback Interface Commands”

Section 5.3, “ARP commands”

Section 5.4, “L3 Subinterfaces Commands”

Section 5.5, “UDP Broadcast Forwarder”

Section 5.6, “Static routes”

Section 5.7, “ECMP commands”

Section 5.8, “eBGP Command Reference”

Section 5.11, “OSPFv2 commands”

Section 5.12, “Source Interface Commands”

Section 5.13, “Virtual Router Redundancy Protocol Commands”

5.1. L3 Interfaces

5.1.1. routing

The command enables or disables the routing for the interface.

Enter the following syntax under the interface context.

Syntax [no] routing
Authority Admin

Example

```
hostname(config-if)# routing
hostname(config-if)#
```

5.1.2. vrf attach

The command attaches or detaches an interface to or from a VRF.

Enter the following syntax under the interface context.



Only default VRF is supported. Multiple VRF is not supported.

Syntax [no] vrf attach <vrf-name>
Authority Admin
<vrf-name> The name of the VRF.

Example

Attach an interface to a VRF (interface: 1, VRF: myVRF)

```
hostname(config)# interface 1
hostname(config-if)# vrf attach myVRF
hostname(config-if)#
```

5.1.3. ip address

This command configures an IPv4 address to the specified interface.

Enter the following syntax under the interface context.

Syntax [no] ip address <address/mask> [secondary]
Authority Admin
<address/mask> The address and mask.

<secondary> Configures a secondary address.

Example

Configure an IPv4 address on the interface.

```
hostname(config-if)# interface 1
hostname(config-if)# ip address 172.16.100.10/24
hostname(config-if)#
```

5.1.4. ipv6 address

This command configures an IPv6 address to the specified interface.

Enter the following syntax under the interface context.

Syntax [no] ipv6 address <address/prefix> [secondary]

Authority Admin

<ad-
dress/prafix> The address and prefix length.

<secondary> Configures a secondary address.

Example

Configure an IPv6 address on the interface.

```
hostname(config)# interface 1
hostname(config-if)# ipv6 address fd00:5708::f02d:4df6/64
hostname(config-if)#
```

5.1.5. ip proxy-arp

The command enables/disables proxy ARP on the specified interface. By default, it is disabled.

Enter the following syntax under the interface context.

Syntax [no] ip proxy-arp

Authority Admin

Example

Configure the proxy ARP on an interface

```
hostname(config)# interface 1
hostname(config-if)# ip proxy-arp
```

5.1.6. ip local-proxy-arp

The command enables or disables local proxy ARP on the specified interface. By default, the local proxy ARP is disabled.

Enter the following syntax under the interface context.

Syntax [no] ip local-proxy-arp
Authority Admin

Example

Configure the local proxy ARP on an interface.

```
hostname(config)# interface 1
hostname(config-if)# ip local-proxy-arp
```

5.1.7. interface vlan

This command lets you create and configure an L3 VLAN interface that corresponds to the specified VLAN ID.

Enter the following syntax under the config context.

Syntax [no] interface vlan <vlan-id>
Authority Admin
<vlan-id> The VLAN ID
<no> Removes the VLAN interface corresponding to the specified VLAN ID

Example

```
hostname(config)# interface vlan 101
hostname(config-if-vlan)#
```

5.1.8. interface

This command lets you create and configure an L3 VLAN interface corresponding to the specified VLAN name.

Enter the following syntax under the config context.

Syntax [no] interface <vlan-name>
Authority Admin
<vlan-name> The VLAN name
<no> Removes the VLAN interface corresponding to the specified VLAN name

Example

```
hostname(config)# interface vlan101
hostname(config-if-vlan)#
```

5.1.9. show interface

This command displays information for the interfaces, including the statistics, the configuration, and the interface state.

Enter the following syntax under the privileged mode.

- Syntax** show interface [brief | mgmt]
Authority Operator.
<brief> Displays brief information of the interfaces.
<mgmt> Displays the management interface details.

Example

Show management interface details.

```
hostname# show interface mgmt
  Address Mode           : dhcp
  IPv4 address/subnet-mask : 120.92.216.83/25
  Default gateway IPv4    : 120.92.216.1
  IPv6 address/prefix     :
  IPv6 link local address/prefix: fe80::4a0f:cfff:feaf:216/64
  Default gateway IPv6    :
  Primary Nameserver      :
  Secondary Nameserver    :
```

Show specific interface in detail mode (interface: 1).

```
hostname# show interface 1

Interface 1 is up
Admin state is up
Hardware: Ethernet, MAC Address: 48:0f:cf:af:02:17
Proxy ARP is enabled
Local Proxy ARP is enabled
MTU 1500
Full-duplex
Speed 1000 Mb/s
Auto-Negotiation is turned on
Input flow-control is off, output flow-control is off
RX
    0 input packets           0 bytes
    0 input error             0 dropped
    0 short frame             0 overrun
    0 CRC/FCS
  L3:
    ucast: 0 packets, 0 bytes
    mcast: 0 packets, 0 bytes
TX
    0 output packets          0 bytes
    0 input error             21 dropped
    0 collision
  L3:
    ucast: 0 packets, 0 bytes
    mcast: 0 packets, 0 bytes
```

Show specific interface in brief mode (interface: 1).

```
hostname# show interface 1 brief
```

Ethernet Interface	VLAN	Type	Mode	Status	Reason	Speed (Mb/s)	Port Ch#
1	--	eth	--	up		1000	--

5.1.10. show interface vlan-name

This command displays the interface VLAN configuration.

Enter the following syntax under the privileged mode.

Syntax show interface <vlan-name>

Authority Operator.

<vlan-name> The VLAN name.

Example

Display the VLAN interface configuration for VLAN: vlan10.

```
hostname# show interface vlan10
```

```
Interface vlan10 is up
Admin state is up
Hardware: Ethernet, MAC Address: 70:72:cf:fd:e9:26
IPv4 address 3.3.3.1/24
RX
    L3:
        ucast: 0 packets, 0 bytes
        mcast: 0 packets, 0 bytes
TX
    L3:
        ucast: 0 packets, 0 bytes
        mcast: 0 packets, 0 bytes
```

5.1.11. show ip interface

This command displays L3 and IPv4 specific information for the interfaces including the statistics, the configuration and the interface state. Currently this command is only supported for L3 physical interfaces and does not support other L3 VLAN interfaces.

Enter the following syntax under the privileged mode.

Syntax show ip interface [ifname] <brief>

Authority Operator.

<ifname> Name of the interface

<brief> Show brief info of routing interfaces

Example

Show L3 IPv4 interface details (interface: 1).

```
hostname# show ip interface 1
Interface 1 is up
Admin state is up
Hardware: Ethernet, MAC Address: 48:0f:cf:af:02:17
IPv4 address: 2.2.2.1/24
MTU 1500
RX
    ucast: 10 packets, 750 bytes
    mcast: 0 packets, 0 bytes
TX
    ucast: 10 packets, 750 bytes
    mcast: 0 packets, 0 bytes
```

5.1.12. show ipv6 interface

This command displays L3 and IPv6 specific information for the interfaces including the statistics, the configuration and the interface state. Currently this command is only supported for L3 physical interfaces and does not support other L3 VLAN interfaces.

Enter the following syntax under the privileged mode.

Syntax show ipv6 interface [ifname] <brief>
Authority Operator.
<ifname> Name of the interface
<brief> Show brief info of routing interfaces

Example

Show L3 IPv6 interface details (interface: 1).

```
hostname# show ipv6 interface 1

Interface 1 is up
Admin state is up
Hardware: Ethernet, MAC Address: 48:0f:cf:af:02:17
IPv6 address: 2000::1001/120
MTU 1500
RX
    ucast: 10 packets, 750 bytes
    mcast: 0 packets, 0 bytes
TX
    ucast: 10 packets, 750 bytes
    mcast: 0 packets, 0 bytes
```

5.2. Loopback Interface Commands

5.2.1. Create loopback interface

This command creates a loopback interface and enters loopback configuration mode.

Syntax interface loopback instance
Authority All Users
<instance> loopback interface ID 1 to 2147483647

Examples

```
switch# configure terminal
switch(config)# interface loopback 1
switch(config-loopback-if)#
```

5.2.2. Delete loopback interface

This command deletes a loopback interface.

Syntax no interface loopback instance
Authority All Users
<instance> loopback interface ID 1 to 2147483647

Examples

```
switch# configure terminal
switch(config)# no interface loopback 1
```

5.2.3. Set/Unset IPv4 address

This command sets the IPv4 address for a loopback interface.

Syntax [no] ip address <ipv4_address/prefix-length>
Authority All Users
<ipv4_address/IPv4 address with prefix-length for the loopback interface
prefix-length>

Examples

```
switch# configure terminal
switch(config)# interface loopback 1
switch(config-loopback-if)# ip address 16.93.50.2/24
```

5.2.4. Set or unset IPv6 addresses

This command sets the IPv6 address for a loopback interface.

Syntax [no] ip address <ipv6_address/prefix-length>
Authority All Users
 <ipv6_address/IPv6 address with prefix-length for the loopback interface
 prefix-length>

Examples

```
switch# configure terminal
switch(config)# interface loopback 1
switch(config-loopback-if)# ipv6 address fd00:5708::f02d:4df6/64
```

5.2.5. Show running configuration

This command displays all loopback interfaces.

Syntax show running-config
Authority All Users

Examples

```
switch# show running-config
.....
.....
interface loopback 1
  no shutdown
  ip address 192.168.1.1/24
interface loopback 2
  no shutdown
  ip address 182.168.1.1/24
.....
.....
```

5.2.6. Show loopback interfaces

This command displays all configured loopback interfaces.

Syntax show interface loopback [brief]
Authority All Users

Examples

```
switch# show interface loopback
Interface loopback 1 is up
Admin state is up
Hardware is Loopback
IPv4 address 192.168.1.1/24
Interface loopback 2 is up
Admin state is up
Hardware is Loopback
IPv4 address 182.168.1.1/24
```

```
switch# show interface loopback brief
```

```
.....
Loop          IPv4 Address      Status
Interface
.....
1            192.168.1.1/24   up
2            192.168.1.2/24   up
```

5.2.7. Show loopback interface

This command displays the configuration and status of a loopback interface.

Syntax show interface loopback instance
Authority All Users
 <instance> loopback interface ID 1 to 2147483647

Examples

```
switch# show interface loopback 1
Interface loopback 1 is up
Admin state is up
Hardware is Loopback
IPv4 address 192.168.1.1/24
```

5.2.8. Supportability Commands

Following events will be logged for loopback interfaces.

- Create loopback interface.
- Configure loopback interface with IPv4 address.
- Configure loopback interface with IPv6 address.
- Remove IPv4 address from loopback interface.
- Remove IPv6 address from loopback interface.
- Delete loopback interface.

5.2.8.1. Display event logs

This command displays all the events logged by loopback interfaces.

Syntax show events category loopback
Authority All Users

Examples

```
switch# show events category loopback
2016-05-31:06:25:43.691954|ops-portd|9001|LOG_INFO|Loopback Interface lo10,
```

```
created
2016-05-31:07:09:03.390671|ops-portd|9001|LOG_INFO|Loopback Interface lo11,
created
2016-05-31:07:09:10.847426|ops-portd|9003|LOG_INFO|Loopback Interface lo11,
configured with ip address 101.2.2.2/24
```

5.2.8.2. Daignostic Dump

This command will dump number of created loopback interfaces.

Syntax diag-dump loopback basic

Authority All Users

Examples

```
switch# diag-dump loopback basic
=====
[Start] Feature loopback Time : Tue May 31 07:19:40 2016

-----
-----
[Start] Daemon ops-portd
-----
-----
Number of Configured loopback interfaces are : 2.

-----
-----
[End] Daemon ops-portd
-----
-----
[End] Feature loopback
=====
```

5.2.8.3. show tech command

This command will display configurations configured to all the loopback interfaces.

Syntax show tech loopback

Authority All Users

Examples

```
switch# show tech loopback
interface loopback 1
  no shutdown
  ip address 192.168.1.1/24
interface loopback 2
  no shutdown
  ip address 182.168.1.1/24
```

5.3. ARP commands

Displays the IPv4 addresses from the Address Resolution Protocol (ARP) table.

Syntax show arp
Authority Operator.

Example

```
hostname# show arp
ARP IPv4 Entries:
-----
IPv4 Address MAC Port Status
172.16.1.1 48:0F:CF:AF:D1:C7 1 --
172.16.1.2 48:0F:CF:AF:D1:C8 2 --
```

5.3.1. show ipv6 neighbors

Displays IPv6 addresses from the neighbor table.

Syntax show ipv6 neighbors
Authority Operator.

Example

```
hostname# show ipv6 neighbors
IPv6 Entries:
-----
IPv6 Address MAC Port Status
FE80:0000:0000:0000:0202:B3FF:FE1E:8329 00:01:02:03:04:08 4 --
FE80:0000:0000:0000:0202:B3FF:FE1E:8328 00:01:02:03:04:07 3 --
```

5.3.2. arp aging

This command sets the ARP entry ageout time.

Syntax [no] arp aging-time <15-21600>
Authority Operator.
<15-21600> ARP entry ageout time (in seconds)

Example

```
switch# configure
switch(config)# arp aging-time 30
```

5.3.3. arp response

This command sets the ARP entry request response timeout.

Syntax [no] arp response-time <1-10>
Authority Operator.
<1-10> ARP entry request response timeout (in seconds)

Example

```
switch# configure  
switch(config)# arp response-time 10
```

5.3.4. arp retry count

This command sets the ARP entry count of maximum requests for retries.

Syntax [no] arp retry-count <1-10>
Authority Operator.
<1-10> ARP entry count of maximum requests for retries

Example

```
switch# configure  
switch(config)# arp retry-count 10
```

5.4. L3 Subinterfaces Commands

5.4.1. Create subinterface

This command creates a subinterface on an L3 interface and enters subinterface configuration mode.

Syntax interface L3_interface.subinterface
Authority All Users
<L3_interface>Name of the interface. System defined.
<subinter- Subinterface ID from 1 to 4294967293
face>

Examples

```
switch# configure terminal
switch(config)# interface 1.1
switch(config-subif)#
```

5.4.2. Delete subinterface

This command deletes a subinterface from an L3 interface.

Syntax no interface L3_interface.subinterface
Authority All Users
<L3_interface>Name of the interface. System defined.
<subinter- Subinterface ID from 1 to 4294967293
face>

Examples

```
switch# configure terminal
switch(config)# no interface 1.1
```

5.4.3. Set or unset IPv4 addresses

This command sets or unsets the IPv4 address for a subinterface.

Syntax [no] ip address <ipv4_address/prefix-length>
Authority All Users
<ipv4_address>IPv4 address with prefix-length for the subinterface
prefix-length>

Examples

```
switch# configure terminal
switch(config)# interface 1.1
```

```
switch(config-subif)# ip address 10.0.10.1/24
```

5.4.4. Set or unset IPv6 addresses

This command sets or unsets the IPv6 address for a subinterface.

Syntax [no] ipv6 address <ipv6_address/prefix-length>

Authority All Users

<ipv6_address/IPv6 address with prefix-length for the subinterface
prefix-length>

Examples

```
switch# configure terminal
switch(config)# interface 1.1
switch(config-subif)# ipv6 address fd00:5708::f02d:4df6/64
```

5.4.5. Set or unset an IEEE 802.1Q VLAN encapsulation

There is no need to remove the old VLAN ID with the "no" option. Instead, enter the VLAN command with a different VLAN ID.

Syntax [no] encapsulation dot1Q vlan-id

Authority All Users

<vlan-id> Represents VLAN and takes values from 1 to 4094

Examples

```
switch# configure terminal
switch(config)# interface 1.1
switch(config-subif)#encapsulation dot1Q 33
```

```
switch# configure terminal
switch(config)# interface 1.1
switch(config-subif)#no encapsulation dot1Q 33
```

5.4.6. Enable interface

This command enables a subinterface.

Syntax no shutdown

Authority All Users

Examples

```
switch# configure terminal
switch(config)# interface 1.1
switch(config-subif)# no shutdown
```

5.4.7. Disable interface

This command disables a subinterface.

Syntax shutdown

Authority All Users

Examples

```
switch# configure terminal
switch(config)# interface 1.1
switch(config-if)# shutdown
```

5.4.8. Show running configuration

This command displays all configured subinterfaces.

Syntax show running-config

Authority All Users

Examples

```
switch# show running-config
.....
.....
interface 1.1
  no shutdown
  ip address 10.0.10.1/24
interface 1.2
  no shutdown
  ip address 10.0.20.1/24
  encapsulation dot1Q 44
.....
.....
```

5.4.9. Show subinterfaces

This command displays all configured subinterfaces. This command also optionally displays a particular L3 interface.

Syntax show interface <L3_interface> sub-interface [brief]

Authority All Users

<L3_interface> Name of the interface. System defined.

<brief> Formats the output in tabular form.

Examples

```
switch# show interface 1 sub-interface
Interface 1.1 is down(Parent Interface Admin down)
```

```

Admin state is down
parent interface is 1
encapsulation dot1Q 33
Hardware: Ethernet, MAC Address: 70:72:cf:fd:e7:b4
IPv4 address 10.0.10.1/24
Input flow-control is off, output flow-control is off
RX
    0 input packets      0 bytes
    0 input error        0 dropped
    0 CRC/FCS
TX
    0 output packets    0 bytes
    0 input error        0 dropped
    0 collision
Interface 1.2 is down(Parent Interface Admin down)
Admin state is down
parent interface is 1
encapsulation dot1Q 44
Hardware: Ethernet, MAC Address: 70:72:cf:fd:e7:b4
IPv4 address 10.0.20.1/24
Input flow-control is off, output flow-control is off
RX
    0 input packets      0 bytes
    0 input error        0 dropped
    0 CRC/FCS
TX
    0 output packets    0 bytes
    0 input error        0 dropped
    0 collision

```

```

switch# show interface 1 sub-interface brief
.....
Sub          VLAN   Type   Mode   Status   Reason                               Speed   Port
Interface                                         Mb/s)   Ch#
.....
1.1         33    eth    ..    down     Administratively down auto         ..
1.2         44    eth    ..    down     Administratively down auto         ..

```

5.4.10. Show subinterface

This command displays the configuration and status of a subinterface.

Syntax show interface <L3_interface.subinterface> [brief]

Authority All Users

<L3_interface>Name of the interface. System defined.

<subinter-
face> Subinterface ID from 1 to 1024

<brief> Formats the output in tabular form.

Examples

```

switch# show interface 1.1
Interface 1.1 is down(Parent Interface Admin down)
Admin state is down
parent interface is 1
encapsulation dot1Q 33
Hardware: Ethernet, MAC Address: 70:72:cf:fd:e7:b4
IPv4 address 10.0.10.1/2
Input flow-control is off, output flow-control is off
RX
    0 input packets      0 bytes
    0 input error        0 dropped
    0 CRC/FCS
TX
    0 output packets    0 bytes
    0 input error        0 dropped
    0 collision
switch# show interface 1.1 brief
.....
Sub          VLAN   Type  Mode   Status  Reason                               Speed  Port
Interface                                         Mb/s)  Ch#
.....
1.1          33    eth   ..    down    Administratively down auto         ..

```

5.4.11. Supportability Commands

5.4.11.1. Display event logs

Description This command displays all the events logged by sub-interfaces.

Following events will be logged for sub-interfaces.

- Create subinterface.
- Configure subinterface with IPv4 address.
- Configure subinterface with IPv6 address.
- Configure subinterface with encapsulation dot 1Q vlan ID.
- Configure subinterface with admin up.
- Configure subinterface with admin down.
- Remove IPv4 address.
- Remove IPv6 address.
- Remove encapsulation dot 1Q vlan ID.
- Delete subinterface.

Syntax show events category subinterface

Authority All users

Examples

```
switch# show events category subinterafce
2016-05-31:06:26:27.363923|ops-portd|10001|LOG_INFO|Sub-Interface 4.5,
created
2016-05-31:07:08:51.351755|ops-portd|10001|LOG_INFO|Sub-Interface 4.4,
created
2016-05-31:07:08:57.418705|ops-portd|10003|LOG_INFO|Sub-Interface 4.4,
configured with ip address 10.1.1.1/24
```

5.4.11.2. Daignostic Dump

This command will dump number of created subinterfaces.

Syntax diag-dump subinterface basic

Authority All users

Examples

```
switch# diag-dump subinterface basic
=====
[Start] Feature subinterface Time : Tue May 31 07:19:57 2016
=====
-----
[Start] Daemon ops-portd
-----
Number of Configured sub-interfaces are : 2.
-----
[End] Daemon ops-portd
-----
[End] Feature subinterface
=====
```

5.5. UDP Broadcast Forwarder

5.5.1. Global enable/disable UDP broadcast forwarding

This command enables/disables the UDP broadcast forwarding.

Syntax [no] ip udp-bcast-forward

Authority Root and Admin users.

Examples

```
switch(config)#ip udp-bcast-forward
switch(config)#no ip udp-bcast-forward
```

5.5.2. Configure UDP forward-protocol on an interface

This command configures a UDP broadcast server on the interface for a particular UDP port.

Syntax [no] ip forward-protocol udp <IPv4-address> <port-number | protocol-name>

Authority Root and Admin users.

<IPv4-address> The IPv4 address of the protocol server. This can be either be a unicast address of a destination server on another subnet, or the broadcast address of the subnet on which a destination server operates.

<port-number> Any UDP port number corresponding to a UDP application supported on a device.

<protocol-name> Any common names for certain well-known UDP port numbers. Supported protocol names are: dns: Domain Name Service (53), ntp: Network Time Protocol (123), netbios-ns: NetBIOS Name Service (137), netbios-dgm: NetBIOS Datagram Service (138), radius: Remote Authentication Dial-In User Service (1812), radius-old: Remote Authentication Dial-In User Service (1645), rip: Routing Information Protocol (520), snmp: Simple Network Management Protocol (161), snmp-trap: Simple Network Management Protocol (162), tftp: Trivial File Transfer Protocol (69), timep: Time Protocol (37).

Examples

```
switch(config)#interface 1
switch(config-if)#ip forward-protocol udp 1.1.1.1 53
```

```
switch(config)#interface 1
switch(config-if)#ip forward-protocol udp 1.1.1.1 dns
```

5.5.3. Show UDP forward-protocol

This command shows the server addresses where broadcast requests received by the switch are to be forwarded.

Syntax show ip forward-protocol [interface <WORD>]

Authority Root and Admin users.

<interface> Select the interface on which UDP broadcast forwarding information needs to be displayed.

Examples

```
switch(config)#ip udp-bcast-forward
switch(config)#interface 1
switch(config-if)#ip forward-protocol udp 1.1.1.1 53
switch(config-if)#ip forward-protocol udp 8.1.1.1 161
switch(config-if)#ip forward-protocol udp 4.4.4.4 137
switch(config)#interface 2
switch(config-if)#ip forward-protocol udp 2.2.2.2 161
```

```
switch#show ip forward-protocol
UDP Broadcast Forwarder : enabled
Interface: 1
  IP Forward Address      UDP Port
  -----
  4.4.4.4                 137
  1.1.1.1                 53
  8.1.1.1                 161
Interface: 2
  IP Forward Address      UDP Port
  -----
  2.2.2.2                 161
```

```
switch#show ip forward-protocol interface 1
```

```
UDP Broadcast Forwarder : enabled
Interface: 1
  IP Forward Address      UDP Port
  -----
  4.4.4.4                 137
  1.1.1.1                 53
  8.1.1.1                 161
```

5.6. Static routes

5.6.1. ip route

This command configures IPv4 static routes.

Under the config context

Syntax	[no] ip route <destination> <nexthop interface> [<distance>]
Authority	Admin
<destination>	The address and mask
<nexthop>	The address of the nexthop
<interface>	The name of the interface
<distance>	Distance for this route. Default is 1 for static routes. 1-255
<no>	Removes the specified configuration for an IPv4 address

Examples

Configuring IPv4 route with nexthop as an IP address (nexthop: 10.10.10.1):

```
hostname(config)# ip route 172.16.32.0/24 10.10.10.1
```

Configuring IPv4 route with nexthop as an interface (interface: 32):

```
hostname(config)# ip route 172.16.32.0/24 32
```

Configuring IPv4 route with nexthop as a VLAN interface (interface: vlan10):

```
hostname(config)# interface vlan10
hostname(config-if-vlan)# ip address 10.10.10.2/24
hostname(config-if-vlan)# exit
hostname(config)# ip route 172.16.32.0/24 vlan10
```

Configuring IPv4 route with nexthop as a subinterface (interface: 1.1):

```
hostname(config)# interface 1.1
hostname(config-subif)# ip address 10.10.10.3/24
hostname(config-subif)# exit
hostname(config)# ip route 172.16.32.0/24 1.1
```

Configuring IPv4 route with nexthop as a L3 LAG interface (interface: lag10):

```
hostname(config)# interface lag10
hostname(config-lag-if)# ip address 10.10.10.3/24
hostname(config-lag-if)# exit
hostname(config)# ip route 172.16.32.0/24 lag10
```

5.6.2. ipv6 route

This command configures IPv6 static routes.

Under the config context

Syntax [no] ipv6 route <destination> <nexthop | interface> [<distance>]
Authority Admin
 <destination> The address and prefix length, X:X::X:X/P.
 <nexthop> The address of the nexthop, X:X::X:X.
 <interface> The name of the interface.
 <distance> Distance for this route. Default is 1 for static routes, 1-255.
 <no> Removes the specified configuration for an IPv6 address

Examples

Configuring IPv6 route with nexthop as an IP address (nexthop: 2010:bda::/):

```
hostname(config)# ipv6 route fde1:87a5:2185:a5fc::/64 2010:bda::/
```

Configuring IPv6 route with nexthop as an interface (interface: 32):

```
hostname(config)# ipv6 route fde1:87a5:2185:a5fc::/64 32
```

Configuring IPv6 route with nexthop as a VLAN interface (interface: vlan10):

```
hostname(config)# interface vlan10
hostname(config-if-vlan)# ipv6 address 2001::1/120
hostname(config-if-vlan)# exit
hostname(config)# ipv6 route fde1:87a5:2185:a5fc::/64 vlan10
```

Configuring IPv6 route with nexthop as a subinterface (interface: 1.1):

```
hostname(config)# interface 1.1
hostname(config-subif)# ipv6 address 2001::2/120
hostname(config-subif)# exit
hostname(config)# ipv6 route fde1:87a5:2185:a5fc::/64 1.1
```

Configuring IPv6 route with nexthop as a L3 LAG interface (interface: lag10):

```
hostname(config)# interface lag10
hostname(config-lag-if)# ipv6 address 2001::3/120
hostname(config-lag-if)# exit
hostname(config)# ipv6 route fde1:87a5:2185:a5fc::/64 lag10
```

5.6.3. show ip route

This command displays the routing table.

Under privileged mode

Syntax show ip route
Authority Operator

Example

```
hostname# show ip route
Displaying ipv4 routes selected for forwarding
'[x/y]' denotes [distance/metric]

10.10.10.0/24, 1 unicast next-hops
    via 1, [0/0], connected
172.16.32.0/24, 1 unicast next-hops
    via 10.10.10.1, [1/0], static
```

5.6.4. show ipv6 route

This command displays the routing table.

Under privileged mode

Syntax show ipv6 route

Authority Operator

Example

```
hostname# show ipv6 route
Displaying ipv6 routes selected for forwarding
'[x/y]' denotes [distance/metric]

fdel:87a5:2185:a5fc::/64, 1 unicast next-hops
    via 2010:bda::, [1/0], static
2010:bda::/64, 1 unicast next-hops
    via 2, [0/0], connected
```

5.7. ECMP commands

5.7.1. ip ecmp load-balance dst-ip disable

Disable destination IP based load balancing. Use the *no* variant to enable.

Under the config context.

Syntax [no] ip ecmp load-balance dst-ip disable

Authority Admin.

Example

```
hostname(config)# ip ecmp load-balance dst-ip disable
hostname(config)#
```

5.7.2. ip ecmp load-balance src-ip disable

Disable source IP based load balancing. Use the *no* variant to enable.

Under the config context.

Syntax [no] ip ecmp load-balance src-ip disable

Authority Admin.

Example

```
hostname(config)# ip ecmp load-balance src-ip disable
hostname(config)#
```

5.7.3. ip ecmp load-balance dst-port disable

Disable destination port based load balancing. Use the *no* variant to enable.

Under the config context.

Syntax [no] ip ecmp load-balance dst-port disable

Authority Admin.

Example

```
hostname(config)# ip ecmp load-balance dst-port disable
hostname(config)#
```

5.7.4. ip ecmp load-balance src-port disable

Disable source port based load balancing. Use the *no* variant to enable.

Under the config context.

Syntax [no] ip ecmp load-balance src-port disable

Authority Admin.

Example

```
hostname(config)# ip ecmp load-balance src-port disable
hostname(config)#
```

5.7.5. ip ecmp load-balance resilient

Disable resilient hashing for load balancing. When enabled, preserves in-flight traffic flows when ECMP group membership changes. Use the *no* variant to enable.

Under the config context.

Syntax [no] ip ecmp load-balance resilient disable

Authority Admin.

Example

```
hostname(config)# ip ecmp load-balance resilient disable
hostname(config)#
```

5.7.6. show ip ecmp

Displays the ECMP configuration.

Under privileged mode.

Syntax show ip ecmp

Authority Operator.

Example

```
hostname# show ip ecmp
ECMP Configuration
-----

ECMP Status      : Enabled
Resilient Hashing : Enabled

ECMP Load Balancing by
-----
Source IP        : Enabled
Destination IP   : Enabled
Source Port      : Enabled
Destination Port : Enabled
```

5.8. eBGP Command Reference



Not all of these commands are implemented, some of them are reserved for the later release.

5.8.1. router bgp

To use the eBGP feature, first configure the eBGP router as shown below.

This command is used to configure the eBGP router. The Autonomous System (AS) number is needed to configure the eBGP router. The BGP protocol uses the AS number to detect whether the BGP connection is internal or external.

Syntax	[no] router bgp <asn>
Authority	Admin user.
<asn>	The AS number, 1 - 4294967295.
<no>	Destroys an eBGP router with the specified AS number.

Examples

```
s1(config)#router bgp 6001
s1(config)#no router bgp 6001
```

5.8.2. bgp router-id

This command specifies the eBGP router-ID for an eBGP router.

Syntax	[no] bgp router-id <A.B.C.D>
Authority	Admin user.
<A.B.C.D>	The IPv4 address.
<no>	Deletes the eBGP router IP address.

Examples

```
s1(config-router)# bgp router-id 10.1.2.1
s1(config-router)# no bgp router-id 10.1.2.1
```

5.9. IPv4 network

This command adds the announcement network.

- Syntax** [no] network <A.B.C.D/M>
Authority Admin user.
<A.B.C.D/M> IPv4 address with the prefix length.
<no> Removes the announced network for the eBGP router.

Examples

The following configuration example shows that network 10.1.2.0/24 is announced to all neighbors:

```
s1(config-router)# network 10.1.2.0/24
s1(config)# do sh run
Current configuration:
!
router bgp 6001
    bgp router-id 10.1.2.1
    network 10.1.2.0/24
```

5.9.1. maximum-paths

This command sets the maximum number of paths for an eBGP router.

- Syntax** [no] maximum-paths <num>
Authority Admin user.
<num> Maximum number of paths, 1-255.
<no> Sets the maximum number of paths to the default value of 1.

Examples

```
s1(config)# router bgp 6001
s1(config-router)# maximum-paths 5
```

5.9.2. timers bgp

This command sets the keepalive interval and hold time for an eBGP router.

- Syntax** [no] timers bgp <keepalive> <holdtime>
Authority Admin user.
<Keepalive> The keepalive interval in seconds, 0-65535.
<holdtime> Hold time in seconds, 0-65535.
<no> Resets the keepalive and hold time values to their default values (60 seconds for the keepalive interval and 180 seconds for the hold time value).

Examples

```
s1(config)# router bgp 6001
s1(config-router)# timers bgp 60 30
```

5.9.3. IPv6 network

This command advertises the IPv6 prefix network.

Syntax [no] network <X:X::X:X/M>
Authority Admin user.
<X:X::X:X/M> The IPv6 prefix address and prefix length.
<no> Deletes the IPv6 prefix network.

Examples

```
s1(config-router)# ipv6 bgp network 2001:1::1/64
s1(config-router)# no ipv6 bgp network 2001:1::1/64
```

5.9.4. bgp fast-external-failover

This command is used to enable fast external failover for eBGP directly connected peering sessions.

Syntax [no] bgp fast-external-failover
Authority Admin user.
<no> Disables eBGP fast external failover.

Examples

```
s1(config-router)# bgp fast-external-failover
s1(config-router)# no bgp fast-external-failover
```

5.9.5. bgp log-neighbor-changes

This command enables logging of eBGP neighbor resets and status changes (up and down).

Syntax [no] bgp log-neighbor-changes
Authority Admin user.
<A.B.C.D> The IPv4 address.
<no> Disables the logging of neighbor status changes.

Examples

```
s1(config-router)# bgp log-neighbor-changes
s1(config-router)# no bgp log-neighbor-changes
```

5.9.6. redistribute routes

This command configures the route redistribution of the specified protocol or kind into eBGP; filtering the routes using the given route-map, if specified.

Syntax	[no] redistribute <connected static ospf> route-map <name>
Authority	Admin user.
<name>	The route-map name, up to 80 chars.
<no>	Removes the redistribution of routes from eBGP.

Examples

```
s1(config)# router bgp 6001
s1(config-router)# redistribute kernel
s1(config-router)# redistribute connected
s1(config-router)# redistribute static
s1(config-router)# redistribute ospf
s1(config-router)# redistribute kernel route-map rml
s1(config-router)# redistribute connected route-map rml
s1(config-router)# redistribute static route-map rml
s1(config-router)# redistribute ospf route-map rml
```

5.9.7. neighbor remote-as

This command creates a neighbor whose remote-as is asn, an autonomous system number. Currently only IPv4 addresses are supported.

Syntax	[no] neighbor <A.B.C.D> remote-as <asn>
Authority	Admin user.
<A.B.C.D>	The peer IPv4 address.
<asn>	The autonomous system number of the peer, 1 - 4294967295.
<no>	Deletes a configured eBGP peer.

Examples

```
s1(config)# router bgp 6001
s1(config-router)# neighbor 10.1.2.1 remote-as 6002
s1(config-router)# no neighbor 10.1.2.1 remote-as 6002
```

5.9.8. neighbor description

This command sets the description for the peer.

Syntax	[no] neighbor <A.B.C.D> description <text>
Authority	Admin user.
<A.B.C.D>	The peer IPv4 address.
<text>	Description of the peer, up to 80 chars.
<no>	Deletes the peer description.

Examples

```
s1(config)# router bgp 6001
s1(config-router)# neighbor 10.1.2.1 remote-as 6002
```

```
s1(config-router)# neighbor 10.1.2.1 description peer1
```

5.9.9. neighbor password

This command enables MD5 authentication on a TCP connection between eBGP peers.

Syntax [no] neighbor <A.B.C.D> password <text>
<A.B.C.D> The peer IPv4 address.
<text> Password for the peer connection, up to 80 chars.
<no> Disables authentication for the peer connection.

Examples

```
s1(config)# router bgp 6001
s1(config-router)# neighbor 10.1.2.1 remote-as 6002
s1(config-router)# neighbor 10.1.2.1 password secret
```

5.9.10. neighbor timers

This command sets the keepalive interval and hold time for a specific eBGP peer.

Syntax [no] neighbor <A.B.C.D> timers <keepalive> <holdtimer>
Authority Admin user.
<Keepalive> The keepalive interval in seconds, 0-65535.
<holdtime> The hold time in seconds, 0-65535.
<no> Resets the keepalive and hold time values to their default values which are 0.

Examples

```
s1(config)# router bgp 6001
s1(config-router)# neighbor 10.1.2.1 remote-as 6002
s1(config-router)# neighbor 10.1.2.1 timers 20 10
```

5.9.11. neighbor allowas-in

This command specifies an allow-as-in occurrence number for an AS to be in the AS path. Issue the no command to clear the state.

Syntax [no] neighbor <A.B.C.D> allowas-in <val>
Authority Admin user.
<A.B.C.D> The peer IPv4 address.
<val> Number of times eBGP allows an instance of AS to be in the AS_PATH, 1-10.
<no> Clears the state.

Examples

```
s1(config)# router bgp 6001
```

```
s1(config-router)# neighbor 10.1.2.1 remote-as 6002
s1(config-router)# neighbor 10.1.2.1 allowas-in 2
```

5.9.12. neighbor remove-private-AS

This command removes private AS numbers from the AS path in outbound routing updates.

Syntax [no] neighbor <A.B.C.D> remove-private-AS
Authority Admin user.
<A.B.C.D> The peer IPv4 address.
<no> Resets to a cleared state (default).

Examples

```
s1(config)# router bgp 6001
s1(config-router)# neighbor 10.1.2.1 remote-as 6002
s1(config-router)# neighbor 10.1.2.1 remove-private-AS
```

5.9.13. neighbor soft-reconfiguration inbound

This command enables software-based reconfiguration to generate inbound updates from a neighbor without clearing the eBGP session. Issue the no command to clear this state.

Syntax [no] neighbor <A.B.C.D> soft-reconfiguration inbound
Authority Admin user.
<A.B.C.D> The peer IPv4 address.
<no> Resets to a cleared state (default).

Examples

```
s1(config)# router bgp 6001
s1(config-router)# neighbor 10.1.2.1 remote-as 6002
s1(config-router)# neighbor 10.1.2.1 soft-reconfiguration inbound
```

5.9.14. neighbor shutdown

This command shuts down the peer. Use this syntax to preserve the neighbor configuration, but drop the eBGP peer state.

Syntax [no] neighbor <A.B.C.D> shutdown
Authority Admin user.
<A.B.C.D> The peer IPv4 address.
<no> Deletes the neighbor state of the peer.

Examples

```
s1(config)# router bgp 6001
```

```
s1(config-router)# neighbor 10.1.2.1 remote-as 6002
s1(config-router)# neighbor 10.1.2.1 shutdown
```

5.9.15. neighbor peer-group

This command assigns a neighbor to a peer-group.

Syntax [no] neighbor <A.B.C.D> peer-group <name>
Authority Admin user.
<A.B.C.D> The peer IPv4 address.
<name> The peer-group name, up to 80 chars.
<no> Removes the neighbor from the peer-group.

Examples

```
s1(config)# router bgp 6001
s1(config-router)# neighbor 10.1.2.1 remote-as 6002
s1(config-router)# neighbor 10.1.2.1 peer-group pgl
```

5.9.16. neighbor route-map

This command applies a route-map on the neighbor for the direction given (in or out).

Syntax [no] neighbor <A.B.C.D> route-map <name> in|out
Authority Admin user.
<A.B.C.D> The peer IPv4 address.
<name> The route-map name, up to 80 chars.
<no> Removes the route-map for the neighbor.

Examples

```
s1(config)# router bgp 6001
s1(config-router)# neighbor 10.1.2.1 remote-as 6002
s1(config-router)# neighbor 10.1.2.1 route-map rml in
```

5.9.17. neighbor advertisement-interval

This command sets the advertisement interval for route updates for a specified neighbor with an IPv4 or IPv6 address.

Syntax [no] neighbor <A.B.C.D|X::X::X:X> advertisement-interval <interval>
Authority Admin user.
<A.B.C.D> The peer IPv4 address.
<X::X::X:X> The peer IPv6 address.
<interval> The time interval for sending eBGP routing updates in secs, 0-600.

<no> Deletes the advertisement interval for a configured eBGP peer.

Examples

```
s1(config)# router bgp 6001
s1(config-router)# neighbor 10.1.2.1 advertisement-interval 400
s1(config-router)# no neighbor 10.1.2.1 advertisement-interval 400
```

```
s1(config)# router bgp 6001
s1(config-router)# neighbor 2001:db8:0:1 advertisement-interval 400
s1(config-router)# no neighbor 2001:db8:0:1 advertisement-interval 400
```

5.9.18. neighbor ebgp-multihop

This command attempts eBGP connections with external AS routers that are not directly connected.

Syntax [no] neighbor <A.B.C.D | X:X::X:X | peer_group_name> ebgp-multihop

Authority Admin user.

<A.B.C.D> The peer IPv4 address.

<X:X::X:X> The peer IPv6 address.

<peer_group_name> The peer-group name, up to 80 chars.

<no> Removes the ebgp-multihop configuration for the neighbor.

Examples

```
s1(config-router)# neighbor 10.1.2.1 ebgp-multihop
s1(config-router)# no neighbor 10.1.2.1 ebgp-multihop
```

5.9.19. neighbor filter-list

This command applies a filter list to the neighbor to filter incoming and outgoing routes.

Syntax [no] neighbor <A.B.C.D|X:X::X:X|WORD> filter-list WORD (in|out)

Authority Admin user.

<A.B.C.D> The peer IPv4 address.

<X:X::X:X> The peer IPv6 address.

<WORD> The neighbor tag.

<WORD> The AS_PATH access list name.

<in> Filters incoming routes.

<out> Filters outgoing routes.

Examples

```
s1(config-router)# neighbor 192.18.1.1 filter-list 1 out
s1(config-router)# no neighbor 192.18.1.1 filter-list 1 out
```

5.9.20. neighbor prefix-list

This command applies a prefix-list to the neighbor to filter updates to and from the neighbor.

Syntax	[no] neighbor (A.B.C.D X::X::X WORD) prefix-list WORD (in out)
Authority	Admin user.
<A.B.C.D>	The peer IPv4 address.
<X::X::X>	The peer IPv6 address.
<WORD>	The neighbor tag.
<WORD>	The name of a prefix list.
<in>	Filters incoming routes.
<out>	Filters outgoing routes.

Examples

```
s1(config-router)# neighbor 10.1.4.2 prefix-list abc in
s1(config-router)# no neighbor 10.1.4.2 prefix-list abc in
```

5.9.21. neighbor soft-reconfiguration

This command allows an inbound soft reconfiguration of the neighbor.

Syntax	[no] neighbor (A.B.C.D X::X::X WORD) soft-reconfiguration inbound
Authority	Admin user.
<A.B.C.D>	The peer IPv4 address.
<X::X::X>	The peer IPv6 address.
<WORD>	The neighbor tag.

Examples

```
s1(config-router)# neighbor 10.108.1.1 soft-reconfiguration inbound
s1(config-router)# no neighbor 10.108.1.1 soft-reconfiguration inbound
```

5.9.22. neighbor ttl-security

This command specifies the maximum number of hops to the eBGP peer.

Syntax	[no] neighbor (A.B.C.D X::X::X WORD) ttl-security hops <1-254>
Authority	Admin user.
<A.B.C.D>	The peer IPv4 address.
<X::X::X>	The peer IPv6 address.
<WORD>	The neighbor tag.
<1-254>	The hop count.

Examples

```
s1(config-router)# neighbor 10.1.1.1 ttl-security hops 2
s1(config-router)# no neighbor 10.1.1.1 ttl-security hops 2
```

5.9.23. as-path access-list

This command facilitates the configuration of access lists, based on autonomous system paths that control routing updates. Autonomous system paths are based on eBGP autonomous paths information. Access lists are filters that restrict the routing information that a router learns or advertises to and from a neighbor. Multiple eBGP peers or route maps can reference a single access list. These access lists can be applied to both inbound and outbound route updates. Each route update is passed through the access list. eBGP applies each rule in the access list in the order it appears in the list. When a route matches a rule, the decision to permit the route through or deny the route from the filter is made, and no further rules are processed. A regular expression is a pattern used to match against an input string. In eBGP, regular expression can be built to match information about an autonomous system path.

Syntax	[no] ip as-path access-list WORD <deny permit> .LINE
Authority	Admin user.
<WORD>	The access list name, up to 80 chars.
<deny>	Denies access for matching conditions.
<permit>	Permits access for matching conditions.
<.LINE>	An autonomous system in the access list in the form of a regular expression, up to 80 chars.
<no>	Disables an access list rule.

Examples

```
s1(config)#ip as-path access-list 1 permit _234_
s1(config)#ip as-path access-list 1 permit _345_
s1(config)#ip as-path access-list 1 deny any
```

5.9.24. route-map

This command configures the order of the entry in the route map name with either the permit or deny match policy.

Syntax	[no] route-map WORD <deny permit> <order>
Authority	Admin user.
<WORD>	The route map name, up to 80 chars.
<order>	The order number of the route map, 1-65535.
<deny>	Denies the order of the entry.
<permit>	Permits the order of the entry
<no>	Deletes the route map.

Examples

```
s1(config)# route-map ex-pbr-1 permit 1
```

```
s1(config)# match ip address access-list pbr
s1(config)# set ip next-hop 1.1.1.1
```

5.9.25. match as-path

This command matches an eBGP autonomous system path access list.

Syntax [no] match as-path WORD
Authority Admin user.
<WORD> The AS path access list name.
<no> Deletes the AS path access list entry.

Examples

```
s1(config-route-map)# match as-path WORD
s1(config-route-map)# no match as-path WORD
s1(config-route-map)# no match as-path
```

5.9.26. match community

This command matches an eBGP community. Use this command in route-map configuration mode.

Syntax [no] match community (<1-99>|<100-500>|WORD)
Authority Admin user.
<1-99> The community list number (standard).
<100-500> The community list number (expanded).
<WORD> The community list name.
<no> Removes the match community entry.

Examples

```
s1(config-route-map)# match community 10
s1(config-route-map)# no match community 10
s1(config-route-map)# no match community
```

5.9.27. match community exact-match

This command matches an eBGP community with an exact match of communities.

Syntax [no] match community (<1-99>|<100-500>|WORD) exact-match
Authority Admin user.
<1-99> The community list number (standard).
<100-500> The community list number (expanded).
<WORD> The community list name.
<Exact-match> Does exact matching of communities.

<no> Removes the match community exact-match entry.

Examples

```
s1(config-route-map)# match community c1 exact-match
s1(config-route-map)# no match community c1 exact-match
```

5.9.28. match extcommunity

This command matches the eBGP extended community list attributes. Use this command in route-map mode.

Syntax [no] match extcommunity (<1-99>|<100-500>|WORD)
Authority Admin user.
<1-99> The extended community list number (standard).
<100-500> The extended community list number (expanded).
<WORD> The extended community list name.
<no> Removes the match extcommunity entry.

Examples

```
s1(config-route-map)# match extcommunity 10
s1(config-route-map)# no match extcommunity 10
s1(config-route-map)# no match extcommunity
```

5.9.29. match ip address prefix-list

To distribute any routes that have a destination network number address that is permitted by a prefix list.

Syntax [no] match ip address prefix-list WORD
Authority Admin user.
<WORD> The IP prefix list name.
<no> Removes the match ip address prefix-list entry.

Examples

```
s1(config-route-map)# match ip address prefix-list p11
s1(config-route-map)# no match ip address prefix-list p11
s1(config-route-map)# no match ip address prefix-list
```

5.9.30. match ipv6 address prefix-list

This command distributes IPv6 routes that have a prefix specified in an IPv6 prefix list.

Syntax [no] match ipv6 address prefix-list WORD
Authority Admin user.
<WORD> The IPv6 prefix list.

<no> Removes the match ipv6 address prefix-list entry.

Examples

```
s1(config-route-map)# match ipv6 address prefix-list p1
s1(config-route-map)# no match ipv6 address prefix-list p1
```

5.9.31. match ipv6 next-hop

This command distributes IPv6 routes that have a specified next hop.

Syntax [no] match ipv6 next-hop X:X::X:X
Authority Admin user.
<X:X::X:X> The IPv6 address of the next hop.
<no> Removes the match ipv6 next-hop entry.

Examples

```
s1(config-route-map)# match ipv6 next-hop 2001::1
s1(config-route-map)# no match ipv6 next-hop 2001::1
```

5.9.32. match metric

This command redistributes routes with the specified metric.

Syntax [no] match metric <0-4294967295>
Authority Admin user.
<0-4294967295> The metric value.
<no> Removes the match metric entry.

Examples

```
s1(config-route-map)# match metric 400
s1(config-route-map)# no match metric 400
s1(config-route-map)# no match metric
```

5.9.33. match origin

This command matches eBGP routes based on the origin of the specified route.

Syntax [no] match origin (egp|igp|incomplete)
Authority Admin user.
<EGP> Remote egp.
<IGP> Local igp.
<Incomplete> Unknown heritage.
<no> Removes the match origin entry.

Examples

```
s1(config-route-map)# match origin egp
s1(config-route-map)# no match origin egp
s1(config-route-map)# no match origin
```

5.9.34. match probability

This command matches the portion of eBGP routes defined by a percentage value.

Syntax [no] match probability <0-100>
Authority Admin user.
<0-100> Percentage of routes.
<no> Removes the match probability entry.

Examples

```
s1(config-route-map)# match probability 50
s1(config-route-map)# no match probability 50
s1(config-route-map)# no match probability
```

5.9.35. Route-map set

The set community command sets the eBGP community attribute. The set metric command sets the eBGP attribute MED.

Syntax Route-map Command: [no] set community <AA:NN> [additive]
Syntax Route-map Command: [no] set metric <val>
Authority Admin user.
<AA:NN> Sets the eBGP community attribute. AS1:AS2 where AS is an integer in the range <1-4294967295>.
<val> Sets the metric value in the range <0-4294967295>.
<no> Clears the community attribute.

Examples

```
s1(config)# route-map RMAP1 deny 1
s1(config-route-map)# set community 6001:7002 additive
s1(config-route-map)# set metric 100
s1(config-route-map)# no set metric 100
```

5.9.36. set aggregator

This command sets the originating AS of an aggregated route. The value specifies from which AS the aggregate route originated. The range is from 1 to 4294967295. The set-aggregator-ip value must also be set to further identify the originating AS.

Syntax [no] set aggregator as <value> <A.B.C.D>
Authority Admin user.
<value> The AS value. Integer in the range <1-4294967295>.

- <A.B.C.D> The IPv4 address of AS.
<no> Clears the aggregator configuration for the route map.

Examples

```
s1(config)# route-map RMAP1 deny 1
s1(config-route-map)#set aggregator as 1 10.1.2.1
```

5.9.37. set as-path exclude

This command excludes the given AS number from the AS_PATH.

- Syntax** [no] set as-path exclude .<value>
Authority Admin user.
<value> The AS value to be excluded from the AS_PATH. Integer in the range <1-4294967295>.
<no> Clears the AS value exclusion from the AS_PATH.

Examples

```
s1(config)# route-map RMAP1 deny 1
s1(config-route-map)#set as-path exclude 2
```

5.9.38. set as-path prepend

This command prepends the given AS number to the AS_PATH.

- Syntax** [no] set as-path prepend .<value>
Authority Admin user.
<value> The AS value to be added to the AS_PATH. Integer in the range <1-4294967295>.
<no> Clears the AS value from the AS_PATH.

Examples

```
s1(config)# route-map RMAP1 deny 1
s1(config-route-map)#set as-path prepend 2
```

5.9.39. set atomic-aggregate

This command enables a warning to upstream routers, through the ATOMIC_AGGREGATE attribute, that address aggregation has occurred on an aggregate route.

- Syntax** [no] set atomic-aggregate
Authority Admin user.
<no> Disables the route-aggregation notification to upstream routers.

Examples

```
s1(config)# route-map RMAP1 deny 1
```

```
s1(config-route-map)#set atomic-aggregate
```

5.9.40. set comm-list delete

This command removes the COMMUNITY attributes from the eBGP routes identified in the specified community list. It also deletes matching communities for the route map.

Syntax [no] set comm-list <list-name> delete
Authority Admin user.
<list-name> The community list name. Integer in the range <1-99> or <100-500>, or a valid community string not exceeding 80 characters.
<no> Deletes the community list exclusion under the route map.

Examples

```
s1(config)# route-map RMAP1 deny 1  
s1(config-route-map)#set comm-list 1 delete
```

5.9.41. set community

This command sets the COMMUNITY attributes for route-map. The community number may be one of the following:

- aa:nn format
- local-AS|no-advertise|no-export|internet
- Additive
- None

Syntax [no] set community <list-name>
Authority Admin user.
<list-name> The community list name. An integer in the range <1-99> or <100-500>, or a valid community string not exceeding 80 characters.
<no> Deletes the community list configuration under the route map.

Examples

```
s1(config)# route-map RMAP1 deny 1  
s1(config-route-map)#set community 6000:100
```

5.9.42. set community rt

This command sets the target extended community (in decimal notation) of an eBGP route. The COMMUNITY attribute value has the syntax AA:NN, where AA represents an AS or IP address, and NN is the community identifier.

Syntax [no] set extcommunity rt <asn-community-identifier>
Authority Admin user.

<asn-community-identifier> The community attribute in the form of AA:nn or IP address:nn.

<no> Deletes the configuration for the rt extended community list under the route map.

Examples

```
s1(config)# route-map RMAP1 deny 1
s1(config-route-map)#set extcommunity rt 6000:100
s1(config-route-map)#set extcommunity rt 10.1.2.1:100
```

5.9.43. set extcommunity soo

This command sets the site-of-origin extended community (in decimal notation) of an eBGP route. The COMMUNITY attribute value has the syntax AA:NN, where AA represents an AS or IP address, and NN is the community identifier.

Syntax [no] set extcommunity soo <asn-community-identifier>

Authority Admin user.

<asn-community-identifier> The community attribute in the form of AA:nn or IP address:nn.

<no> Deletes the configuration for the site-of-origin extended community list under the route map.

Examples

```
s1(config)# route-map RMAP1 deny 1
s1(config-route-map)#set extcommunity soo 6000:100
s1(config-route-map)#set extcommunity soo 10.1.2.1:100
```

5.9.44. set ipv6 next-hop global

This command sets the eBGP-4+ global IPv6 next hop address.

Syntax [no] set ipv6 next-hop global <X:X::X:X>

Authority Admin user.

<X:X::X:X> The IPv6 address.

<no> Unsets the eBGP-4+ global IPv6 next hop address for the route map.

Examples

```
s1(config)# route-map RMAP1 deny 1
s1(config-route-map)#set ipv6 next-hop global 2001:db8:0:1
```

5.9.45. set local-preference

This command sets the BGP local preference and the local preference value of an IBGP route. The value is advertised to IBGP peers. The range is from 0 to 4294967295. A higher number signifies a preferred route among multiple routes to the same destination.

Syntax	[no] set local-preference <value>
Authority	Admin user.
<value>	The value of an IBGP route.
<no>	Unsets the BGP local preference for the route map.

Examples

```
s1(config)# route-map RMAP1 deny 1
s1(config-route-map)#set local-preference 1
```

5.9.46. set metric

This command specifies the relative change of metric which is used with eBGP route advertisement. This command takes the route's current metric and increases or decreases it by a specified value before it is propagated. If the value is specified as negative and ends up being negative after the metric decrease, the value is interpreted as an increase in metric.

Syntax	[no] set metric <expr>
Authority	Admin user.
<expr>	The metric expression.
<no>	Unsets the eBGP local preference for the route map.

Examples

```
s1(config)# route-map RMAP1 deny 1
s1(config-route-map)#set metric +2
```

```
s1(config)# route-map RMAP1 deny 1
s1(config-route-map)#set metric -367
In this case -367 is treated as +367.
```

5.9.47. set origin

This command sets the ORIGIN attribute of a local eBGP route to one of the following:

- **egp**: Sets the value to the Network Layer Reachability Information (NLRI) learned from the Exterior Gateway Protocol (EGP).
- **igp**: Sets the value to the NLRI learned from a protocol internal to the originating AS.
- **incomplete**: If the value is not **egp** or **igp**.

Syntax	[no] set origin <egp igp incomplete>
Authority	Admin user.
<egp>	Specifies the type-1 metric.
<igp>	Specifies the type-2 metric.
<incomplete>	Specifies the type-2 metric.
<no>	Unsets the eBGP origin attribute for the route map.

Examples

```
s1(config)# route-map RMAP1 deny 1
s1(config-route-map)#set origin egp
```

5.9.48. set weight

This command sets the weight of an eBGP route. A route's weight has the most influence when two identical eBGP routes are compared. A higher number signifies a greater preference.

Syntax [no] set weight <value>
Authority Admin user.
<value> The weight value. Integer in the range <1-4294967295>.
<no> Unsets the weight attribute for the route map.

Examples

```
s1(config)# route-map RMAP1 deny 1
s1(config-route-map)# set weight 9
```

5.9.48.1. Route-map description

This command sets the route-map description.

Syntax [no] description <text>
Authority Admin user.
<text> The route-map description. Up to 80 chars.
<no> Clears the description for the route map.

Examples

```
s1(config)# route-map RMAP1 deny 1
s1(config-route-map)# description rmap-mcast
```

5.9.49. Route-map call

This command jumps to another route map after match and set.

Syntax [no] call WORD
Authority Admin user.
<WORD> The target route map name.
<no> Disables jumping to another route map.

Examples

```
s1(config-route-map)# call rmap
s1(config-route-map)# no call
```

5.9.50. Route-map continue

This command continues onto a different entry within the route map.

Syntax	[no] continue <1-65535>
Authority	Admin user.
<1-65535>	The route map entry sequence number.
<no>	Disables continuing onto a different entry.

Examples

```
s1(config-route-map)# continue 300
s1(config-route-map)# no continue 300
s1(config-route-map)# no continue
```

5.9.51. IPv4 prefix-list

The ip prefix-list command provides a powerful prefix-based filtering mechanism. It has prefix length range and sequential number specifications. You can add or delete prefix-based filters to arbitrary points of a prefix-list by using a sequential number specification. If no ip prefix-list is specified, it acts as a permit. If the ip prefix-list is defined, and no match is found, the default deny is applied.

Syntax	[no] ip prefix-list WORD seq <num> (deny permit) <A.B.C.D/M any>
Syntax	[no] ip prefix-list WORD seq <num> (deny permit) A.B.C.D/M le <0-32> ge <0-32>
Syntax	[no] ip prefix-list WORD seq <num> (deny permit) A.B.C.D/M ge <0-32>
Syntax	[no] ip prefix-list WORD seq <num> (deny permit) A.B.C.D/M le <0-32>
Authority	Admin user.
<WORD>	The IP prefix-list name. String of maximum length 80 characters.
<num>	The sequence number. 1-4294967295
<A.B.C.D/M>	The IPv4 prefix.
<0-32>	Minimum prefix length to be matched.
<0-32>	Maximum prefix length to be matched.
<no>	Deletes the IP prefix-list.

Examples

```
s1(config)# ip prefix-list PLIST1 seq 5 deny 10.1.1.0/24
s1(config)# ip prefix-list PLIST2 seq 10 permit 10.2.2.0/24
s1(config)# no ip prefix-list PLIST1 seq 5 deny 10.3.2.0/24
s1(config)# no ip prefix-list PLIST2
```

5.9.52. IPv6 prefix-list

The ipv6 prefix-list command provides IPv6 prefix-based filtering mechanism. Descriptions may be added to prefix lists. The description command adds a description to the prefix list. The ge

command specifies prefix length, and the prefix list is applied if the prefix length is greater than or equal to the ge prefix length. The le command specifies prefix length, and the prefix list is applied if the prefix length is less than or equal to the le prefix length. If no ipv6 prefix-list is specified, it acts as permit. If ipv6 prefix-list is defined, and no match is found, the default deny is applied.

Syntax	[no] ipv6 prefix-list WORD description .LINE
Syntax	[no] ipv6 prefix-list WORD seq <num> <deny permit> <X::X:X/M any>
Syntax	[no] ipv6 prefix-list WORD seq <num> <deny permit> <X::X:X/M> ge <length>
Syntax	[no] ipv6 prefix-list WORD seq <num> <deny permit> <X::X:X/M> ge <length> le <length>
Syntax	[no] ipv6 prefix-list WORD seq <num> <deny permit> <X::X:X/M> le <length>
<WORD>	The IP prefix-list name. String of maximum length of 80 characters.
<num>	The sequence number. 1-4294967295
<.LINE>	The prefix list description. String of maximum length 80 characters.
<X::X:X/M>	The IPv6 prefix.
<length>	The prefix length. 0-128
<no>	Deletes the IPv6 prefix-list.

Examples

```
s1(config)# ipv6 prefix-list COMMON-PREFIXES description prefixes
s1(config)# no ipv6 prefix-list COMMON-PREFIXES
s1(config)# ipv6 prefix-list COMMON-PREFIXES seq 5 permit 2001:0DB8:0000::/48
s1(config)# ipv6 prefix-list COMMON-PREFIXES seq 10 deny any
s1(config)# ipv6 prefix-list COMMON-PREFIXES seq 15 permit 2001:0DB8:0000::/48 ge 64
s1(config)# no ipv6 prefix-list COMMON-PREFIXES
s1(config)# ipv6 prefix-list PEER-A-PREFIXES seq 5 permit 2001:0DB8:AAAA::/48 ge 64
s1(config)# no ipv6 prefix-list PEER-A-PREFIXES
```

5.9.53. Community lists configuration commands

This command defines a new community list. LINE is a string expression of the communities attribute. LINE can include a regular expression to match the communities attribute in eBGP updates. The community is compiled into a community structure. Multiple community lists can be defined under the same name. In that case, the match happens in user-defined order. Once the community list matches to the communities attribute in eBGP updates, it returns a permit or deny based on the community list definition. When there is no matched entry, deny is returned. When the community is empty, the system matches to any routes.

Syntax	[no] ip community-list WORD <deny permit> .LINE
Authority	Admin user.
<WORD>	The community list name.
<deny>	Denies access for matching conditions.
<permit>	Permits access for matching conditions.
<.LINE>	Community numbers specified as regular expressions.
<no>	Deletes the rule for the specified community.

Examples

```
S1(config)#ip community-list EXPANDED permit [1-2]00
S1(config)#ip community-list ANY-COMMUNITIES deny ^0:.*_
S1(config)#ip community-list ANY-COMMUNITIES deny ^65000:.*_
S1(config)#ip community-list ANY-COMMUNITIES permit .*
```

5.9.54. Extended community lists configuration commands

This command defines a new extended community list. LINE is a string expression of the extended communities attribute, and can include a regular expression to match the extended communities attribute in eBGP updates.

Syntax [no] ip extcommunity-list WORD <deny|permit> .LINE
Authority Admin user.
<WORD> The extended community list name.
<.LINE> The string expression of the extended communities attribute.
<deny> Denies access for matching conditions.
<permit> Permits access for matching conditions.
<no> Deletes the extended community list.

Examples

```
s1(config)# ip extcommunity-list expanded ROUTES permit REGULAR_EXPRESSION
s1(config)# no ip extcommunity-list expanded ROUTES
```

5.9.55. show ip bgp

This command displays eBGP routes from the BGP route table. When no route is specified, all IPv4 routes are displayed.

Syntax show ip bgp [A.B.C.D][A.B.C.D/M]
Authority Admin user.
<A.B.C.D> The IPv4 prefix.
<A.B.C.D/M> The IPv4 prefix with prefix length.

Examples

```
s1# show ip bgp
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
Local router-id 10.1.2.1
  Network          Next Hop          Metric LocPrf Weight Path
*> 10.1.2.0/24     0.0.0.0           0      0   32768  i
*> 10.2.3.0/24     10.10.10.2        0      0       0 2 5  i
```

```
* 10.3.4.0/24      10.20.20.2      0      0      0 3 5 i
* 10.4.5.0/24      10.30.30.2      0      0      0 4 5 i
Total number of entries 4
```

5.9.56. show ip bgp summary

The command provides a summary of the eBGP neighbor status.

Syntax show ip bgp summary

Authority Admin user.

Examples

```
s1# show ip bgp summary
BGP router identifier 10.1.2.1, local AS number 1
RIB entries 2
Peers 1
```

Neighbor	AS	MsgRcvd	MsgSent	Up/Down	State
10.1.2.1	2	4	5	00:00:28	Established

5.9.57. show bgp neighbors

This command displays detailed information about eBGP neighbor connections.

Syntax show bgp neighbors

Authority Admin user.

Examples

```
s1# show bgp neighbors
name: 10.1.2.1, remote-as: 6002
  state: undefined
  shutdown: yes
  description: peer1
  capability: undefined
  local_as: undefined
  local_interface: undefined
  inbound_soft_reconfiguration: yes
  maximum_prefix_limit: undefined
  tcp_port_number: undefined
  statistics:
name: pgl, remote-as: undefined
  state: undefined
  shutdown: undefined
  description: undefined
  capability: undefined
  local_as: undefined
  local_interface: undefined
  inbound_soft_reconfiguration: undefined
  maximum_prefix_limit: undefined
```

```
tcp_port_number: undefined
statistics:
```

5.9.58. show ip bgp route-map WORD

This command displays route-map set and match attributes.

Syntax show ip bgp route-map WORD

Authority Admin user.

<WORD> Route-map name.

Examples

```
s1# show ip bgp route-map BGP_IN
BGP route map table entry for BGP_IN
Entry 1:
  action : permit
  Set parameters :
  metric : 4
  aggregator_as : 1 10.1.2.1
  as_path_prepend : 1 1
  atomic_aggregate : true
  comm_list : test delete
  ipv6_next_hop_global : 2001::4
  local_preference : 33
  origin : egp
  weight : 44
  Match parameters :
```

```
s2# show ip bgp route-map BGP_OUT
BGP route map table entry for BGP_OUT
Entry 1:
  action : permit
  Set parameters :
  Match parameters :
  as_path : test
  origin : egp
  metric : 4
  probability : 20
```

5.9.59. show ip prefix list

This command displays all ip prefix list configurations.

Syntax show ip prefix list

Authority Admin user.

Examples

```
s1# show ip prefix-list
```

```
ip prefix-list BGP_IN_ : 5 entries
seq 5 deny 10.1.1.0/24
seq 10 permit 10.2.2.0/24
seq 15 permit 172.16.15.0/20 ge 21 le 28
seq 20 permit 192.168.15.0/16 ge 19
seq 25 deny 192.168.15.0/16 le 25
```

5.9.60. show ip prefix-list WORD seq num

This command displays ip prefix list configuration with a specific name and sequence number.

Syntax show ip prefix list WORD seq <num>
Authority Admin user.
<WORD> The IP prefix-list name.
<num> The sequence number. 1-4294967295.

Examples

```
s1# show ip prefix-list BGP_IN_ seq 10
seq 10 permit 10.1.0.0/24
```

5.9.61. show ip prefix list detail WORD

This command displays the detailed IP prefix list configuration with a specific name.

Syntax show ip prefix-list detail WORD
Authority Admin user.
<WORD> The IP prefix-list name.

Examples

```
s1# show ip prefix-list detail BGP_IN_
ip prefix-list BGP_IN_:
count: 5, sequences: 5 - 25
seq 5 deny 10.1.0.0/24
seq 10 permit 10.2.0.0/24
seq 15 permit 172.16.15.0/20 ge 25 le 28
seq 20 permit 192.168.15.0/16 ge 27
seq 25 deny 192.168.15.0/16 le 25
```

5.9.62. show ip prefix list summary WORD

This command displays the summarized ip prefix list configuration with a specific name.

Syntax show ip prefix-list summary WORD
Authority Admin user.
<WORD> The IP prefix-list name.

Examples

```
s1# show ip prefix-list summary BGP_IN_  
ip prefix-list BGP_IN_  
count: 5, sequences: 5 - 25
```

5.9.63. show ipv6 prefix list

This command displays all ipv6 prefix list configurations.

Syntax show ipv6 prefix list

Authority Admin user.

Examples

```
s1# show ipv6 prefix-list  
ipv6 prefix-list BGP_IN: 5 entries  
Description: IPV6 Prefix Test  
seq 10 deny 9966:1:2::/64 ge 80 le 100  
seq 20 permit 7d5d:1:1::/64 le 70  
seq 30 permit 5d5d:1:1::/64 le 70  
seq 40 permit 2ccd:1:1::/64 ge 65  
seq 50 permit 4ddc:1:1::/64
```

5.9.64. show ipv6 prefix list WORD

This command displays ipv6 prefix list configuration with a specific name.

Syntax show ipv6 prefix list WORD

Authority Admin user.

<WORD> The IPv6 prefix-list name.

Examples

```
s1# show ipv6 prefix-list BGP_IN  
ipv6 prefix-list BGP_IN: 5 entries  
Description: IPV6 Prefix Test  
seq 10 deny 9966:1:2::/64 ge 80 le 100  
seq 20 permit 7d5d:1:1::/64 le 70  
seq 30 permit 5d5d:1:1::/64 le 70  
seq 40 permit 2ccd:1:1::/64 ge 65  
seq 50 permit 4ddc:1:1::/64
```

5.9.65. show ipv6 prefix-list WORD seq num

This command displays the ipv6 prefix list configuration with the specific name and sequence number.

Syntax show ipv6 prefix list <WORD> seq <num>

Authority Admin user.

<WORD> The IPv6 prefix-list name.

<num> The sequence number, 1-4294967295.

Examples

```
s1# show ipv6 prefix-list BGP_IN seq 10
   seq 10 deny 9966:1:2::/64 ge 80 le 100
```

5.9.66. show ipv6 prefix list detail

This command displays the detailed IP prefix list configuration.

Syntax show ipv6 prefix-list detail

Authority Admin user.

Examples

```
s1# show ipv6 prefix-list detail
ipv6 prefix-list BGP_IN:
  Description: IPV6 Prefix Test
  count: 5, sequences: 10 - 50
  seq 10 deny 9966:1:2::/64 ge 80 le 100
  seq 20 permit 7d5d:1:1::/64 le 70
  seq 30 permit 5d5d:1:1::/64 le 70
  seq 40 permit 2ccd:1:1::/64 ge 65
  seq 50 permit 4ddc:1:1::/64
```

5.10. show ipv6 prefix list detail WORD

This command displays the detailed IP prefix list configuration with a specific name.

Syntax show ipv6 prefix-list detail WORD
Authority Admin user.
<WORD> The IPv6 prefix-list name.

Examples

```
s1# show ipv6 prefix-list detail BGP_IN
ipv6 prefix-list BGP_IN:
  Description: IPV6 Prefix Test
  count: 5, sequences: 10 - 50
  seq 10 deny 9966:1:2::/64 ge 80 le 100
  seq 20 permit 7d5d:1:1::/64 le 70
  seq 30 permit 5d5d:1:1::/64 le 70
  seq 40 permit 2ccd:1:1::/64 ge 65
  seq 50 permit 4ddc:1:1::/64
```

5.10.1. show ipv6 prefix list summary

This command displays the summarized ipv6 prefix list configuration.

Syntax show ipv6 prefix-list summary
Authority Admin user.

Examples

```
s1# show ipv6 prefix-list summary
ipv6 prefix-list BGP_IN:
  Description: IPV6 Prefix Test
  count: 5, sequences: 10 - 50
```

5.10.2. show ipv6 prefix list summary WORD

This command displays the summarized ipv6 prefix list configuration with a specific name.

Syntax show ipv6 prefix-list summary WORD
Authority Admin user.
<WORD> The IPv6 prefix-list name.

Examples

```
s1# show ipv6 prefix-list summary BGP_IN
ipv6 prefix-list BGP_IN:
  Description: IPV6 Prefix Test
  count: 5, sequences: 10 - 50
```

5.10.3. show ipv6 prefix list WORD X:X::X:X/M

This command displays the ipv6 prefix list configuration with a specific name and ipv6 address.

Syntax show ipv6 prefix list WORD X:X::X:X/M
Authority Admin user.
<WORD> The IP prefix-list name.
<X:X::X:X/M> The IPv6 address with prefix length M.

Examples

```
s1# show ipv6 prefix-list BGP_IN 9966:1:2::/64
seq 10 deny 9966:1:2::/64 ge 80 le 100
seq 80 permit 9966:1:2::/64 ge 110
```

5.10.4. show ipv6 prefix list WORD X:X::X:X/M first-match

This command displays the first ipv6 prefix list configuration with a specific name and ipv6 address.

Syntax show ipv6 prefix list WORD first-match
Authority Admin user.
<WORD> The IP prefix-list name.
<X:X::X:X/M> The IPv6 address with prefix length M.

Examples

```
s1# show ipv6 prefix-list BGP_IN 9966:1:2::/64 first-match
seq 10 deny 9966:1:2::/64 ge 80 le 100
```

5.10.5. show ipv6 prefix list WORD X:X::X:X/M longer

This command displays the ipv6 prefix list configuration with a specific name, ipv6 address, and prefix-length greater than or equal to M.

Syntax show ipv6 prefix list WORD longer.
Authority Admin user.
<WORD> The IP prefix-list name.
<X:X::X:X/M> The IPv6 address with prefix length M.

Examples

```
s1# show ipv6 prefix-list BGP_IN 9966:1:2::/64 longer
seq 10 deny 9966:1:2::/64 ge 80 le 100
seq 60 permit 9966:1:2::/70
seq 80 permit 9966:1:2::/64 ge 110
```

5.10.6. show ip community list

This command displays all community list configurations.

Syntax show ip community list

Authority Admin user.

Examples

```
s1# show ip community-list
ip community-list BGPclist
  permit 2:0
  deny 4:0
```

5.10.7. show ip extcommunity list

This command displays all extended community list configuration.

Syntax show ip extcommunity list

Authority Admin user.

Examples

```
s1# show ip extcommunity-list
ip extcommunity-list BGPclist
  permit 2:0
  deny 4:0
```

5.10.8. show as-path access list

This command displays all as-path access list configuration.

Syntax show ip as-path-access-list

Authority Admin user.

Examples

```
s1# show ip as-path-access-list
ip as-path access-list BGP_Filter
  permit 3
  deny 2
```

5.10.9. show as-path access list WORD

This command displays the as-path access list configuration with a specific name.

Syntax show ip as-path-access-list WORD

Authority Admin user.

<WORD> The as-path-access-list name. String of 80 characters maximum length.

Examples

```
s1# show ip as-path-access-list BGP_Filter
ip as-path access-list BGP_Filter
  permit 3
  deny 2
```

5.11. OSPFv2 commands

In vtysh every command belongs to a particular context.



Not all of these commands are implemented, some of them are reserved for the later release.

5.11.1. Create OSPF instance

This command creates the OSPF instance (if not created already) and enters the *router ospf* context.

Syntax router ospf
Authority All users.

Examples

```
switch# configure terminal
switch# router ospf
```

5.11.2. Remove OSPF instance

This command removes the OSPF instance.

Syntax no router ospf
Authority All users.

Examples

```
switch# configure terminal
switch# no router ospf
```

5.11.3. Set router ID

This command sets an id for the router in an IPv4 address format.

Syntax router-id <router_address>
Authority All users.
<router_address> Router id in IPv4 address format.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# router-id 1.1.1.1
```

5.11.4. Set router ID to default

This command unconfigures the router-id for the instance. The Router-id is changed to the global router-id, if configured. Otherwise, it is changed to the dynamically selected router-id.

Syntax no router-id

Authority All users.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# no router-id
```

5.11.5. Set OSPF network for the area

This command will run the OSPF protocol on the configured network address. The interfaces which have an IP address configured in this network or in a subset of this network, will participate in the OSPF protocol.

Syntax network <network_prefix> area (<area_ip>|<area_id>)

Authority All users.

<network_prefix> Specify the network prefix for the area.

<area_ip> OSPF area identifier in IPv4 address format.

<area_id> Pass the OSPF area identifier as a decimal value, 0-4294967295.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# network 10.10.10.0/24 area 1
switch(config-router)# network 100.10.10.0/24 area 0.0.0.2
```

5.11.6. Unset OSPF network for the area

This command disables OSPF on the network. The interfaces which have an IP address configured in this network or in a subset of this network, will stop participating in the OSPF protocol.

Syntax no network <network_prefix> area (<area_ip>|<area_id>)

Authority All users.

<network_prefix> Specify the network prefix for the area.

<area_ip> OSPF area identifier in IPv4 address format.

<area_id> Pass the OSPF area identifier as a decimal value, 0-4294967295.

Examples

```
switch# configure terminal
```

```
switch# router ospf
switch(config-router)# no network 10.10.10.0/24 area 1
switch(config-router)# no network 100.10.10.0/24 area 0.0.0.2
```

5.11.7. Enable OSPF area authentication

This command enables authentication for an area.

Syntax area (<area_ip>|<area_id>) authentication [message-digest]
Authority All users.
<area_ip> OSPF area identifier in IPv4 address format.
<area_id> Pass the OSPF area identifier as a decimal value, 0-4294967295.
<authentication> Enable authentication for the area with a simple password.
<message-digest> Enable message-digest authentication.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# area 1 authentication
switch(config-router)# area 0.0.0.2 authentication
switch(config-router)#
switch(config-router)# area 0.0.0.2 authentication message-digest
switch(config-router)#
```

5.11.8. Disable OSPF area authentication

This command disables authentication for an area.

Syntax no area (<area_ip>|<area_id>) authentication
Authority All users.
<area_ip> OSPF area identifier in IPv4 address format.
<area_id> Pass the OSPF area identifier as a decimal value, 0-4294967295.
<authentication> Disable authentication for the area.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router) no area 1 authentication
switch(config-router)
```

5.11.9. Set cost for default LSA summary

This command sets the cost of default-summary LSAs announced to NSSA or the stub areas.

Syntax	area (<area_ip> <area_id>) default-cost <cost>
Authority	All users.
<area_ip>	OSPF area identifier in IPv4 address format.
<area_id>	Pass the OSPF area identifier as a decimal value, 0-4294967295.
<default-cost>	Sets the cost of default-summary LSAs announced to NSSA or the stub areas.
<cost>	Cost of default-summary LSAs announced to the stubby areas, 0-16777215.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# area 1 default-cost 2
switch(config-router)# area 0.0.0.2 default-cost 2
switch(config-router)#
```

5.11.10. Set cost for default LSA summary to default

This command resets the cost of the default-summary LSAs announced to NSSA or stub areas, to the default. The default value is one.

Syntax	no area (<area_ip> <area_id>) default-cost [<cost>]
Authority	All users.
<area_ip>	OSPF area identifier in IPv4 address format.
<area_id>	Pass the OSPF area identifier as a decimal value, 0-4294967295.
<default-cost>	Sets the cost of the default-summary LSAs announced to NSSA or stub areas, to default.
<cost>	Configured cost of default-summary LSAs announced to the stubby areas, 0-16777215.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# no area 1 default-cost 2
switch(config-router)# no area 0.0.0.2 default-cost 2
switch(config-router)#
```

5.11.11. Set the area as NSSA

This command changes the area type to NSSA (Not So Stubby Area).

Syntax	area (<area_ip> <area_id>) nssa {translate-candidate translate-never translate-always} [no-summary]
Authority	All users.
<area_ip>	OSPF area identifier in IPv4 address format.
<area_id>	Pass the OSPF area identifier as a decimal value, 0-4294967295.

<translate-candidate>	Configure NSSA-ABR for translate election. This is the default behaviour.
<translate-never>	Configure NSSA-ABR to never translate.
<translate-always>	Configure NSSA-ABR to always translate.
<nssa>	Configure OSPF area as NSSA.
<no-summary>	Do not inject inter-area routes into NSSA.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# area 1 nssa
switch(config-router)# area 1 nssa no-summary
switch(config-router)# area 1 nssa translate-always no-summary
switch(config-router)# area 1 nssa translate-always
switch(config-router)#
```

5.11.12. Unset the area as NSSA

This command unsets the area type as NSSA (Not So Stubby Area). That is, the configured area will not be NSSA. The no area (<area_ip>|<area_id>) nssa no_summary command enables sending inter-area routes into NSSA, but will not unset the area as NSSA.

Syntax	no area (<area_ip> <area_id>) nssa [no_summary]
Authority	All users.
<area_ip>	OSPF area identifier in IPv4 address format.
<area_id>	Pass the OSPF area identifier as a decimal value, 0-4294967295.
<nssa>	Unset area as NSSA.
<no-summary>	Inject inter-area routes into NSSA.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# no area 1 nssa
switch(config-router)# no area 1 nssa no-summary
switch(config-router)#
```

5.11.13. Configure the area as stub

This command sets the area type as stub.

Syntax	area (<area_ip> <area_id>) stub [no_summary]
---------------	--

Authority	All users.
<area_ip>	OSPF area identifier in IPv4 address format.
<area_id>	Pass the OSPF area identifier as a decimal value, 0-4294967295.
<stub>	Configure OSPF area as stub.
<no-summa- ry>	Do not inject inter-area routes into stub areas.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# area 1 stub
switch(config-router)# area 1 stub no-summary
switch(config-router)#
```

5.11.14. Unset the area as stub

This command unsets the area type as stub. This means that the configured area becomes an area type default. The no area (<area_ip>|<area_id>) stub no_summary command will stop sending inter-area routes into the stub area, but will not unset the area as stub.

Syntax	no area (<area_ip> <area_id>) stub [no_summary]
Authority	All users.
<area_ip>	OSPF area identifier in IPv4 address format.
<area_id>	Pass the OSPF area identifier as a decimal value, 0-4294967295.
<stub>	Unset area as stub.
<no-summa- ry>	Inject inter-area routes into stub areas.

5.11.15. Summarize intra-area paths

This command summarizes the routes with the matching address or masks. This command only works for border routers.

Syntax	area (<area_ip> <area_id>) range <ipv4_address> {cost <range_cost> not-advertise}
Authority	All users.
<area_ip>	OSPF area identifier in IPv4 address format.
<area_id>	Pass the OSPF area identifier as a decimal value, 0-4294967295.
<ipv4_address>	Area range prefix.
<cost>	User specified metric for this range.
<range_cost>	Metric for this range, 0-16777215.
<not-adver- tise>	Do not advertise this range to other areas.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# area 1 range 16.77.114.0/24
switch(config-router)# area 1 range 16.77.114.0/24 cost 40
switch(config-router)# area 1 range 16.77.114.0/24 not-advertise
```

5.11.16. Unset summarization

This command unsets the route summarization for the configured IPv4 prefix address on the ABR.

Syntax no area (<area_ip>|<area_id>) range <ipv4_address> {cost <range_cost> | not-advertise}

Authority All users.

<area_ip> OSPF area identifier in IPv4 address format.

<area_id> Pass the OSPF area identifier as a decimal value, 0-4294967295.

<ipv4_address> Area range prefix.

<cost> User specified metric for this range.

<range_cost> Metric for this range, 0-16777215.

<not-advertise> Do not advertise this range to other areas.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# no area 1 range 16.77.114.0/24
switch(config-router)# no area 1 range 16.77.114.0/24 cost 40
switch(config-router)# no area 1 range 16.77.114.0/24 not-advertise
```

5.11.17. Filter networks between OSPF areas

This command filters networks between OSPF areas. The filtering is done as per the prefix lists. This command is only used on area border routers.

Syntax area (<area_ip>|<area_id>) filter-list <list-name> (in|out)

Authority All users.

<area_ip> OSPF area identifier in IPv4 address format.

<area_id> Pass the OSPF area identifier as a decimal value, 0-4294967295.

<filter-list> Filter networks/routes between OSPF areas.

<list-name> Prefix list name.

<in> Filter networks sent to this area.

<out> Filter networks sent from this area.

Examples

```
switch# configure terminal
```

```
switch# router ospf
switch(config-router)# area 1 filter-list list1 in
switch(config-router)# area 1 filter-list list2 out
switch(config-router)#
```

5.11.18. Disable filtering of networks between OSPF areas

This command disables network filtering for a particular area. This command is only used on area border routers.

Syntax	no area (<area_ip> <area_id>) filter-list <list-name> (in out)
Authority	All users.
<area_ip>	OSPF area identifier in IPv4 address format.
<area_id>	Pass the OSPF area identifier as a decimal value, 0-4294967295.
<filter-list>	Stop filtering networks/routes between OSPF areas.
<list-name>	Prefix list name.
<in>	Disable filtering of networks sent to this area.
<out>	Disable filtering of networks sent from this area.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# no area 1 filter-list list1 in
switch(config-router)# no area 1 filter-list list2 out
switch(config-router)#
```

5.11.19. Configure OSPF virtual links

This command creates a virtual link with the remote ABR and optionally sets authentication type that will be used. The area (<area_ip>|<area_id>) virtual-link <remote_address> command creates an OSPF virtual link with remote ABR.

Syntax	area (<area_ip> <area_id>) virtual-link <remote_address> {authentication (message-digest null)}
Authority	All users.
<area_ip>	OSPF area identifier in IPv4 address format.
<area_id>	Pass the OSPF area identifier as a decimal value, 0-4294967295.
<virtual-link>	Configure a virtual link.
<remote_address>	Router ID of the remote ABR.
<authentication>	Select authentication type for the virtual link.
<message-digest>	Set authentication as message-digest.

<null> Use null authentication.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# area 100 virtual-link 100.0.1.1
switch(config-router)# area 100 virtual-link 100.0.1.1 authentication
message-digest
switch(config-router)# area 100 virtual-link 100.0.1.1 authentication null
```

5.11.20. Delete OSPF virtual links

This command deletes a virtual link with the remote ABR and optionally sets authentication type to the default. The `no area (<area_ip>|<area_id>) virtual-link <remote_address>` command deletes an OSPF virtual link with remote ABR.

Syntax `no area (<area_ip>|<area_id>) virtual-link <remote_address> [authentication]`

Authority All users.

<area_ip> OSPF area identifier in IPv4 address format.

<area_id> Pass the OSPF area identifier as a decimal value, 0-4294967295.

<virtual-link> Configure a virtual link to the default settings/Delete the virtual link.

<remote_address> Router ID of the remote ABR.

<authentication> Set the authentication type for virtual link to the default. By default the virtual link will have no authentication.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# no area 100 virtual-link 100.0.1.1
switch(config-router)# no area 100 virtual-link 100.0.1.1 authentication
```

5.11.21. Set OSPF virtual links authentication keys

This command sets the authentication key that is used for a particular authentication. The `area (<area_ip>|<area_id>) virtual-link <remote_address> authentication-key <auth_key>` command sets a plain text authentication key and the `area (<area_ip>|<area_id>) virtual-link <remote_address> message-digest-key <key_id> md5 <key>` command sets the message digest authentication key.

Syntax `area (<area_ip>|<area_id>) virtual-link <remote_address> [authentication-key <auth_key> | message-digest-key <key_id> md5 <key>]`

Authority All users.

<area_ip> OSPF area identifier in IPv4 address format.

<area_id> Pass the OSPF area identifier as a decimal value, 0-4294967295.

<virtual-link> Configure a virtual link.

- <remote_address> Router ID of the remote ABR.
- <authentication-key> Set authentication key for plain text authentication.
- <auth_key> Key value for authentication.
- <message-digest-key> Set authentication key for message digest authentication.
- <key_id> Key identification number, 1-255.
- <md5> Use message-digest algorithm as md5.
- <key> message-digest key string.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# area 100 virtual-link 100.0.1.1 authentication-key
opswitch
switch(config-router)# area 100 virtual-link 100.0.1.1 message-digest-key
1 md5 opswitch
```

5.11.22. Delete OSPF virtual links authentication keys

This command deletes the authentication key that is used for a particular authentication. The no area (<area_ip>|<area_id>) virtual-link <remote_address> authentication-key command deletes the plain text authentication key and the no area (<area_ip>|<area_id>) virtual-link <remote_address> message-digest-key <key_id> command deletes the message digest authentication key.

- Syntax** no area (<area_ip>|<area_id>) virtual-link <remote_address> (authentication-key | message-digest-key) [<key_id>]
- Authority** All users.
- <area_ip> OSPF area identifier in IPv4 address format.
- <area_id> Pass the OSPF area identifier as a decimal value, 0-4294967295.
- <virtual-link> Configure a virtual link.
- <remote_address> Router ID of the remote ABR.
- <authentication-key> Delete authentication key for plain text authentication.
- <message-digest-key> Delete authentication key for message digest authentication.
- <key_id> Key identification number, 1-255. This is optional, if not given deletes all the message digest keys.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# no area 100 virtual-link 100.0.1.1 authentication-key
switch(config-router)# no area 100 virtual-link 100.0.1.1 message-digest-key
```

```
switch(config-router)# no area 100 virtual-link 100.0.1.1 message-digest-key 1
```

5.11.23. Set OSPF virtual link delays and intervals

This command sets the time intervals and time delays for virtual links.

Syntax	area (<area_ip> <area_id>) virtual-link <remote_address> (hello-interval retransmit-interval transmit-delay dead-interval) <time_value>
Authority	All users.
<area_ip>	OSPF area identifier in IPv4 address format.
<area_id>	Pass the OSPF area identifier as a decimal value, 0-4294967295.
<virtual-link>	Configure a virtual link.
<remote_address>	Router ID of the remote ABR.
<hello-interval>	Set time interval between OSPF hello packets.
<retransmit-interval>	Set time between retransmitting lost link state advertisements.
<transmit-delay>	Set time delay in Link state transmission.
<dead-interval>	Set interval after which a neighbor is declared dead if no response comes.
<time_value>	Time delay/interval for the above parameters, 1-65535.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# area 100 virtual-link 100.0.1.1 hello-interval 30
switch(config-router)# area 100 virtual-link 100.0.1.1 retransmit-interval 30
switch(config-router)# area 100 virtual-link 100.0.1.1 transmit-delay 30
switch(config-router)# area 100 virtual-link 100.0.1.1 dead-interval 30
```

5.11.24. Set OSPF virtual links delay or interval to default

This command sets the time interval and delay defaults for virtual links.

Syntax	no area (<area_ip> <area_id>) virtual-link <remote_address> (hello-interval retransmit-interval transmit-delay dead-interval)
Authority	All users.
<area_ip>	OSPF area identifier in IPv4 address format.
<area_id>	Pass the OSPF area identifier as a decimal value, 0-4294967295.
<virtual-link>	Configure a virtual link.
<remote_address>	Router ID of the remote ABR.

<hello-interval>	Set time interval OSPF hello packets to the default. Default value is 10 seconds.
<retransmit-interval>	Set time between retransmitting lost link state advertisements to the default. Default value is 5 seconds.
<transmit-delay>	Set delay in Link state transmission to the default. The default value is 1 second.
<dead-interval>	Set interval after which a neighbor is declared dead, to default. The default value is 40 seconds (Generally 4 times the hello packet interval).

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# no area 100 virtual-link 100.0.1.1 hello-interval
switch(config-router)# no area 100 virtual-link 100.0.1.1 retransmit-interval
switch(config-router)# no area 100 virtual-link 100.0.1.1 transmit-delay
switch(config-router)# no area 100 virtual-link 100.0.1.1 dead-interval
```

5.11.25. Control distribution of default route information

This command controls the distribution of default route information.

Syntax

Authority All users.

<always> Always advertise the default route even if no default route in present.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# default-information originate
switch(config-router)# default-information originate always
switch(config-router)#
```

5.11.26. Disable distribution of default route information

This command disables the distribution of default route information.

Syntax no default-information originate

Authority All users.

Examples

```
switch# configure terminal
switch# router ospf
```

```
switch(config-router)# no default-information originate
switch(config-router)#
```

5.11.27. Set default metric for redistributed routes

This command sets the default metric to use for redistributed routes in the OSPF. The metric values are dependent on bandwidth, MTU, and so on.

Syntax default-metric <metric_value>

Authority All users.

<metric_value> Sets the default metric value to use for redistributed routes, 0-16777214.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# default-metric 37
```

5.11.28. Set default metric of redistributed routes to default

This command sets the default metric to be used for redistributed routes into OSPF to the default. The default value is 20.

Syntax no default-metric [metric_value]

Authority All users.

<metric_value> Sets the default metric value to use for redistributed routes, 0-16777214.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# no default-metric
switch(config-router)# no default-metric 37
```

5.11.29. Define OSPF administrative distance

This command defines an administrative distance for OSPF. Administrative distance is used as a criteria to select the best route when multiple routes are present.

Syntax distance <admin_distance>

Authority All users.

<admin_distance> OSPF administrative distance, 1-255.

Examples

```
switch# configure terminal
switch# router ospf
```

```
switch(config-router)# distance 100
```

5.11.30. Set OSPF administrative distance to default

This command sets the OSPF administrative distance to the default. The default value is 110.

Syntax no distance <admin_distance>
Authority All users.
<admin_distance> OSPF administrative distance, 1-255.

Examples

```
switch# configure terminal  
switch# router ospf  
switch(config-router)# no distance 100
```

5.11.31. Set OSPF administrative distance for a particular route type

This command sets the OSPF administrative distance for different OSPF route types.

Syntax distance ospf {intra-area <intra_area>|inter-area <inter_area>|external <ext_area>}
Authority All users.
<intra-area> OSPF administrative distance for intra area routes.
<intra_area> OSPF administrative distance, 1-255.
<inter-area> OSPF administrative distance for inter area routes.
<inter_area> OSPF administrative distance, 1-255.
<external> OSPF administrative distance for external routes.
<ext_area> OSPF administrative distance, 1-255.

Examples

```
switch# configure terminal  
switch# router ospf  
switch(config-router)# distance ospf inter-area 110  
switch(config-router)# distance ospf intra-area 110  
switch(config-router)# distance ospf external 110  
switch(config-router)# distance ospf external 110 inter-area 110
```

5.11.32. Set OSPF administrative distance for a particular route type to default

This command sets the OSPF administrative distance for different OSPF route types to the default. The default value is 110.

Syntax no distance (intra-area |inter-area |external)

- Authority** All users.
- <intra-area> OSPF administrative distance for intra area routes to the default.
- <inter-area> OSPF administrative distance for inter area routes to the default.
- <external> OSPF administrative distance for external routes to the default.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# no distance ospf inter-area
switch(config-router)# no distance ospf intra-area
switch(config-router)# no distance ospf external
```

5.11.33. Stub router advertisement

This command maximizes the cost metrics for Router LSA. The Router LSA, or type-1 LSA, has a 16-bit field (65535 in decimal) to represent the “interface output cost”. Maximizing the Router LSA will take the traffic away from the router being configured. Without any argument, maximized cost will be set administratively (indefinitely).

- Syntax** max-metric router-lsa {on-startup <time_startup>}
- Authority** All users.
- <on-startup> Automatically advertises stub Router-LSA (or maximizes the router-LSA cost metric), for specified time interval, upon OSPF startup.
- <time_startup>Time (seconds) to advertise self as stub-router, 5-86400.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# max-metric router-lsa
switch(config-router)# max-metric router-lsa on-startup 3000
```

5.11.34. Advertise normal cost metric

This command advertises the normal cost metrics instead of advertising the maximized cost metric. This setting causes the router to be considered in traffic forwarding.

- Syntax** no max-metric router-lsa (on-startup)
- Authority** All users.
- <on-startup> Does not automatically advertise the stub Router LSA (or maximize the Router LSA cost metric) during OSPF startup.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# no max-metric router-lsa
switch(config-router)# no max-metric router-lsa on-startup
```

5.11.35. Log changes in the adjacency state

This command configures the router to log the adjacency status changes. With the optional detail argument, all the changes in the adjacency status are displayed. Without the optional detail argument, only status changes to full or regressions are displayed.

Syntax log-adjacency-changes [detail]
Authority All users.
<detail> Send a syslog message for all the link state changes.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# log-adjacency-changes
switch(config-router)# log-adjacency-changes detail
```

5.11.36. Disable logging changes in the adjacency state

This command disables logging a syslog message when there is an OSPF link state change or when a neighbor goes up or down. The no log-adjacency-changes command disables logging completely.

Syntax no log-adjacency-changes [detail]
Authority All users.
<detail> Disable logging link state changes. Neighbor up or down events are still be reported.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# no log-adjacency-changes
switch(config-router)# no log-adjacency-changes detail
```

5.11.37. Enable OSPF RFC1583 compatibility

This command enables OSPF compatibility with RFC1583 (backward compatibility). If RFC1583 compatibility is enabled then the route cost calculation follows a different method.

Syntax compatible rfc1583
Authority All users.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# compatible rfc1583
```

5.11.38. Disable OSPF RFC1583 compatibility

This command disables OSPF compatibility with RFC1583 (backward compatibility). By default the RFC1583 compatibility is disabled.

Syntax no compatible rfc1583

Authority All users.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# no compatible rfc1583
```

5.11.39. Redistribute routes into OSPF

This command redistributes routes originating from other protocols to OSPF.

Syntax redistribute {bgp | connected | static}

Authority All users.

<bgp> Redistribute BGP routes into OSPF.

<connected> Redistribute connected routes (directly attached subnet or host).

<static> Redistribute static routes into OSPF.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# redistribute connected
switch(config-router)# redistribute bgp
switch(config-router)# redistribute static
```

5.11.40. Disable redistributing routes into OSPF

This command disables redistributing routes originating from other protocols to OSPF.

Syntax no redistribute {bgp | connected | static}

Authority All users.

<bgp> Redistribute BGP routes into OSPF.

<connected> Redistribute connected routes (directly attached subnet or host).

<static> Redistribute static routes into OSPF.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# no redistribute connected
switch(config-router)# no redistribute bgp
```

```
switch(config-router)# no redistribute static
```

5.11.41. OSPF BFD configuration

This command enables the Bidirectional Forwarding Detection (BFD) protocol.

The no form of this command disables the Bidirectional Forwarding Detection (BFD) protocol.

Syntax [no] bfd all-interfaces
Authority All users.
<all-inter- Apply to all OSPF interfaces
faces>

Examples

```
switch# configure terminal  
switch# router ospf  
switch(config-router)# bfd all-interfaces  
switch(config-router)# no bfd all-interfaces
```

5.11.42. Set OSPF timers

This command sets timers for the OSPF LSA. The timers lsa-group-pacing parameter configures the time interval for grouping different LSAs of the same age.

Syntax timers lsa-group-pacing <time_interval>
Authority All users.
<lsa-group- Sets the timer for LSA grouping of the same age and dropping the group when the
pacing> timer expires.
<time_interval>Time interval in seconds, 1-1800.

Examples

```
switch# configure terminal  
switch# router ospf  
switch(config-router)# timers lsa-group-pacing 75
```

5.11.43. Set OSPF timers to default

This command sets timers for the OSPF LSA to the default. The no timers lsa-group-pacing command configures the time interval for grouping different LSAs of the same age to the default.

Syntax no timers lsa-group-pacing
Authority All users.
<lsa-group- Sets the timer for LSA grouping LSAs of the same age to the default. The default
pacing> value is 10 seconds.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# no timers lsa-group-pacing
```

5.11.44. Set OSPF throttling parameters

This command sets the rate limit values for OSPF SPF calculation. The `timers throttle spf` command sets rate limits for SPF calculation. Initial SPF calculation is done after a specific delay named start time interval. After each topology change (needing SPF calculation) the hold time is doubled until the maximum hold time is reached. If there is no more topology change before the hold timer expires, then the hold time is set back to the start time interval value and the process continues. Throttling is done to avoid continuous spike in cpu usage.

Syntax `timers throttle spf <spf_delay_time> <spf_hold_time> <spf_maximum_time>`

Authority All users.

<spf> Sets the rate limit for SPF calculation.

<spf_delay_time> Set delay in milliseconds for initial SPF calculation, 1-600000.

<spf_hold_time> Set initial hold time for next SPF calculation, 1-600000.

<spf_maximum_time> Set maximum hold time for SPF calculation, 1-600000.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# timers throttle spf 100 100000 300000
```

5.11.45. Set OSPF throttling parameters to default

This command sets the rate limit values for OSPF SPF calculation to the default.

Syntax `no timers throttle spf`

Authority All users.

<spf> Sets the rate limit for SPF calculation to the default. The default start time, hold time and maximum hold time are 200, 1000 and 10000 respectively.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)# no timers throttle spf
```

5.11.46. Configure NBMA neighbor

This command specifies the NBMA neighbor and can also optionally set priority and polling interval (in seconds) for that neighbor.

Syntax `neighbor <neighbor_ip> {poll-interval <poll_value> | priority <priority_value>}`

Authority All users.

- <neighbor_ip> IP address of the neighbor.
- <poll-inter- val> Sets the dead neighbor polling interval.
- <poll_value> Polling interval value in seconds, 1-65535.
- <priority> Sets priority for the neighbor.
- <priority_value> Priority value for the neighbor, 0-255.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)#
switch(config-router)# neighbor 16.77.114.14
switch(config-router)# neighbor 16.77.114.14 poll-interval 40
switch(config-router)# neighbor 16.77.114.14 priority 20
switch(config-router)# neighbor 16.77.114.14 priority 20 poll-interval 40
```

5.11.47. Remove NBMA neighbor

This command removes a NBMA neighbor and can also reset priority and polling interval (in seconds) for that neighbor as a default.

- Syntax** no neighbor <neighbor_ip> {poll-interval | priority}
- Authority** All users.
- <neighbor_ip> IP address of the neighbor.
- <poll-inter- val> Sets the dead neighbor polling interval to the default. The default value is 60 seconds.
- <priority> Sets the neighbor priority to the default. The default value is 0.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)#
switch(config-router)# no neighbor 16.77.114.14
switch(config-router)# no neighbor 16.77.114.14 poll-interval
switch(config-router)# no neighbor 16.77.114.14 priority
```

5.11.48. Set the interface as OSPF passive interface

This command configures the interface as an OSPF passive interface. With this setting the interface does not participate in the OSPF protocol.

- Syntax** passive-interface <interface>
- Authority** All users.
- <interface> Interface name as defined by the system.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)#
switch(config-router)# passive-interface 1
```

5.11.49. Set the interface as OSPF active interface

This command resets the interface as active. With this setting the interface starts participating in the OSPF.

Syntax no passive-interface <interface>
Authority All users.
 <interface> Interface name as defined by the system.

Examples

```
switch# configure terminal
switch# router ospf
switch(config-router)#
switch(config-router)# no passive-interface 1
```

5.11.50. Enable authentication on the interface

These commands enable authentication on the interface. The ip ospf authentication null command disables authentication on the interface, in case it was enabled by area level authentication commands. The ip ospf authentication command enables simple authentication on the interface. The ip ospf authentication message-digest command enables message digest authentication on the interface. To set the key for authentication the ip ospf authentication-key <key> and ip ospf message-digest-key <key_id> md5 <message_digest_key> commands are used.

Syntax ip ospf authentication null
Syntax
Authority All users.
 <null> Disables authentication on the interface, in case it was enabled by area level authentication commands.
 <message-digest> Enables message digest authentication.
 <key> Key for authentication.
 <key_id> Key id of the authentication key, 1-255.
 <md5> Uses the md5 authentication algorithm.
 <message_digest_key> Key for message digest authentication.

Examples

```
switch# configure terminal
switch# interface 1
switch(config-if)# ip ospf authentication
switch(config-if)# ip ospf authentication-key openswitch
```

```
switch(config-if)# ip ospf authentication message-digest
switch(config-if)# ip ospf message-digest-key 1 md5 openswitch
```

5.11.51. Disable authentication on the interface

These commands disable authentication on the interface. The `no ip ospf authentication` command disables authentication on the interface completely. To unset the key for authentication use the `no ip ospf authentication-key` and `no ip ospf message-digest-key <key_id>` commands.

Syntax `no ip ospf authentication`
Syntax `no ip ospf authentication-key`
Syntax `no ip ospf message-digest-key <key_id>`
Authority All users.
<key_id> Key id of the authentication key, 1-255.

Examples

```
switch# configure terminal
switch# interface 1
switch(config-if)# no ip ospf authentication
switch(config-if)# no ip ospf authentication-key
switch(config-if)# no ip ospf message-digest-key 1
```

5.11.52. Set time interval between hello packets for the interface

This command sets interval in seconds, between hello packets.

Syntax `ip ospf hello-interval <hello_interval>`
Authority All users.
<hello_interval> Time interval in seconds, 1-65535.

Examples

```
switch# configure terminal
switch# interface 1
switch(config-if)# ip ospf hello-interval 120
```

5.11.53. Set time interval between hello packets for the interface to default

This command sets the interval between hello packets in seconds. The default value is 10 seconds.

Syntax `no ip ospf hello-interval`
Authority All users.

Examples

```
switch# configure terminal
switch# interface 1
switch(config-if)# no ip ospf hello-interval
```

5.11.54. Set neighbor dead interval for the interface

This command sets the interval in seconds, in which a neighbor connected to the interface is declared dead.

Syntax ip ospf dead-interval <dead_interval>

Authority All users.

<dead_interval> Time interval in seconds, 1-65535.

Examples

```
switch# configure terminal
switch# interface 1
switch(config-if)# ip ospf dead-interval 120
```

5.11.55. Set neighbor dead interval for the interface to default

This command sets the interval in seconds, after which a neighbor connected to the interface is declared dead to the default. The default value is 40 seconds (four times the hello-interval).

Syntax no ip ospf dead-interval

Authority All users.

Examples

```
switch# configure terminal
switch# interface 1
switch(config-if)# no ip ospf dead-interval
```

5.11.56. Disable MTU mismatch detection

This command disables the MTU mismatch detection on the interface. When the MTU value in the database description packet that is coming from a neighbor is larger than the router can handle then the packet may be dropped without this setting.

Syntax ip ospf mtu-ignore

Authority All users.

Examples

```
switch# configure terminal
switch# interface 1
```

```
switch(config-if)# ip ospf mtu-ignore
```

5.11.57. Enable MTU mismatch detection

This command enables the MTU mismatch detection on the interface. When the MTU value in the database description packet that is coming from a neighbor is larger than the router can handle, the packet may be dropped with this setting.

Syntax no ip ospf mtu-ignore

Authority All users.

Examples

```
switch# configure terminal
switch# interface 1
switch(config-if)# no ip ospf mtu-ignore
```

5.11.58. Set the interface cost

This command sets the cost (metric) associated with a particular interface. The interface cost is used as a parameter to calculate the best routes.

Syntax no ip ospf cost <interface_cost>

Authority All users.

<interface_cost> interface cost value, 1-65535.

Examples

```
switch# configure terminal
switch# interface 1
switch(config-if)# ip ospf cost 100
```

5.11.59. Set the interface cost to default

This command sets the cost (metric) associated with a particular interface to the default. The default cost is calculated automatically depending on the bandwidth of the interface.

Syntax no ip ospf cost

Authority All users.

Examples

```
switch# configure terminal
switch# interface 1
switch(config-if)# no ip ospf cost
```

5.11.60. Set OSPF network type for the interface

This command explicitly sets the network type for the interface.

Syntax ip ospf network (broadcast|point-to-point)
Authority All users.
<broadcast> Sets the OSPF network type as a broadcast multi-access network.
<point-to-point> Sets the OSPF network type as a point-to-point network.

Examples

```
switch# configure terminal
switch# interface 1
switch(config-if)# ip ospf network broadcast
switch(config-if)# ip ospf network point-to-point
```

5.11.61. Set OSPF network type for the interface to default

This command sets the network type for the interface to the system default.

Syntax no ip ospf network
Authority All users.

Examples

```
switch# configure terminal
switch# interface 1
switch(config-if)# no ip ospf network
```

5.11.62. Set the OSPF priority for the interface

This command sets the OSPF priority for the interface. The larger the numeric value of the priority, the higher the chances there is for it to become the designated router. Setting a priority of 0 makes the router ineligible to become a designated router.

Syntax ip ospf priority <priority_value>
Authority All users.
<priority_value> OSPF priority value, 0-255.

Examples

```
switch# configure terminal
switch# interface 1
switch(config-if)# ip ospf priority 50
```

5.11.63. Set the OSPF priority for the interface to default

This command sets the OSPF priority for the interface to the default. The default priority for any interface is one.

Syntax no ip ospf priority

Authority All users.

Examples

```
switch# configure terminal
switch# interface 1
switch(config-if)# no ip ospf priority
```

5.11.64. Set the retransmit interval for the interface

This command sets time interval between transmitting and then retransmitting the lost link state advertisements for the interface.

Syntax ip ospf retransmit-interval <retransmit_interval>

Authority All users.

<retransmit_interval> interval in seconds, 3-65535.

Examples

```
switch# configure terminal
switch# interface 1
switch(config-if)# ip ospf retransmit-interval 10
```

5.11.65. Set the retransmit interval for the interface to default

This command sets the time interval between transmitting and then retransmitting the lost link state advertisements for the interface to the default. The default value is five seconds.

Syntax no ip ospf retransmit-interval

Authority All users.

Examples

```
switch# configure terminal
switch# interface 1
switch(config-if)# no ip ospf retransmit-interval
```

5.11.66. Set the transmit delay for the interface

This command sets the time delay for the OSPF packet transmission. The LSA age is incremented by this value when transmitting.

Syntax ip ospf transmit-delay <transmit_delay_time>

Authority All users.

<transmit_delay_time> interval in seconds, 1-65535.

Examples

```
switch# configure terminal
switch# interface 1
switch(config-if)# ip ospf transmit-delay 10
```

5.11.67. Set the transmit delay for the interface to default

This command sets the time delay for the OSPF packet transmission to the default. The default value is one second.

Syntax no ip ospf transmit-delay
Authority All users.

Examples

```
switch# configure terminal
switch# interface 1
switch(config-if)# no ip ospf transmit-delay
```

5.11.68. Show general OSPF configurations

This command shows information on a variety of general OSPF, area, state, and configuration information.

Syntax show ip ospf [border-routers]
Authority All users.
<bor- Show information only of border-routers.
der-routers>

Examples

```
switch# show ip ospf
OSPF Routing Process, Router ID: 16.77.114.14
Supports only single TOS (TOS0) routes
This implementation conforms to RFC2328
RFC1583Compatibility flag is enabled
OpaqueCapability flag is enabled
Stub router advertisement is configured
  Enabled for 2000s after start-up
Initial SPF scheduling delay 3000 millise(c)s
Minimum hold time between consecutive SPFs 3000 millise(c)s
Maximum hold time between consecutive SPFs 5000 millise(c)s
Hold time multiplier is currently 1
Refresh timer 10 secs
This router is an ABR, This router is ASBR
Number of external LSA 0. Checksum Sum 0x00000000
Number of opaque AS LSA 0. Checksum Sum 0x00000000
```

```
Number of areas attached to this router: 2
All adjacency changes are logged
```

```
Area ID: 0.0.0.0 (Backbone)
  Number of interfaces in this area: Total: 1, Active: 1
  Number of fully adjacent neighbors in this area: 0
  Area has no authentication
  SPF algorithm last executed 24m00s ago
  SPF algorithm executed 2 times
  Number of LSA 2
  Number of router LSA 1. Checksum Sum 0x0000267e
  Number of network LSA 0. Checksum Sum 0x00000000
  Number of summary LSA 1. Checksum Sum 0x00006220
  Number of ASBR summary LSA 0. Checksum Sum 0x00000000
  Number of NSSA LSA 0. Checksum Sum 0x00000000
  Number of opaque link LSA 0. Checksum Sum 0x00000000
  Number of opaque area LSA 0. Checksum Sum 0x00000000
```

```
Area ID: 0.0.0.1
  Number of interfaces in this area: Total: 1, Active: 1
  Number of fully adjacent neighbors in this area: 1
  Area has message digest authentication
  Number of full virtual adjacencies going through this area: 0
  SPF algorithm executed 7 times
  Number of LSA 3
  Number of router LSA 2. Checksum Sum 0x00012363
  Number of network LSA 1. Checksum Sum 0x00008761
  Number of summary LSA 0. Checksum Sum 0x00000000
  Number of ASBR summary LSA 0. Checksum Sum 0x00000000
  Number of NSSA LSA 0. Checksum Sum 0x00000000
  Number of opaque link LSA 0. Checksum Sum 0x00000000
  Number of opaque area LSA 0. Checksum Sum 0x00000000
```

```
switch# show ip ospf border-routers
===== OSPF router routing table =====
R    16.77.114.14      [10] area: 0.0.0.1, ABR
      via 16.77.114.14, eth0
```

5.11.69. Show OSPF database information

This command shows the OSPF link state database summary. The `show ip ospf database` command displays the link state database overview. Use the filters as parameters to get information for a particular link state.

Syntax `show ip ospf database {asbr-summary|external|network|router|summary|nssa-external|opaque-link|opaque-area|opaque-as|max-age} [<lsa_id>] {self-originate | adv-router <router_id>}`

Authority All users.

<asbr-summary> Show ASBR summary link states (LSA type 4).

<external> Show external link states (LSA type 5).

- <network> Show network LSAs.
- <router> Show router LSAs.
- <summary> Show network-summary link states (LSA type 3).
- <nssa-external> Show NSSA external link states (LSA type 7).
- <opaque-link> Show opaque Link-Local LSAs.
- <opaque-area> Show opaque Area LSAs.
- <opaque-as> Show opaque AS LSAs.
- <max-age> Show LSAs in max age list.
- <lsa_id> Show information filtered by link state identifier.
- <self-originate> Shows self-originated link states.
- <adv-router> Shows link states for a particular advertising router.
- <router_id> Router id of the advertising router.

Examples

```
Switch# ip ospf database
      OSPF Router with ID (16.77.114.14)
          Router Link States (Area 0.0.0.0)
```

Link ID	ADV Router	Age	Seq#	ChkSum	Link count
16.77.114.14	16.77.114.14	723	0x80000004	0x247f	0

Summary Link States (Area 0.0.0.0)

Link ID	ADV Router	Age	Seq#	ChkSum	Route
16.77.114.0	16.77.114.14	482	0x80000003	0x0f79	16.77.114.0/24

Router Link States (Area 0.0.0.1)

Link ID	ADV Router	Age	Seq#	ChkSum	Link count
16.77.114.12	16.77.114.12	830	0x80000004	0x5483	1
16.77.114.14	16.77.114.14	633	0x80000004	0xcae2	1

Net Link States (Area 0.0.0.1)

Link ID	ADV Router	Age	Seq#	ChkSum
16.77.114.12	16.77.114.12	790	0x80000002	0x8562

```
switch# show ip ospf database asbr-summary
```

```
      OSPF Router with id(192.168.239.66) (Process ID 300)
          Displaying Summary ASB Link States(Area 0.0.0.0)
LS age: 1463
Options: (No TOS-capability)
LS Type: Summary Links(AS Boundary Router)
```

Layer 3 features

```
Link State ID: 172.16.245.1 (AS Boundary Router address)
Advertising Router: 172.16.241.5
LS Seq Number: 80000072
Checksum: 0x3548
Length: 28
Network Mask: 0.0.0.0
      TOS: 0  Metric: 1
```

```
switch# show ip ospf database external
```

```
      OSPF Router with id(192.168.239.66) (Autonomous system 300)
          Displaying AS External Link States
LS age: 280
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 10.105.0.0 (External Network Number)
Advertising Router: 172.16.70.6
LS Seq Number: 80000AFD
Checksum: 0xC3A
Length: 36
Network Mask: 255.255.0.0
      Metric Type: 2 (Larger than any link state path)
      TOS: 0
      Metric: 1
      Forward Address: 0.0.0.0
      External Route Tag: 0
```

```
switch# show ip ospf database network
```

```
      OSPF Router with ID (2.2.2.2)
          Net Link States (Area 0.0.0.1 [NSSA])

LS age: 3600
Options: 0x2  : *|-|-|-|-|E|*
LS Flags: 0x3
LS Type: network-LSA
Link State ID: 16.77.114.10 (address of Designated Router)
Advertising Router: 16.77.114.10
LS Seq Number: 80000001
Checksum: 0x6988
Length: 32
Network Mask: /24
      Attached Router: 16.77.114.10
      Attached Router: 16.77.114.11

LS age: 754
Options: 0x8  : *|-|-|-|N/P|-|-|*
LS Flags: 0x6
LS Type: network-LSA
Link State ID: 16.77.114.11 (address of Designated Router)
Advertising Router: 1.1.1.1
LS Seq Number: 80000003
Checksum: 0xb1b5
```

```

Length: 32
Network Mask: /24
    Attached Router: 2.2.2.2
    Attached Router: 1.1.1.1
    
```

```

LS age: 104
Options: 0x8 : *|---|N/P|---|*
LS Flags: 0x3
LS Type: network-LSA
Link State ID: 16.77.114.11 (address of Designated Router)
Advertising Router: 2.2.2.2
LS Seq Number: 80000002
Checksum: 0x95ce
Length: 32
Network Mask: /24
    Attached Router: 2.2.2.2
    Attached Router: 1.1.1.1
    
```

```

switch# show ip ospf database router
      OSPF Router with ID (2.2.2.2)
          Router Link States (Area 0.0.0.1 [NSSA])
LS age: 676
Options: 0x8 : *|---|N/P|---|*
LS Flags: 0x6
Flags: 0x0
LS Type: router-LSA
Link State ID: 1.1.1.1
Advertising Router: 1.1.1.1
LS Seq Number: 80000007
Checksum: 0xc7b8
Length: 36
Number of Links: 1
  Link connected to: a Transit Network
    (Link ID) Designated Router address: 16.77.114.11
    (Link Data) Router Interface address: 16.77.114.11
    Number of TOS metrics: 0
      TOS 0 Metric: 10
LS age: 680
Options: 0x8 : *|---|N/P|---|*
LS Flags: 0x3
Flags: 0x2 : ASBR
LS Type: router-LSA
Link State ID: 2.2.2.2
Advertising Router: 2.2.2.2
LS Seq Number: 80000008
Checksum: 0xbcc3
Length: 36
Number of Links: 1
  Link connected to: a Transit Network
    (Link ID) Designated Router address: 16.77.114.11
    (Link Data) Router Interface address: 16.77.114.10
    Number of TOS metrics: 0
    
```

```
TOS 0 Metric: 65535
```

```
switch# show ip ospf database summary
      OSPF Router with id(192.168.239.66) (Process ID 300)
      Displaying Summary Net Link States(Area 0.0.0.0)
LS age: 1401
Options: (No TOS-capability)
LS Type: Summary Links(Network)
Link State ID: 172.16.240.0 (summary Network Number)
Advertising Router: 172.16.241.5
LS Seq Number: 80000072
Checksum: 0x84FF
Length: 28
Network Mask: 255.255.255.0
      TOS: 0 Metric: 1
```

```
switch# show ip ospf database nssa-external
      OSPF Router with ID (2.2.2.2)
      NSSA-external Link States (Area 0.0.0.1 [NSSA])
LS age: 43
Options: 0xa : *|---|N/P|---|E|*
LS Flags: 0xb
LS Type: NSSA-LSA
Link State ID: 0.0.0.0 (External Network Number for NSSA)
Advertising Router: 2.2.2.2
LS Seq Number: 80000001
Checksum: 0xc81d
Length: 36
Network Mask: /0
      Metric Type: 2 (Larger than any link state path)
      TOS: 0
      Metric: 1
      NSSA: Forward Address: 16.77.114.10
      External Route Tag: 0
```

```
switch# show ip ospf database external 0.0.0.0
      OSPF Router with ID (2.2.2.2)
      AS External Link States
LS age: 338
Options: 0x2 : *|---|---|E|*
LS Flags: 0xb
LS Type: AS-external-LSA
Link State ID: 0.0.0.0 (External Network Number)
Advertising Router: 2.2.2.2
LS Seq Number: 80000004
Checksum: 0xaa1c
Length: 36
Network Mask: /0
      Metric Type: 2 (Larger than any link state path)
      TOS: 0
      Metric: 1
      Forward Address: 0.0.0.0
```

External Route Tag: 0

```
switch# show ip ospf database network 16.77.114.11
      OSPF Router with ID (2.2.2.2)
        Net Link States (Area 0.0.0.1 [NSSA])
LS age: 805
Options: 0x8  : *|-|-|-|N/P|-|-|*
LS Flags: 0x6
LS Type: network-LSA
Link State ID: 16.77.114.11 (address of Designated Router)
Advertising Router: 1.1.1.1
LS Seq Number: 80000003
Checksum: 0xb1b5
Length: 32
Network Mask: /24
    Attached Router: 2.2.2.2
    Attached Router: 1.1.1.1
LS age: 154
Options: 0x8  : *|-|-|-|N/P|-|-|*
LS Flags: 0x3
LS Type: network-LSA
Link State ID: 16.77.114.11 (address of Designated Router)
Advertising Router: 2.2.2.2
LS Seq Number: 80000002
Checksum: 0x95ce
Length: 32
Network Mask: /24
    Attached Router: 2.2.2.2
    Attached Router: 1.1.1.1
```

5.11.70. Show OSPF interface information

This command displays information about OSPF-enabled interfaces.

Syntax show ip ospf interface [<interface_name>]

Authority All users.

<interface_name> shows information only of a particular interface.

Examples

```
switch# show ip ospf interface
eth0 is up
MTU 1500 bytes, BW 0 Mbps <UP,BROADCAST,RUNNING>
Internet Address 16.77.114.10/24, Area 0.0.0.1 [NSSA]
MTU mismatch detection:enabled
Router ID 2.2.2.2, Network Type BROADCAST, Cost: 333
Transmit Delay is 1 sec, State Backup, Priority 100
Designated Router (ID) 1.1.1.1, Interface Address 16.77.114.11
Backup Designated Router (ID) 2.2.2.2, Interface Address 16.77.114.10
Saved Network-LSA sequence number 0x80000002
Multicast group memberships: OSPFAllRouters OSPFDesignatedRouters
```

```
Timer intervals configured, Hello 10s, Dead 40s, Wait 40s, Retransmit 5
Hello due in 1.976s
Neighbor Count is 1, Adjacent neighbor count is 1
lo is up
ifindex 1, MTU 65536 bytes, BW 0 Kbit <UP,LOOPBACK,RUNNING>
OSPF not enabled on this interface
```

```
switch# show ip ospf interface eth0
eth0 is up
ifindex 444, MTU 1500 bytes, BW 0 Kbit <UP,BROADCAST,RUNNING>
Internet Address 16.77.114.10/24, Broadcast 16.77.114.255, Area 0.0.0.1 [NSSA]
MTU mismatch detection:enabled
Router ID 2.2.2.2, Network Type BROADCAST, Cost: 333
Transmit Delay is 1 sec, State Backup, Priority 100
Designated Router (ID) 1.1.1.1, Interface Address 16.77.114.11
Backup Designated Router (ID) 2.2.2.2, Interface Address 16.77.114.10
Multicast group memberships: OSPFAllRouters OSPFDesignatedRouters
Timer intervals configured, Hello 10s, Dead 40s, Wait 40s, Retransmit 5
Hello due in 1.976s
Neighbor Count is 1, Adjacent neighbor count is 1
```

5.11.71. Show OSPF neighbor information

This command displays information about OSPF neighbors.

- Syntax** show ip ospf neighbor {<interface_name> | <neighbor_id>} [detail] [all]
- Authority** All users.
- <interface_name> Shows information only of a neighbor connected to a particular interface.
- <neighbor_id> Shows information about a particular neighbor.
- <detail> Shows detailed information about the neighbors.
- <all> Shows information about all the neighbors include those which are dead.

Examples

```
switch# show ip ospf neighbor
Neighbor ID Pri State          Dead Time   Address      Interface      RXmtL R
1.1.1.1      120 Full/DR      31.403s    16.77.114.11 eth0:16.77.114.10 1
```

```
switch# show ip ospf neighbor eth0
Neighbor ID Pri State          Dead Time   Address      Interface      RXmtL R
1.1.1.1      120 Full/DR      31.403s    16.77.114.11 eth0:16.77.114.10 1
```

```
switch# show ip ospf neighbor detail
Neighbor 1.1.1.1, interface address 16.77.114.11
In the area 0.0.0.1 [NSSA] via interface eth0
Neighbor priority is 120, State is Full, 17 state changes
Most recent state change statistics:
Progressive change 56m55s ago
Regressive change 56m55s ago, due to SeqNumberMismatch
DR is 16.77.114.11, BDR is 16.77.114.10
```

```
Options 72 *|O|-|-|N/P|-|-|*
Dead timer due in 37.217s
Database Summary List 0
Link State Request List 0
Link State Retransmission List 1
```

```
switch# show ip ospf neighbor all
Neighbor ID Pri State          Dead Time   Address      Interface      RXmtL R
1.1.1.1      120 Full/DR      31.403s    16.77.114.11 eth0:16.77.114.10 1
//No down status neighbors.
```

5.11.72. Show OSPF routing table

This command displays the OSPF routing table.

Syntax show ip ospf route

Authority All users.

Examples

```
switch# show ip ospf route
===== OSPF network routing table =====
N    16.77.114.0/24      [65535] area: 0.0.0.1
                                   directly attached to eth0
===== OSPF router routing table =====

===== OSPF external routing table =====
```

5.11.73. Show OSPF active non default configurations

This command displays the OSPF active configurations.

Syntax show running-configuration ospf

Authority All users.

Examples

```
switch# show running-config ospf
Building OSPF configuration...
Current configuration:
!
ospf enable
router ospf
ospf router-id 2.2.2.2
log-adjacency-changes detail
compatible rfc1583
timers throttle spf 3000 3000 5000
max-metric router-lsa
area 0.0.0.1 authentication message-digest
area 0.0.0.1 nssa translate-always
neighbor 16.77.114.10 priority 30 poll-interval 30
```

```
default-metric 30
default-information originate always
distance 110
distance ospf inter-area 40 external 30
capability opaque
!
end
```

5.12. Source Interface Commands

5.12.1. Setting a source-interface IP address to the TFTP protocol

This command works in the configuration context and sets a source-interface IP address to the TFTP protocol.



As of now the CLI infra is ready, end to end functionality of source interface selection to the TFTP protocol is not implemented.

Syntax ip source-interface tftp address <A.B.C.D>
Authority All users.
<address> Sets the IP address defined on any interface to the TFTP protocol.

Examples

```
switch# configure terminal
switch(config)# ip source-interface tftp address 1.1.1.1
```

5.12.2. Setting a source-interface IP address for all the specified protocols

This command works in the configuration context and sets a source-interface IP address for all the specified protocols.



As of now the CLI infra is ready, end to end functionality of source interface selection for all the specified protocols is not implemented.

Syntax ip source-interface all address <A.B.C.D>
Authority All users.
<address> Sets the IP address defined on any interface for all the specified protocols.

Examples

```
switch# configure terminal
switch(config)# ip source-interface all address 1.1.1.1
```

5.12.3. Setting a source-interface to TFTP protocol

This command works in the configuration context and sets a source-interface to the TFTP protocol.



As of now the CLI infra is ready, end to end functionality of source interface selection to the TFTP protocol is not implemented.

Syntax ip source-interface tftp interface <IFNAME>
Authority All users.
<interface> Sets an IP address-defined interface to the TFTP protocol.

Examples

```
switch# configure terminal
switch(config)# ip source-interface tftp interface 1
```

5.12.4. Setting a source-interface for all the specified protocols

This command works in the configuration context and sets a source-interface for all the specified protocols.



As of now the CLI infra is ready, end to end functionality of source interface selection for all the specified protocols is not implemented.

Syntax ip source-interface all interface <IFNAME>
Authority All users.
<interface> Sets an IP address-defined interface for all the specified protocols.

Examples

```
switch# configure terminal
switch(config)# ip source-interface all interface 1
```

5.12.5. Unsetting a source-interface to TFTP protocol

This command works in the configuration context and removes the TFTP protocol from the source-interface.



As of now the CLI infra is ready, end to end functionality of source interface selection to the TFTP protocol is not implemented.

Syntax no ip source-interface tftp
Authority All users.

Examples

```
switch# configure terminal
switch(config)# no ip source-interface tftp
```

5.12.6. Unsetting a source-interface for all the specified protocols

This command works in the configuration context and removes all the specified protocols from a source-interface.



As of now the CLI infra is ready, end to end functionality of source interface selection for all the specified protocols is not implemented.

Syntax no ip source-interface tftp

Authority All users.

Examples

```
switch# configure terminal
switch(config)# no ip source-interface all
```

5.12.7. Showing source-interface selection configuration assigned to the TFTP protocol.

This command displays source-interface selection configuration assigned to the TFTP protocol.



As of now the CLI infra is ready, end to end functionality of source interface selection to the TFTP protocol is not implemented.

Syntax show ip source-interface tftp

Authority All users.

Examples

```
switch# show ip source-interface tftp
Source-interface Information
Protocol           Source Interface
-----
tftp               1
```

5.12.8. Showing source-interface selection configuration for all the specified protocols.

This command displays the source-interface selection configuration for all the specified protocols.



As of now the CLI infra is ready, end to end functionality of source interface selection for all the specified protocols is not implemented.

Syntax show ip source-interface

Authority All users.

Examples

```
switch# show ip source-interface
Source-interface Information
Protocol          Source Interface
-----          -
tftp              1
```

5.13. Virtual Router Redundancy Protocol Commands

This section describes the commands you use to view and configure Virtual Router Redundancy Protocol (VRRP) and to view VRRP status information. VRRP helps provide failover and load balancing when you configure two devices as a VRRP pair.

5.13.1. ip vrrp

Use this command in Interface Config mode to create a virtual router associated with the interface or range of interfaces. The parameter *vrid* is the virtual router ID, which has an integer value range from 1 to 255.

Syntax	ip vrrp <1-255>
Authority	All users.
<1-255>	Enter virtual router ID

5.13.2. ip vrrp authentication

This command sets the authorization details value for the virtual router configured on a specified interface or range of interfaces. The parameter {none | simple} specifies the authorization type for virtual router configured on the specified interface. The parameter [key] is optional, it is only required when authorization type is simple text password. The parameter *vrid* is the virtual router ID which has an integer value ranges from 1 to 255.

Syntax	[no] ip vrrp <1-255> authentication {none simple WORD}
Authority	All users.
<1-255>	Enter virtual router ID
<none>	Configure authentication type as none
<simple>	Configure authentication type as simple
<WORD>	Enter a key to be used for authentication

Example

```
switch# configure
switch(config)# interface 1
switch(config-if)# ip vrrp 2
switch(config-if)# ip vrrp 2 authentication none
```

5.13.3. ip vrrp ip

This command sets the virtual router IP address value for an interface or range of interfaces. The value for *ipaddr* is the IP address which is to be configured on that interface for VRRP. The parameter *vrid* is the virtual router ID which has an integer value range from 1 to 255. You can use the optional [secondary] parameter to designate the IP address as a secondary IP address.

Syntax	[no] ip vrrp <1-255> ip A.B.C.D
---------------	---------------------------------

Authority	All users.
<1-255>	Enter virtual router ID
<A.B.C.D>	Set IP address

Example

```
switch# configure
switch(config)# interface 1
switch(config-if)# ip vrrp 2
switch(config-if)# ip vrrp 2 ip 192.136.0.1
```

5.13.4. ip vrrp mode

This command enables the virtual router configured on the specified interface. Enabling the status field starts a virtual router. The parameter *vrid* is the virtual router ID which has an integer value ranging from 1 to 255.

Default	disabled
Syntax	[no] ip vrrp <1-255> mode
Authority	All users.
<1-255>	Enter virtual router ID
<mode>	Enable/disable the VRID on the interface

Examples

```
switch# configure
switch(config)# interface 1
switch(config-if)# ip vrrp 2
switch(config-if)# ip vrrp 2 mode
switch(config-if)# no ip vrrp 2 mode
```

5.13.5. ip vrrp preempt

This command sets the preemption mode value for the virtual router configured on a specified interface or range of interfaces. The parameter *vrid* is the virtual router ID, which is an integer from 1 to 255.

Default	enabled
Syntax	[no] ip vrrp <1-255> preempt delay minimum <0-3600>
<delay>	Configure delay timer
<minimum>	Configure minimum value
<0-3600>	Enter time value in seconds

Examples

```
switch# configure
switch(config)# interface 1
switch(config-if)# ip vrrp 2
```

```
switch(config-if)# ip ip vrrp 2 preempt
switch(config-if)# no ip vrrp 2 preempt
switch(config-if)# ip vrrp 2 preempt delay minimum 20
switch(config-if)# no ip vrrp 2 preempt delay
```

5.13.6. ip vrrp priority

This command sets the priority of a router within a VRRP group. It can be used to configure an interface or a range of interfaces. Higher values equal higher priority. The range is from 1 to 254. The parameter *vid* is the virtual router ID, whose range is from 1 to 255.

The router with the highest priority is elected master. If a router is configured with the address used as the address of the virtual router, the router is called the always 255 so that the address owner is always the 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 the router will take over as master only if preempt mode is enabled.

Default 100 unless the router is the address owner, in which case its priority is automatically set to 255.

Syntax [no] ip vrrp <1-255> priority 1-254

<1-255> Enter virtual router ID

<priority> Set the priority for a virtual router

<1-254> Enter priority value

Examples

```
switch# configure
switch(config)# interface 1
switch(config-if)# ip vrrp 2 priority 25
switch(config-if)# no ip vrrp 2 priority 25
```

5.13.7. ip vrrp timers advertise

This command sets the frequency, in seconds, that an interface or range of interfaces on the specified virtual router sends a virtual router advertisement.

Default 1

Syntax [no] ip vrrp <1-255> timers advertise <1-40>

<1-255> Enter virtual router ID

<timers> The timer used for VRRP advertisement

<advertise> VRRP advertisement timer in seconds

<1-40> Enter time in seconds

Examples

```
switch# configure
switch(config)# interface 1
switch(config-if)# ip vrrp 2 timers advertise 40
```

Layer 3 features

```
switch(config-if)# no ip vrrp 2 timers advertise 40
```

Chapter 6. Data Center Command

This chapter describes the commands to configure the data center features available in the OpenSwitch CLI:

Section 6.1, “Priority-Based Flow Control Commands”

Section 6.2, “OpenFlow CLI Commands”

Section 6.3, “VXLAN Commands”

6.1. Priority-Based Flow Control Commands

Ordinarily, when flow control is enabled on a physical link, it applies to all traffic on the link. When congestion occurs, the hardware sends pause frames that temporarily suspend traffic flow.

Pausing traffic helps prevent buffer overflow and dropped frames.

Priority-based flow control (PFC) provides a way to distinguish which traffic on physical link is paused when congestion occurs, based on the priority of the traffic. An interface can be configured to pause only high priority (i.e., loss-sensitive) traffic when necessary prevent dropped frames while allowing traffic that has greater loss tolerance to continue to flow on the interface.

Priorities are differentiated by the priority field of the IEEE 802.1Q VLAN header, which identifies an IEEE 802.1p priority value. In ICOS, these priority values must be mapped to internal class-of-service (CoS) values. To enable priority-based flow control for a particular CoS value on an interface:

1. Ensure that VLAN tagging is enabled on the interface so that the 802.1p priority values are carried through the network.
2. Ensure that 802.1p priority values are mapped to ICOS CoS values.

When priority-flow-control is disabled, the interface defaults to the IEEE 802.3x flow control setting for the interface. When priority-based flow control is enabled, the interface will not pause any CoS unless there is, at least, one no-drop priority.

6.1.1. priority-flow-control mode

Use the **priority-flow-control mode** command in the Interface Config mode to enable Priority-Flow-Control (PFC) on the given interface.

Use the **no** form of the command to return the mode to the default (off). VLAN tagging (trunk or general mode) must be enabled on the interface in order to carry the dot1p value through the network. Additionally, the dot1mapping to class-of-service must be set to one-to-one.

When PFC is enabled on an interface, the normal PAUSE control mechanism is operationally disabled.

Default	Priority-flow-control mode is off (disabled) by default.
Syntax	priority-flow-control mode { on off }
Authority	Admin.
<on>	Enable PFC on the interface.
<off>	Disable PFC on the interface.

Example: The following example enables PFC on an interface.

```
switch# configure
switch(config)# interface 1
switch(config-if)# priority-flow-control mode on
```

6.1.1.1. no priority-flow-control mode

Use the no priority-flow-control mode command to return the PFC mode to the default (off).

Syntax no priority-flow-control mode

Authority Admin.

6.1.2. priority-flow-control priority

Use the priority-flow-control priority command in the Interface Config mode to enable the priority group for lossless (no-drop) or lossy (drop) behavior on the selected interface. Up to two lossless priorities can be enabled on an interface. The administrator must configure the same no-drop priorities across the network in order to ensure end-to-end lossless behavior.

The command has no effect on interfaces not enabled for PFC. VLAN tagging needs to be turned on in order to carry the dot1p value through the network. Additionally, the dot1p mapping to class of service must be set to one to one.

Default The default behavior for all priorities is drop.

Syntax priority-flow-control priority priority-list {drop | no-drop}

Authority Admin.

<drop> Disable lossless behavior on the selected priorities.

<no-drop> Enable lossless behavior on the selected priorities.

Example: The following example sets priority 3 to no drop behavior.

```
switch# configure
switch(config)# interface 1
switch(config-if)#priority-flow-control mode on
switch(config-if)# priority-flow-control priority 1 no-drop
```

6.1.2.1. no priority-flow-control priority

Use the no priority-flow-control priority command in Datacenter-Bridging Config mode to enable lossy behavior on all priorities on the interface. This has no effect on interfaces not enabled for PFC or with no lossless priorities configured.

Syntax no priority-flow-control priority

Authority Admin.

6.2. OpenFlow CLI Commands

Command	Function
openflow	Enter OpenFlow mode.
controller A.B.C.D {port <1-65535> (tcp/ssl)}	Configure the controller information.
hybridmode	Configure Normal Port to be used to OpenFlow.
openflow-port	Configure Normal Port to be an Openflow Port and dedicate for OpenFlow pipeline.
show openflow	Display the OpenFlow configurations.
show openflow flows	Display the flow information.
show openflow groups	Display the group information.
show openflow meters	Display the meter information.

6.2.1. openflow

Use this command to enter OpenFlow mode.

Syntax openflow

Authority Admin

Example:

```
switch(config)# openflow
switch(config-openflow)#
```

6.2.2. controller

Use this command to configure the controller information.

Default Port 6653 and TCP

Syntax [no] controller A.B.C.D {port <1-65535> (tcp|ssl)}

Authority Admin

Example:

```
switch(config-openflow)# controller 192.168.1.100
switch(config-openflow)# do show openflow
OpenFlow Configuration:
-----
OpenFlow Datapath Type : ofdpa
Number of OpenFlow Ports : 0
Hybrid Port Mode : disable
Controller IP Port Mode
-----
```

```
192.168.1.100 6653 tcp
OpenFlow Port
-----
switch(config-openflow)
```

6.2.3. hybridmode

Use this command to configure Normal Port (L3 port or L2 port) to be used by OpenFlow in the OpenFlow hybrid switch.

Default Disable
Syntax [no] hybridmode
Authority Admin

Example:

```
switch(config-openflow)# hybridmode
switch(config-openflow)# do show openflow
OpenFlow Configuration:
-----
OpenFlow Datapath Type : ofdpa
Number of OpenFlow Ports : 0
Hybrid Port Mode : enable
Controller IP Port Mode
-----
192.168.1.100 6653 tcp
OpenFlow Port
-----
switch(config-openflow)#
```

6.2.4. openflow-port

Use this command to configure Normal Port (L3 port or L2 port) to be an Openflow Port and dedicate for OpenFlow pipeline in the OpenFlow hybrid switch.

Default Disable
Syntax [no] openflow-port
Authority Admin

Example:

```
switch(config-if-range-intf 13,31,47)# openflow-port
switch(config-if-range-intf 13,31,47)# do show openflow
OpenFlow Configuration:
-----
OpenFlow Datapath Type : ofdpa
Number of OpenFlow Ports : 3
Hybrid Port Mode : disable
Controller IP Port Mode
-----
```

```

192.168.1.100 6653 tcp
OpenFlow Port
-----
13
31
47
switch(config-if-range-intf 13,31,47)#

```

6.2.5. show openflow

Use this command to display the OpenFlow configurations.

Syntax show openflow

Authority Admin

Example:

```

switch# show openflow
OpenFlow Configuration:
-----
OpenFlow Datapath Type : ofdpa
Number of OpenFlow Ports : 3
Hybrid Port Mode : disable
Controller IP Port Mode
-----
192.168.1.100 6653 tcp
OpenFlow Port
-----
13
31
47
switch#

```

6.2.6. show openflow flows

Use this command to display the flow information.

Syntax show openflow flows

Authority Admin

Example:

```

switch# show openflow flows
Flows:
-----
cookie=0x0, duration=418.659s, table=20, n_packets=83, n_bytes=139851186626542,
ip,dl_dst=00:00:00:11:22:33 actions=goto_table:30
cookie=0x0, duration=418.621s, table=30, n_packets=83, n_bytes=139851186626542,
ip,nw_dst=1.1.1.0/24 actions=write_actions(group:536870913),goto_table:60
cookie=0x0, duration=418.588s, table=30, n_packets=83, n_bytes=139851186626542,
ip,nw_dst=2.2.2.0/24 actions=write_actions(group:536870914),goto_table:60

```

```

cookie=0x0, duration=418.559s, table=30, n_packets=83, n_bytes=139851186626542,
ip,nw_dst=3.3.3.0/24 actions=write_actions(group:536870915),goto_table:60
cookie=0x0, duration=418.531s, table=30, n_packets=83, n_bytes=139851186626542,
ip,nw_dst=4.4.4.0/24 actions=write_actions(group:1879048193),goto_table:60
cookie=0x0, duration=418.497s, table=60, n_packets=83, n_bytes=139851186626542,
ip,in_port=47,dl_dst=00:00:00:11:22:33,nw_dst=1.1.1.2
actions=write_actions(group:536870914)
switch#

```

6.2.7. show openflow groups

Use this command to display the group information.

Syntax show openflow groups

Authority Admin

Example:

```

switch# show openflow groups
Groups:
-----
group_id=536870915,type=all,bucket=actions=set_field:4396->vlan_vid,
set_field:00:00:00:11:22:33->eth_src,set_field:00:00:00:00:00:33->eth_dst,
group:19660847
group_id=6553613,type=all,bucket=actions=output:13
group_id=13107231,type=all,bucket=actions=output:31
group_id=536870913,type=all,bucket=actions=set_field:4196->vlan_vid,
set_field:00:00:00:11:22:33->eth_src,set_field:00:00:00:00:00:11->eth_dst,
group:6553613
group_id=19660847,type=all,bucket=actions=output:47
group_id=1879048193,type=all,bucket=actions=group:536870913,
bucket=actions=group:536870914
group_id=536870914,type=all,bucket=actions=set_field:4296->vlan_vid,
set_field:00:00:00:11:22:33->eth_src,set_field:00:00:00:00:00:22->eth_dst,
group:13107231
switch#

```

6.2.8. show openflow meters

Use this command to display the meter information.

Syntax show openflow meters

Authority Admin

Example:

```

switch# show openflow meters
Meters:
-----
meter=1 pktps burst bands=
type=drop,rate=20000,burst_size=100

```

```
meter=2 pktps burst bands=  
type=drop,rate=40000,burst_size=100  
switch#
```

6.3. VXLAN Commands

This section lists the commands that enable the network virtualization technologies (VXLAN) to communicate with another network.

6.3.1. vxlan source-interface

Use this command to specify the loopback source IP address for encapsulated packets sent on a VXLAN.



It is recommended to configure a loopback interface with the intended local VXLAN Gateway IP address and use it as the source-ip for all tenants.

It is also possible to configure tenants with a different source-ip when multiple loopback interfaces are configured and used as local VXLAN Gateways if required. Loopback interfaces intended to be used as local VXLAN Gateways should be dedicated interfaces and must not be used for any other purpose.

Default There is no source IP address.

Syntax vxlan source-interface loopback <1-2147483647>

Authority Admin

<1-2147483647> Loopback interface number

6.3.1.1. no vxlan source

Use this command to remove the source interface.

Syntax no vxlan source-interface

Authority Admin

6.3.2. vxlan tenant-system

Use this command to configure a forwarding entry for the tenant systems MAC address mac-addr' in the given VN that is reachable through the access interface. The user can configure tenant systems incrementally one by one. Normally, the system automatically learns tenant systems MAC address from received traffic on the access interface. The user can configure the tenant systems MAC address mac-addr on the access interface to avoid initial flooding. If the user configures a tenant system on the interface, the configuration overrides learning for the given MAC address in that VN.



This command is valid only on physical and port-channel interfaces. The configured interface should also be a member of VLAN that is associated with the specified vnid.

These tenant system MAC addresses are maintained in a separate table. These are not listed as part of FDB mac-address table. They internally consume shared system hardware L2 address table resources. So, the maximum number of tenant systems configured or learned depend on the number of resources left in the hardware L2 table, which is dynamic in nature.

The configurable range for the VNID 1 to 16777214. 16777215 is reserved for internal purposes.

User is allowed to configure maximum 24 tenant systems per physical or port-channel interface.

Default No tenant MAC addresses are associated with the VN.

Syntax vxlan vnid <1-16777216> tenant-system <mac-addr>

Authority Admin

<1-16777216> VxLAN identifier

<mac-addr> MAC address in the form xx:xx:xx:xx:xx:xx

6.3.2.1. no vxlan tenant-system

Use this command to delete the configured tenant system forwarding entry on an interface when the tenant system mac-address and vnid are specified. This command cannot be used to delete a dynamically-learned tenant system association on the interface in a specified vnid VN.



When an access port configuration of the VN specified by vnid is removed, by removing the port participation of associated VLAN, all forwarding entries, if any, configured by the user and learned by the switch on that access port are also removed.

Syntax no vxlan vnid tenant-system mac-addr

Authority Admin

6.3.3. vni Tunnel Configuration

Use this command to set the tunnel ID for configuration.

Syntax vni <1-16777216>

Authority Admin

<1-16777216> Set the tunnel key

6.3.4. vxlan-vni

Use this command to associate an access VLAN to the specified tunnel.

The packets that arrive with the specified VLAN vlan-id tag are associated to the VXLAN vnid. This command only associates the traffic from the specified VLAN to a given VN identified by vsid. The VLAN vlan-id must be created already for this command to work. The user must configure the access ports for the VN specified by vnid by configuring the VLAN vlan-id membership on the eligible interfaces before or after this command is issued.



It is recommended to configure ingress filtering on all member ports of the VLAN vlan-id.

The configurable range for the VNID 1 to 16777214. 16777215 is reserved for internal purposes.

Default No VLAN is associated with the VXLAN.

Syntax vxlan-vni <1-16777216>

Authority Admin

<1-16777216>VNI number

Example:

```
switch(config)# interface tunnel 1 mode vxlan
switch(config-vxlan-if)# vxlan-vni 1000
```

6.3.4.1. no vxlan vlan

Use this command to remove the association of the specified VLAN from a given VXLAN. All configured access ports of VN specified by vniid are removed.

Syntax no vxlan vniid vlan

Command Global Config

Mode

6.3.5. show vxlan

Use this command to display configuration and status for one or more VXLAN VNs. It also provides information on allowed limits and statistics.

Syntax show vxlan

Authority Admin

Example:

```
switch# show vxlan
VxLAN source interface: loopback1
VxLAN source IP address: 2.2.2.2
  VNID  VLAN    Tunnel    Remote VTEP
-----
     1   N/A
  100  100  tunnel1    1.1.1.1
```

6.3.6. show vxlan tenant-system

Use this command to list all tenant systems currently configured or dynamically learned. This lists tenant systems which are behind the VTEP and also reachable through local access interfaces.

Syntax show vxlan tenant-systems

Authority Admin

Example:

```
switch# show vxlan tenant-system
Number of MAC addresses : 0
```

MAC Address	VNID	Type	Port
-------------	------	------	------

6.3.7. show vxlan tenant-system configuration

Display static VxLAN tenant table information.

Syntax show vxlan tenant-systems

Authority Admin

Example:

```
switch# show vxlan tenant-system configuration
Number of MAC addresses : 0
```

MAC Address	VNID	Type	Port
-------------	------	------	------

6.3.8. show vxlan tunnel

Display VxLAN tunnel interface information.

Syntax show vxlan tunnel

Authority Admin

Example:

```
switch# show vxlan tunnel
```

Tunnel	VNID	Local IP	Remote IP	Status
tunnell	100	2.2.2.2	1.1.1.1	down

Chapter 7. Quality of Service Commands

Section 7.1, "Definition of terms"

Section 7.2, "QoS global configuration commands"

Section 7.3, "QoS interface configuration commands"

Section 7.4, "QoS queue profile configuration commands"

Section 7.5, "QoS schedule profile configuration commands"

Section 7.6, "Display commands"

Section 7.7, "Common troubleshooting"

Section 7.8, "Traffic shape"

7.1. Definition of terms

Term	Description
Class	For networking, a set of packets sharing some common characteristic (for example, all IPv4 packets).
Codepoint	Used in two different ways — either as the name of a packet header field, or as the name of the values carried within a packet header field. Example 1: Priority Code Point (PCP) is the name of a field in the IEEE 802.1Q VLAN tag. Example 2: Differentiated Services codepoint (DSCP) is the name of values carried within the DS field of the header field.
Color	A metadata label associated with each packet within the switch with three values: green, yellow, or red. It is used by the switch when packets encounter congestion for a resource (queue) to distinguish which packets should be dropped.
Class of Service (CoS)	A 3-bit value used to mark packets with one of eight classes (levels of priority). It is carried within the Priority Code Point (PCP) field of the IEEE 802.1Q VLAN tag.
Differentiated Services codepoint (DSCP)	A 6-bit value used to mark packets for different per-hop behavior as originally defined by IETF RFC 2474. It is carried within the Differentiated Services (DS) field of the IPv4 or IPv6 header.
Local-priority	A metadata label associated with a packet within a network switch. It is used by the switch to distinguish packets for different treatment (for example, queue assignment).
Metadata	Information labels associated with each packet in the switch that are separate from the packet headers and data. These labels are used by the switch in its handling of the packet. For example, arrival port, egress port, VLAN membership, local priority, and color.
Priority Code Point (PCP)	The name of a 3-bit field in the IEEE 802.1Q VLAN tag. It carries the CoS value to mark a packet with one of 8 classes (priority levels).
Quality of Service (QoS)	General term used when describing or measuring performance. For networking, it means how different classes of packets are treated across the network or device. For more information, see https://en.wikipedia.org/wiki/Quality_of_service .
Traffic class (TC)	General term for a set of packets sharing some common characteristic. It used to be the name of an 8-bit field in the IPv6 header originally defined by IETF RFC 2460. This field name was changed to Differentiated Services by IETF RFC 2474.
Type of Service (ToS)	General term when there are different levels of treatment (for example, fare class). It used to be the name of an 8-bit field in the IPv4 header originally defined by IETF RFC 791. This field name was changed to Differentiated Services by IETF RFC 2474

7.2. QoS global configuration commands

These commands are entered in the global configuration context.

7.2.1. apply qos queue-profile

The `apply qos` command in the global configuration context configures the given queue profile and schedule profile at the global level. Global profiles are configured on all Ethernet interfaces and LAGs that have not applied their own profiles.

This may cause the interface(s) or LAG(s) to shut down briefly during the reconfiguration.

For a queue profile to be complete and ready to be applied, all local priorities must be mapped to a queue.

For the schedule profile to be complete and ready to be applied, it must have a configuration for each queue defined by the queue profile. All queues must use the same algorithm except for the highest numbered queue, which may be "strict".

There is a special, pre-defined schedule-profile named "strict". It is always present and unalterable. The strict profile services all queues of an associated queue profile using the strict priority algorithm.

Both the queue profile and the schedule profile must specify the same number of queues.

An applied profile cannot be updated or deleted until such time that it is no longer applied.

The `no apply qos` command is disallowed in the global configuration context. It is required to always have a global and schedule profile applied. To cease the use of a profile, apply a different profile.

Syntax	<code>apply qos queue-profile <NAME> schedule-profile {<NAME> strict}</code>
Authority	All configuration users.
<NAME>	The name of the profile to apply
<strict>	Use the strict schedule profile

Examples

```
switch# configure terminal
switch(config)# apply qos queue-profile default schedule-profile strict
```

Troubleshooting

See the Section 7.7, "Common troubleshooting" for error messages that may appear as the output of various commands.

If a profile fails to be applied to the hardware, then the desired configuration may differ from the actual configuration (known as "status"). In this case, the desired configuration and the actual configuration (status) would both be displayed by the **show interface** command. In the following example, the desired schedule profile is strict, but the actual schedule profile in hardware is default:

```
switch# configure terminal
```

```
switch(config)# apply qos queue-profile default schedule-profile strict
switch(config-if)# do show interface 1
```

```
Interface 1 is down (Administratively down)
Admin state is down
State information: admin_down
Hardware: Ethernet, MAC Address: 70:72:cf:e7:cc:67
MTU 1500
Full-duplex
qos trust none
qos queue-profile default
qos schedule-profile strict, status is default
Speed 0 Mb/s
Auto-Negotiation is turned on
Input flow-control is off, output flow-control is off
RX
    0 input packets          0 bytes
    0 input error            0 dropped
    0 CRC/FCS
    L3:
        ucast: 0 packets, 0 bytes
        mcast: 0 packets, 0 bytes
TX
    0 output packets         0 bytes
    0 input error            0 dropped
    0 collision
    L3:
        ucast: 0 packets, 0 bytes
        mcast: 0 packets, 0 bytes
```

Error Message	Description
The queue profile has local priority NUM assigned more than once.	This error message occurs when an apply command is attempted for a queue profile for which the given local priority has been assigned to more than one queue. The solution is to remove the local priority from one of the queues in the queue profile.
The queue profile and the schedule profile cannot contain different queues.	This error message occurs when an apply command is attempted for a queue profile and a schedule profile that have different queues configured. The solution is to add or remove queues from the queue profile or the schedule profile until they both have the same queues configured.
The queue profile and the schedule profile applied on port NUM cannot contain different queues.	This error message occurs when an apply command is attempted for a queue profile that has a different number of queues than a schedule profile that is currently applied at the port level. The solution is to remove the port schedule profile override for the given port, or to modify the queue profile such that it has the same number of queues as the port schedule profile.
Profile NAME does not exist.	This error can occur if an apply command is attempted for a queue profile or a schedule profile that does not exist. The solution is to create the missing queue profile or schedule profile.
The schedule profile must have the same	This error can occur if an apply command is attempted for a schedule profile that does not have the same algorithm assigned to every queue.

Error Message	Description
algorithm assigned to each queue.	The solution is to change the algorithm assigned to each queue until all queues have the same algorithm assigned. The exception is that the highest priority queue is always allowed to be assigned the strict algorithm.

7.2.2. apply qos wred-profile

Syntax	apply qos wred-profile name queue
Authority	All configuration users.
<0-7>	The number of the queue

7.2.3. qos cos-map

The **cos-map** command associates local-priority, color, and optionally a descriptive name to each 802.1 VLAN priority code point (COS).

This table is used when a port's QoS trust mode is set to "cos" to mark packets initial local-priority and color (see qos trust).

The default color is "green". The default name is an empty string.

The **no cos-map** command will restore the assignments for a priority code point back to its factory default.

Syntax	qos cos-map <0-7> local-priority <NUM> [color <COLOR>] [name <DESCRIPTION>]
Syntax	no qos cos-map <0-7>
Authority	All configuration users.
<COS>	802.1 VLAN Priority Code Point from 0 to 7.
<NUM>	Switch-specific local priority value.
<COLOR>	One of the following tokens: green, yellow, or red.
<DESCRIPTION>	Contains up to 64 characters for customer documentation. The allowed characters are alphanumeric, underscore (_), hyphen (-), and dot (.).

Examples

```
switch# configure terminal
switch(config)# qos cos-map 1 local-priority 2 color green name EntryName
```

7.2.4. qos dscp-map

The **dscp-map** command associates local-priority, color, and optionally a descriptive name to each IP differentiated services code point (DSCP). This command can optionally remark the incoming 802.1 VLAN CoS PCP.

This table is used when a port's QoS trust mode is set to *dscp* to assign the packets initial local-priority and color.

The default color is green. The default name is an empty string.

The "no" form of the command restores the assignments for a code point back to its factory default.

Syntax	qos dscp-map <0-63> local-priority <NUM> [color <COLOR>] [name <DESCRIPTION>]
Syntax	no qos dscp-map <0-63>
Authority	All configuration users.
<DSCP>	IP Differentiated Services Code Point from 0 to 63.
<NUM>	Switch-specific local priority value.
<COLOR>	One of the following tokens: green, yellow, or red.
<DESCRIPTION>	Contains up to 64 characters for customer documentation. The allowed characters are alphanumeric, underscore (_), hyphen (-), and dot (.).

Examples

```
switch# configure terminal
switch(config)# qos dscp-map 1 local-priority 2 color green name EntryName
```

7.2.5. qos queue-profile

The **queue-profile** command is used to enter the queue-profile configuration context to create or edit a named queue profile.

The "no" form of the command deletes the named queue profile, if it is not currently applied.

Default profile

There is a special, pre-defined profile named "default". At installation, a factory supplied default queue-profile is automatically applied. The default profile is editable as long as it is not applied.

The **show qos queue-profile default** command displays current contents of the profile.

The profile named "default" cannot be deleted. The no queue-profile default command resets the default profile back to the factory supplied profile.

Syntax	qos queue-profile <NAME>
Syntax	no qos queue-profile <NAME>
Authority	All configuration users.
<NAME>	Contains up to 64 characters for customer documentation. The allowed characters are alphanumeric, underscore (_), hyphen (-), and dot (.).

Examples

```
switch# configure terminal
switch(config)# qos queue-profile Profile_Name_v1
```

Troubleshooting

See the Section 7.7, “Common troubleshooting” for error messages that may appear as the output of various commands.

Error Message	Description
The profile name cannot be <i>strict</i> .	This error occurs when the profile name parameter is the reserved profile name "strict". The solution is to select another profile name that is not "strict".
An applied profile cannot be amended or deleted.	This error occurs when an applied profile is attempted to be modified or deleted. The solution is to modify a different profile, or to apply a different profile so that the given profile can be modified.
A hardware default profile cannot be amended or deleted.	This error occurs when the hardware default profile is attempted to be modified or deleted. The solution is to modify a different profile, since the hardware default profile cannot be modified.

7.2.6. qos schedule-profile

The **schedule-profile** command is used to enter the schedule-profile configuration context to create or edit a named schedule profile.

The "no" form of the command deletes the named schedule profile, if it is not currently applied.

Default schedule profile

There is a special, pre-defined profile named "default". At installation, a factory supplied default schedule-profile is automatically applied. The default profile is editable as long as it is not applied.

The **show qos schedule-profile default** command displays current contents of the profile.

The profile named "default" cannot be deleted. The no schedule-profile default command resets the default profile back to the factory supplied profile.

Syntax qos schedule-profile <NAME>

Syntax no qos schedule-profile <NAME>

Authority All configuration users.

<NAME> Contains up to 64 characters for customer documentation. The allowed characters are alphanumeric, underscore (_), hyphen (-), and dot (.).

Examples

```
switch# configure terminal
switch(config)# qos schedule-profile Profile_Name_v2
```

Troubleshooting

See the Section 7.7, “Common troubleshooting” for error messages that may appear as the output of various commands.

Error Message	Description
The profile name cannot be <i>strict</i> .	This error occurs when the profile name parameter is the reserved profile name "strict". The solution is to select another profile name that is not "strict".

Error Message	Description
An applied profile cannot be amended or deleted.	This error occurs when an applied profile is attempted to be modified or deleted. The solution is to modify a different profile, or to apply a different profile so that the given profile can be modified.
A hardware default profile cannot be amended or deleted.	This error occurs when the hardware default profile is attempted to be modified or deleted. The solution is to modify a different profile, since the hardware default profile cannot be modified.

7.2.7. qos trust

The **trust** command configures one of three modes that be applied globally on all Ethernet interfaces and LAGs. The modes determine which of any packet field values are used to assign the initial Local-priority and Color metadata values to the packet from the CoS or DSCP Map tables.

The **no qos trust** command restores the trust mode back to the factory default.

Syntax qos trust {none|cos|dscp}

Syntax no qos trust

Authority All configuration users.

<none> Ignores all packet headers. The packet is initially assigned local_priority of zero and color of green.

<cos> For 802.1 VLAN tagged packets, use the priority code point field value of the outermost VLAN header as the index into the COS Map. If the packet is untagged, use the metadata values at index zero of the COS Map.

<dscp> For IP packets, use the DSCP value as the index into the DSCP Map. For non-IP packets with 802.1 VLAN tag(s), use the priority code point field value of the outermost tag header as the index into the CoS Map. For untagged, non-IP packets, use the metadata values at index zero of the CoS Map.

Examples

```
switch# configure terminal
switch(config)# qos trust dscp
```

7.2.8. qos wred-profile

The **wred-profile** command switches the vtysh context to the WRED configuration.

The **no wred-profile** command restores the factory default.

Syntax qos wred-profile <NAME>

Syntax no qos wred-profile

Authority All configuration users.

<NAME> The name of the WRED Profile

Examples

```
switch# configure terminal
```

```
switch(config)# qos wred-profile name1
switch(config-wred)#
```

7.2.8.1. qos wred-profile queue

Configure the threshold or ECN marking for a queue of WRED Profile

Syntax queue <0-7> (green|yellow|red|non-tcp) min-threshold <0-100> max-threshold <0-100> max-drop <0-100>

Syntax no queue <0-7>

<0-7> The number of the queue

<green> color green TCP

<non-tcp> non-TCP

<red> color red TCP

<remark> ECN marking during congestion

<yellow> color yellow TCP

<min-thresh-
old> minimum threshold

<max-thresh-
old> maximum threshold

<max-drop> max drop probability

Examples

```
switch(config-wred)# queue 1 green min-threshold 30 max-threshold 60
max-drop 10
```

7.3. QoS interface configuration commands

These commands are entered in the interface configuration context.

7.3.1. interface apply qos

The **apply qos** command in the Ethernet or LAG interface configuration context configures the given schedule profile just for that interface. It overrides any schedule-profile applied in the global context.

This may cause the interface (or LAG) to shutdown briefly during the reconfiguration.



The same name as the currently applied schedule-profile can be applied in the global context. This guarantees that the interface always uses this schedule-profile, even when the global context schedule-profile subsequently changes.

For the schedule profile to be complete and ready to be applied, it must have a configuration for each queue defined by the queue profile. All queues must use the same algorithm (for example DWRR), except for the highest numbered queue, which may be "strict".

An applied profile cannot be updated or deleted until it is no longer applied.

Strict schedule profile

There is a special, pre-defined profile named "strict". It is always present and unalterable. The strict profile services all queues of an associated queue profile using strict priority scheduling.

The **no apply qos schedule-profile** command clears a schedule profile override for a given interface and the interface uses the global schedule profile. This is the only way to remove a schedule-profile override from the interface.

Syntax	apply qos schedule-profile {<NAME> strict}
Syntax	no apply qos schedule-profile
Authority	All configuration users.
<NAME>	The name of the profile to apply.
<strict>	Use the strict schedule profile.

Examples

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# apply qos schedule-profile strict
```

Troubleshooting

See the Section 7.7, "Common troubleshooting" for error messages that may appear as the output of various commands.

If a profile fails to be applied to the hardware, then the desired configuration may differ from the actual configuration (known as "status"). In this case, the desired configuration and the actual con-

figuration (status) would both be displayed by the **show interface** command. In the following example, the desired schedule profile is "strict", but the actual schedule profile in hardware is "default":

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# apply qos schedule-profile strict
switch(config-if)# do show interface 1
```

```
Interface 1 is down (Administratively down)
Admin state is down
State information: admin_down
Hardware: Ethernet, MAC Address: 70:72:cf:e7:cc:67
MTU 1500
Full-duplex
qos trust none
qos queue-profile default
qos schedule-profile strict, status is default
Speed 0 Mb/s
Auto-Negotiation is turned on
Input flow-control is off, output flow-control is off
RX
    0 input packets          0 bytes
    0 input error            0 dropped
    0 CRC/FCS
L3:
    ucast: 0 packets, 0 bytes
    mcast: 0 packets, 0 bytes
TX
    0 output packets         0 bytes
    0 input error            0 dropped
    0 collision
L3:
    ucast: 0 packets, 0 bytes
    mcast: 0 packets, 0 bytes
```

Error Message	Description
The queue profile and the schedule profile cannot contain different queues.	This error message occurs when an apply command is attempted for a queue profile and a schedule profile that have different queues configured. The solution is to add or remove queues from the queue profile or the schedule profile until they both have the same queues configured.
Profile NAME does not exist.	This error can occur if an apply command is attempted for a queue profile or a schedule profile that does not exist. The solution is to create the missing queue profile or schedule profile.
The schedule profile must have the same algorithm assigned to each queue.	This error can occur if an apply command is attempted for a schedule profile that does not have the same algorithm assigned to every queue. The solution is to change the algorithm assigned to each queue until all queues have the same algorithm assigned. The exception is that the highest priority queue is always allowed to be assigned the strict algorithm.

7.3.2. interface qos dscp

The `qos dscp` command in the Ethernet or LAG interface configuration context configures a DSCP override just for that interface. It is only allowed if the interface trust mode is "none".



If a DSCP override has been configured, and the trust mode is subsequently set to "cos" or "dscp", then the DSCP override is ignored.

The `no qos dscp` command clears the DSCP override for the interface.

For all arriving IPv4 or IPv6 packets:

- Initial local-priority and color metadata are assigned from the DSCP map entry indexed by the DSCP override value.
- Remark the packet's DSCP in IPv4 or IPv6 DS header field with the DSCP override value.

For all arriving non-IP packets:

- Initial local-priority and color metadata are assigned from the CoS Map entry index 0.
- The CoS of all arriving tagged non-IP packets are unchanged. — If the packet is subsequently transmitted with a 802.1Q VLAN tag, the PCP field contains the unchanged CoS.

Syntax [no] qos dscp <0-63>
Authority All configuration users.
 <0-63> Index into the DSCP Map.

Examples

```
switch# configure terminal
switch(config)# qos trust cos
switch(config)# interface 1
switch(config-if)# qos trust none
switch(config-if)# qos dscp 0
```

Troubleshooting

See the Section 7.7, "Common troubleshooting" for error messages that may appear as the output of various commands.

Error Message	Description
QoS DSCP override is only allowed if the port trust mode is <i>none</i> .	This error occurs when a DSCP override command is attempted when the port trust mode is "none". The solution is to configure the port trust mode to "none".

7.3.3. interface qos trust

The `qos trust` command in the Ethernet or LAG interface configuration context configures a trust mode override just for that interface. It overrides the trust mode applied in the global context. The

modes determine which of any packet field values are used to assign the initial Local-priority and Color metadata values to the packet from the CoS or DSCP Map tables.

The **no qos trust** command clears the trust mode override for a given interface and the interface will use the global schedule profile. This is the only way to remove a trust mode override from the interface.

Syntax qos trust {none|cos|dscp}

Syntax no qos trust

Authority All configuration users.

<none> Ignores all packet headers. The packet is initially assigned local_priority of zero and color of green.

<cos> For 802.1 VLAN tagged packets, use the priority code point field value of the outermost VLAN header as the index into the COS Map. If the packet is untagged, use the metadata values at index zero of the COS Map.

<dscp> For IP packets, use the DSCP value as the index into the DSCP Map. For non-IP packets with 802.1 VLAN tag(s), use the priority code point field value of the outermost tag header as the index into the CoS Map. For untagged, non-IP packets, use the metadata values at index zero of the CoS Map.

Examples

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# qos trust dscp
```

7.4. QoS queue profile configuration commands

To enter the queue profile context, enter the `qos queue-profile` command. The following commands are available in queue profile context:

- `name`
- `map`

Queue numbering

Queues are numbered consecutively starting from zero. Queue zero is the lowest priority queue. The larger the queue number, the higher priority the queue has in scheduling algorithms (see Section 7.5, “QoS schedule profile configuration commands”). The maximum allowed queue number may vary by product. For products supporting eight queues, the largest queue number is seven. Please refer to the product specifications for the maximum.

Default profile

There is a special, pre-defined profile named “default”. At installation, a factory supplied default queue-profile is automatically applied. The default profile is editable as long as it is not applied.

7.4.1. name

The **name** command assigns a descriptive string to a queue number in a queue profile. It has no effect on the product configuration.

The descriptive string contains up to 64 characters for customer documentation. The allowed characters are alphanumeric, underscore (`_`), hyphen (`-`), and dot (`.`).

The **no name** command deletes the name of a queue number in a queue profile.

Syntax `name queue <0-7> <DESCRIPTION> no name queue <0-7>`

Authority All configuration users.

<QUEUE> The queue number from 0 to 7

<DESCRIPTION> The string to assign to the queue number

Examples

```
switch# configure terminal
switch(config)# qos queue-profile Profile_Name
switch(config-queue)# name queue 0 Scavenger_and_backup_data
```

Troubleshooting

See the Section 7.7, “Common troubleshooting” for error messages that may appear as the output of various commands.

Error Message	Description
Profile NAME does not have queue NUM configured.	This error occurs when a "no" command is attempted for a queue that has not yet been configured. The solution is to first configure the queue.

7.4.2. map

The **map** command assigns a local priority to a queue number in a queue profile. Packets marked with that local-priority use the queue.

More than one local-priority can be assigned to use the same queue. A queue without any local-priorities assigned is not used to store packets.

For a queue profile to be suitable to be applied (see `apply qos`), all local-priorities must be assigned to some queue in the profile.

The **no map** command removes the assignment of the local priority from the queue number. If no local priority is provided, then the assignment of all local priorities are removed from the queue.

Syntax `map queue <0-7> local-priority <0-7> no map queue <0-7> [local-priority <0-7>]`

Authority All configuration users.

<QUEUE> The queue number from 0 to 7

<LOCAL_PRIORITY> Local priority to add or remove from the queue number

Examples

```
switch# configure terminal
switch(config)# qos queue-profile ProfileName
switch(config-queue)# map queue 0 local-priority 1
```

Troubleshooting

See the Section 7.7, "Common troubleshooting" for error messages that may appear as the output of various commands.

Error Message	Description
Profile NAME does not have queue NUM configured.	This error occurs when a "no" command is attempted for a queue that has not yet been configured. The solution is to first configure the queue.

7.5. QoS schedule profile configuration commands

To enter the schedule profile context, enter the qos schedule-profile command. The following commands are available in queue profile context:

- strict
- dwrr (deficit weighted round robin)

Queue numbering

Queues in a schedule profile are numbered consecutively starting from zero. Queue zero is the lowest priority queue. The larger the queue number the higher priority the queue has in scheduling algorithms. The maximum allowed queue number may vary by product. For products supporting eight queues, the largest queue number is seven. Please refer to the product specifications for the maximum.

Allowed forms

There are two allowed forms for schedule profiles:

1. All queues use the same scheduling algorithm (for example, dwrr).
2. The highest queue number uses Strict Priority, and all remaining (lower) queues use the same algorithm (for example, dwrr).

The second form supports priority scheduling behavior necessary for the IEFTR RFC 3246 Expedited Forwarding specification.

Default schedule profile

There is a special, pre-defined profile named "default". At installation, a factory supplied default schedule-profile is automatically applied. The default profile is editable as long as it is not applied.

Strict schedule profile

There is a special, pre-defined profile named "strict". It is always present and unalterable. The strict profile services all queues of an associated queue profile using the strict priority algorithm.

7.5.1. strict

The **strict** command assigns the strict priority algorithm to a queue. Strict priority services all packets waiting in a queue before any packets in lower priority queues are serviced.

The **no strict** command only clears the algorithm for a queue when the algorithm already assigned is Strict Priority.

Syntax	strict queue <0-7> no strict queue <0-7>
Authority	All configuration users.
<QUEUE>	The queue number from 0 to 7

Examples

```
switch# configure terminal
switch(config)# qos schedule-profile Profile_1p7q
switch(config-schedule)# strict queue 7
```

Troubleshooting

See the Section 7.7, “Common troubleshooting” for error messages that may appear as the output of various commands.

Error Message	Description
Profile NAME does not have queue NUM configured.	This error occurs when a "no" command is attempted for a queue that has not yet been configured. The solution is to first configure the queue.

7.5.2. dwrr

The **dwrr** command assigns the deficit weighted round robin algorithm and its byte weight to a queue.

Deficit weight round robin apportions available bandwidth among all non-empty queues in relation to their queue weights. A product will either support deficit weighted round robin or weighted round robin, but not both. See the specifications for the product.

The **no dwrr** command only clears the algorithm for a queue when the algorithm already assigned is deficit weighted round robin.

Syntax dwrr queue <0-7> weight <1-127> no dwrr queue <0-7>
Authority All configuration users.
<QUEUE> The queue number from 0 to 7
<WEIGHT> The weight to use for the dwrr scheduling.

Examples

```
switch# configure terminal
switch(config)# qos schedule-profile ProfileName
switch(config-schedule)# dwrr queue 0 weight 11
switch(config-schedule)# dwrr queue 1 weight 17
```

Troubleshooting

See the Section 7.7, “Common troubleshooting” for error messages that may appear as the output of various commands.

Error Message	Description
Profile NAME does not have queue NUM configured.	This error occurs when a "no" command is attempted for a queue that has not yet been configured. The solution is to first configure the queue.

7.6. Display commands

The following commands show configuration and status information.

7.6.1. show interface

This command's display includes the QoS settings that have been configured for an interface.

Syntax show interface <INTERFACE>

Authority All users.

<INTER- Name of the interface.
FACE>

Examples

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# qos trust dscp
switch(config-if)# end
switch# show interface 1
```

```
Interface 1 is down (Administratively down)
Admin state is down
State information: admin_down
Hardware: Ethernet, MAC Address: 70:72:cf:fc:51:de
MTU 0
Half-duplex
qos trust dscp
Speed 0 Mb/s
Auto-Negotiation is turned on
Input flow-control is off, output flow-control is off
RX
      0 input packets          0 bytes
      0 input error           0 dropped
      0 CRC/FCS
TX
      0 output packets         0 bytes
      0 input error           0 dropped
      0 collision
```

7.6.2. show interface queues

This command displays statistics from each queue for an interface:

- Number of packets transmitted
- Number of bytes transmitted
- Number of packets that were not transmitted due to an error (for example: queue full)

Queues are numbered consecutively starting from zero. Queue zero is the lowest priority queue. The larger the queue number the higher priority the queue has in scheduling algorithms. The max-

imum allowed queue number may vary by product. For products supporting eight queues, the largest queue number is seven. Please refer to the product specifications for the maximum.

Syntax show interface <INTERFACE> queues

Authority All users.

<INTER-
FACE> Name of the interface.

Examples

```
switch# show interface 1 queues
```

```
Interface 1 is (Administratively down)
Admin state is down
State information: admin_down
      Tx Packets          Tx Bytes   Tx Packet Errors
Q0           100             8000             0
Q1        1234567          12345678908           5
Q2              0              0             0
Q3              0              0             0
Q4              0              0             0
Q5              0              0             0
Q6              0              0             0
Q7              0              0             0
```

7.6.3. show qos cos-map

This command displays the QoS cos-map.

Syntax show qos cos-map [default]

Authority All configuration users.

<default> The optional "default" parameter displays the factory default values.

Examples

```
switch# show qos cos-map default
code_point local_priority color name
-----
0           1             green Best_Effort
1           0             green Background
2           2             green Excellent_Effort
3           3             green Critical_Applications
4           4             green Video
5           5             green Voice
6           6             green Internetwork_Control
7           7             green Network_Control
```

7.6.4. show qos dscp-map

This command displays the QoS dscp-map.

- Syntax** show qos dscp-map [default]
Authority All users.
<default> The optional "default" parameter displays the factory default values.

Examples

```
switch# show qos dscp-map default
code_point local_priority color name
-----
0          0             green "CS0 "
1          0             green
2          0             green
3          0             green
4          0             green
5          0             green
6          0             green
7          0             green
8          1             green "CS1 "
9          1             green
10         1             green "AF11 "
11         1             green
12         1             yellow "AF12 "
13         1             green
14         1             red    "AF13 "
15         1             green
16         2             green "CS2 "
17         2             green
18         2             green "AF21 "
19         2             green
20         2             yellow "AF22 "
21         2             green
22         2             red    "AF23 "
23         2             green
24         3             green "CS3 "
25         3             green
26         3             green "AF31 "
27         3             green
28         3             yellow "AF32 "
29         3             green
30         3             red    "AF33 "
31         3             green
32         4             green "CS4 "
33         4             green
34         4             green "AF41 "
35         4             green
36         4             yellow "AF42 "
37         4             green
38         4             red    "AF43 "
39         4             green
40         5             green "CS5 "
41         5             green
```

```

42      5      green
43      5      green
44      5      green
45      5      green
46      5      green    "EF"
47      5      green
48      6      green    "CS6"
49      6      green
50      6      green
51      6      green
52      6      green
53      6      green
54      6      green
55      6      green
56      7      green    "CS7"
57      7      green
58      7      green
59      7      green
60      7      green
61      7      green
62      7      green
63      7      green

```

7.6.5. show qos queue-profile

When no parameter is provided, then a sorted list of defined profile names and their status is shown.

When a name is given, this command displays the details of the specified profile. The name "default" can be used to display the current details of that profile.

When the "factory-default" parameter is used in place of a name, then the factory supplied profile is displayed.

Syntax show qos queue-profile [{<NAME> | factory-default}]

Authority All users.

<NAME> The name of the profile to show.

<factory-default> Show the factory default profile.

Examples

```

switch# show qos queue-profile factory-default
queue_num local_priorities name
-----
0          0          Scavenger_and_backup_data
1          1
2          2
3          3
4          4
5          5

```

```
6          6
7          7
```

7.6.6. show qos schedule-profile

When no parameter is provided, then a sorted list of defined profile names and their status is shown.

When a name is given, this command displays the details of the specified profile. The name "default" can be used to display the current details of that profile.

When "factory-default" parameter is used in place of a name, then the factory supplied profile is displayed.

Syntax show qos schedule-profile [{<NAME> | factory-default}]
Authority All users.
<NAME> The name of the profile to show.
<factory-default> Show the factory default profile.

Examples

```
switch# show qos schedule-profile factory-default
queue_num algorithm weight
-----
0          dwrr        1
1          dwrr        1
2          dwrr        1
3          dwrr        1
4          dwrr        1
5          dwrr        1
6          dwrr        1
7          dwrr        1
```

7.6.7. show qos trust

This command displays the global QoS trust setting.

Syntax show qos trust [default]
Authority All users.
<default> The optional "default" parameter displays the factory default value.

Examples

```
switch# show qos trust default
qos trust none
```

7.6.8. show running config

This command displays the QoS settings that have been configured.

Syntax show running-config

Authority All users.

Examples

```
switch# configure terminal
switch(config)# qos trust dscp
switch(config)# interface 1
switch(config-if)# qos trust cos
switch(config-if)# interface lag 10
switch(config-lag-if)# qos trust none
switch(config-lag-if)# end
switch# show running-config
Current configuration:
!
!
!
!
!
interface 1
    qos trust cos
interface lag 10
    qos trust none
qos trust dscp
```

7.6.9. show running config interface

This command displays the QoS settings that have been configured for an interface.

Syntax show running-config interface <interface>

Authority All users.

<interface> Name of the interface.

Examples

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# qos trust dscp
switch(config-if)# end
switch# show running-config interface 1
interface 1
    qos trust dscp
exit
```

7.7. Common troubleshooting

The following error messages may appear as the output of various commands.

Error Message	Description
This field can have a length up to 64 characters.	This error message occurs when a parameter is provided whose length is greater than 64 characters. The solution is to select a name that has 64 or fewer characters.
The allowed characters are alphanumeric, underscore (_), hyphen (-), and dot (.).	This error message occurs when a parameter is provided that contains illegal characters. The allowed characters are alphanumeric, underscore (_), hyphen (-), and dot (.).
Unknown command	This error message can occur if a required parameter is missing from the command, or if a given parameter is out of range. The solution is to ensure that all required parameters are specified for the command, and are within bounds.
Command incomplete	This error message can occur if a required parameter is missing from the command. The solution is to ensure that all required parameters are specified for the command.
PROPERTY cannot be configured on a member of a LAG.	This error message occurs if a command is attempted on an interface that is a member of a LAG. The solution is to execute the command on the LAG, or to remove the interface from the LAG.

7.8. Traffic shape

This command specifies the maximum transmission bandwidth limit for the interface as a whole. You can also specify this value for a range of interfaces or all interfaces. Also known as rate shaping, traffic shaping has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded.

Syntax	traffic-shape rate <0-100>
Authority	Admin.
<rate>	Configure the maximum transmission bandwidth limit
<0-100>	Specify the bandwidth limit in percentage. 0 - disable

Examples

```
switch(config)# interface 1
switch(config-if)# traffic-shape rate 50
```