EnGenius

ECS8830F/ECS8854F

Command Guide

Version 1.1

Contents

Chapter 1 Commands for Basic Switch....1
1.1 Basic Switch....1
1.1.1 Basic Configuration....1
1.1.2 Telnet....14
1.1.3 Configuring Switch IP....22
1.1.4 SNMP....25
1.1.5 Switch Upgrade....35
1.1.6 Boot Configuration....41
1.2 File System....46
1.2.1 cd....46
1.2.2 copy....46
1.2.3 delete....47
1.2.4 dir....47
1.2.5 pwd....48
1.2.6 rename....48
1.3 USB....48
1.3.1 cd usb:....48
1.3.2 dir....48
1.3.3 delete....49
1.3.4 rename....49
1.3.5 copy....49
1.4 Device Management....50
1.4.1 debug devsm....50
1.4.2 force runcfg-sync....50
1.4.3 force sync software-version....50
1.4.4 force switchover....51
1.4.5 reset slot....51
1.4.6 show fan....51
1.4.7 show power....51
1.4.8 show slot....51

Chapter 2 Network Security....53
2.1 Network Security....53
2.1.1 default user password macbased....53
2.1.2 first-login change password....53
2.1.3 userpassword restriction....53
2.1.4 password valid-time....54
2.1.5 user-login failed msg....54
2.1.6 password feedback....54
2.1.7 password security-config....55
2.1.8 boot-file security check....55
2.1.9 ssh-server dst-port....55
2.1.10 telnet-server dst-port....56
2.1.11 snmp-server dst-port....56
2.1.12 ip http secure-ciphersuite....56
2.1.13 ssh-server encryption-algorithm....57
2.1.14 service password-encryption type user....57
2.1.15 bfd authentication key md5....58
2.1.16 enable password....58
2.1.17 enable trustview key....58
2.1.18 ip ftp....59
2.1.19 ntp authentication-key....59
2.1.20 password....60
2.1.21 radius-server accounting host....60
2.1.22 radius-server authentication host....61
2.1.23 radius-server key....61
2.1.24 tacacs-server authentication host....62
2.1.25 tacacs-server key....62

2.1.26 username..... 63

Chapter 3 Commands for Layer 2 services.....64

3.1 Port Configuration.....64
3.1.1 Bandwidth.....64
3.1.2 clear counters interface.....64
3.1.3 description.....64
3.1.4 flow control.....65
3.1.5 interface ethernet.....65
3.1.6 loopback.....65
3.1.7 port-rate-statistics interval.....66
3.1.8 port-scan-mode.....66
3.1.9 rate-violation.....66
3.1.10 show interface.....67
3.1.11 shutdown.....69
3.1.12 storm-control.....70
3.1.13 switchport discard packet.....70
3.2 Port Isolation.....70
3.2.1 isolate-port group.....70
3.2.2 isolate-port group switchport interface.....71
3.2.3 isolate-port apply.....71
3.2.4 show isolate-port group.....72
3.3 Port Loopback Detection.....72
3.3.1 debug loopback-detection.....72
3.3.2 loopback-detection control.....72
3.3.3 loopback-detection control-recovery timeout.....73
3.3.4 loopback-detection interval-time.....73
3.3.5 loopback-detection trap enable.....73
3.3.6 loopback-detection specified-vlan.....74
3.3.7 loopback-detection send packet number.....74
3.3.8 show loopback-detection.....75
3.4 ULDP.....75
3.4.1 debug uldp.....75
3.4.2 debug uldp error.....75
3.4.3 debug uldp event.....76
3.4.4 debug uldp fsm interface ethernet.....76
3.4.5 debug uldp interface ethernet.....76
3.4.6 debug uldp packet.....77
3.4.7 uldp aggressive-mode.....77
3.4.8 uldp enable.....77
3.4.9 uldp disable.....77
3.4.10 uldp hello-interval.....78
3.4.11 uldp manual-shutdown.....78
3.4.12 uldp recovery-time.....78
3.4.13 uldp reset.....79
3.4.14 show uldp.....79
3.5 LLDP.....79
3.5.1 clear lldp remote-table.....79
3.5.2 debug lldp.....79
3.5.3 debug lldp packets.....80
3.5.4 lldp enable.....80
3.5.5 lldp enable (Port).....80
3.5.6 lldp mode.....81
3.5.7 lldp msgTxHold.....81
3.5.8 lldp neighbors max-num.....81
3.5.9 lldp notification interval.....81
3.5.10 lldp tooManyNeighbors.....82
3.5.11 lldp transmit delay.....82
3.5.12 lldp transmit optional tlv.....82
3.5.13 lldp trap.....83
3.5.14 lldp tx-interval.....83

3.5.15 show debugging lldp....83
3.5.16 show lldp....84
3.5.17 show lldp interface ethernet....84
3.5.18 show lldp neighbors interface ethernet....85
3.5.19 show lldp traffic....85
3.6 LLDP-MED....85
3.6.1 civic location....85
3.6.2 {description-language | province-state | city | county | street | locationNum | location | floor | room | postal | otherInfo}....86
3.6.3 ecs location....86
3.6.4 lldp med fast count....87
3.6.5 lldp med trap....87
3.6.6 lldp transmit med tlv all....87
3.6.7 lldp transmit med tlv capability....87
3.6.8 lldp transmit med tlv location....88
3.6.9 lldp transmit med tlv inventory....88
3.6.10 lldp transmit med tlv networkPolicy....89
3.6.11 network policy....89
3.6.12 show lldp....90
3.6.13 show lldp [interface ethernet <IFNAME>]....90
3.6.14 show lldp neighbors....91
3.6.15 show lldp traffic....91
3.7 Port Channel....92
3.7.1 debug port-channel....92
3.7.2 interface port-channel....92
3.7.3 lacp port-priority....92
3.7.4 lacp system-priority....93
3.7.5 lacp timeout....93
3.7.6 load-balance....93
3.7.8 load-balance hash-random....94
3.7.9 load-balance ingress-port....94
3.7.10 load-balance hash-shift....94
3.7.11 port-group....94
3.7.12 port-group mode....95
3.7.13 show port-group....95
3.8 MTU....96
3.8.1 mtu....96
3.9 bpdu-tunnel....97
3.9.1 bpdu-tunnel dmac....97
3.9.2 bpdu-tunnel stp....97
3.9.3 bpdu-tunnel gvrp....97
3.9.4 bpdu-tunnel uldp....98
3.9.5 bpdu-tunnel lacp....98
3.9.6 bpdu-tunnel dot1x....98
3.10 DDM....99
3.10.1 clear transceiver threshold-violation....99
3.10.2 debug transceiver....99
3.10.3 show transceiver....99
3.10.4 show transceiver threshold-violation....100
3.10.5 transceiver-monitoring....100
3.10.6 transceiver-monitoring interval....100
3.10.7 transceiver threshold....101
3.10.8 optician monitor enable|disable....101
3.11 EFM OAM....102
3.11.1 clear ethernet-oam....102
3.11.2 debug ethernet-oam error....102
3.11.3 debug ethernet-oam fsm....102
3.11.4 debug ethernet-oam packet....103
3.11.5 debug ethernet-oam timer....103
3.11.6 ethernet-oam....103
3.11.7 ethernet-oam errored-frame threshold high....104

3.11.8 ethernet-oam errored-frame threshold low....104
3.11.9 ethernet-oam errored-frame window....104
3.11.10 ethernet-oam errored-frame-period threshold high....105
3.11.11 ethernet-oam errored-frame-period threshold low....105
3.11.12 ethernet-oam errored-frame-period window....105
3.11.13 ethernet-oam errored-frame-seconds threshold high....106
3.11.14 ethernet-oam errored-frame-seconds threshold low....106
3.11.15 ethernet-oam errored-frame-seconds window....107
3.11.16 ethernet-oam errored-symbol-period threshold high....107
3.11.17 ethernet-oam errored-symbol-period threshold low....107
3.11.18 ethernet-oam errored-symbol-period window....108
3.11.19 ethernet-oam link-monitor....108
3.11.20 ethernet-oam mode....108
3.11.21 ethernet-oam period....109
3.11.22 ethernet-oam remote-failure....109
3.11.23 ethernet-oam remote-loopback....109
3.11.24 ethernet-oam remote-loopback supported....110
3.11.25 ethernet-oam timeout....110
3.11.26 show ethernet-oam....110
3.11.27 show ethernet-oam events....113
3.11.28 show ethernet-oam link-events-configuration....114
3.11.29 show ethernet-oam loopback-status....115
3.12 Port Security....116
3.12.1 clear port-security....116
3.12.2 show port-security....116
3.12.3 switchport port-security....116
3.12.4 switchport port-security aging....117
3.12.5 switchport port-security mac-address....117
3.12.6 switchport port-security mac-address sticky....118
3.12.7 switchport port-security maximum....118
3.12.8 switchport port-security violation....118
3.13 VLAN....119
3.13.1 vlan....119
3.13.2 vlan internal....119
3.13.3 vlan ingress enable....120
3.13.4 switchport trunk native vlan....120
3.13.5 switchport trunk allowed vlan....120
3.13.6 switchport mode trunk allow-null....121
3.13.7 switchport mode....121
3.13.8 switchport interface....122
3.13.9 switchport hybrid native vlan....122
3.13.10 switchport hybrid allowed vlan....122
3.13.11 switchport forbidden vlan....123
3.13.12 switchport access vlan....123
3.13.13 show vlan....124
3.13.14 private-vlan association....125
3.13.15 private-vlan....125
3.13.16 name....126
3.13.17 vlan-flow-statistics....126
3.14 GVRP....127
3.14.1 garp timer join....127
3.14.2 garp timer leave....127
3.14.3 garp timer leaveAll....128
3.14.4 gvrp (Global)....128
3.14.5 gvrp (Port)....128
3.14.6 no garp timer....128
3.14.7 show garp timer....129
3.14.8 show gvrp fsm information....129
3.14.9 show gvrp leaveAll fsm information....130
3.14.10 show gvrp leavetimer running information....130
3.14.11 show gvrp port-member....130

3.14.12 show gvrp port registerd vlan....131
3.14.13 show gvrp timer running information....131
3.14.14 show gvrp vlan registerd port....131
3.14.15 debug gvrp event....132
3.14.16 debug gvrp packet....132
3.15 Dot1q-tunnel....133
3.15.1 dot1q-tunnel enable....133
3.15.2 dot1q-tunnel tpid....133
3.15.3 show dot1q-tunnel....134
3.16 VLAN translation....134
3.16.1 vlan-translation....134
3.16.2 vlan-translation enable....134
3.16.3 vlan-translation cvid....135
3.16.4 vlan-translation miss drop....135
3.16.5 show vlan-translation....135
3.17 Dynamic VLAN....136
3.17.1 dynamic-vlan mac-vlan prefer....136
3.17.2 dynamic-vlan subnet-vlan prefer....136
3.17.3 mac-vlan....136
3.17.4 mac-vlan vlan....137
3.17.5 protocol-vlan....137
3.17.6 show dynamic-vlan prefer....138
3.17.7 show mac-vlan....138
3.17.8 show mac-vlan interface....138
3.17.9 show protocol-vlan....138
3.17.10 show subnet-vlan....139
3.17.11 show subnet-vlan interface....139
3.17.12 subnet-vlan....139
3.17.13 switchport mac-vlan enable....140
3.17.14 switchport subnet-vlan enable....140
3.18 Voice VLAN....141
3.18.1 show voice-vlan....141
3.18.2 switchport voice-vlan enable....141
3.18.3 voice-vlan....141
3.18.4 voice-vlan vlan....142
3.19 Multi-to-One VLAN Translation....142
3.19.1 vlan-translation n-to-1....142
3.19.2 show vlan-translation n-to-1....143
3.20 Super VLAN....143
3.20.1 supervlan....143
3.20.2 subvlan....143
3.20.3 arp-proxy subvlan....144
3.20.4 ip-addr-range subvlan....144
3.20.5 ip-addr-range....145
3.20.6 show supervlan....145
3.21 MAC Address Table....145
3.21.1 clear collision-mac-address-table....145
3.21.2 clear mac-address-table dynamic....146
3.21.3 mac-address-learning cpu-control....146
3.21.4 mac-address-table aging-time....146
3.21.5 mac-address-table static | static-multicast | blackhole....147
3.21.6 show collision-mac-address-table....147
3.21.7 show mac-address-table....148
3.22 MAC Notification....148
3.22.1 clear mac-notification statistics....148
3.22.2 mac-address-table notification....148
3.22.3 mac-address-table notification history-size....149
3.22.4 mac-address-table notification interval....149
3.22.5 mac-notification....149
3.22.6 show mac-notification summary....150
3.22.7 snmp-server enable traps mac-notification....150

3.23 CFM OAM..... 150
3.23.1 clear ethernet cfm..... 150
3.23.2 continuity-check..... 151
3.23.3 continuity-check interval..... 151
3.23.4 continuity-check receive..... 151
3.23.5 cos..... 152
3.23.6 debug ethernet cfm..... 152
3.23.7 debug ethernet cfm error..... 153
3.23.8 debug ethernet cfm operation..... 153
3.23.9 ethernet cfm alarm..... 153
3.23.10 ethernet cfm auto-traceroute cache..... 154
3.23.11 ethernet cfm domain..... 154
3.23.12 ethernet cfm global..... 155
3.23.13 ethernet cfm logging..... 155
3.23.14 ethernet cfm mep..... 155
3.23.15 ethernet cfm mip..... 156
3.23.16 ethernet cfm mode..... 156
3.23.17 ethernet cfm pvlan..... 156
3.23.18 ethernet cfm snmp-server enable traps..... 157
3.23.19 ethernet cfm y1731 global..... 157
3.23.20 id..... 157
3.23.21 mep mepid..... 158
3.23.22 mip auto-create..... 158
3.23.23 ping ethernet..... 159
3.23.24 sender-id..... 160
3.23.25 service..... 160
3.23.26 show ethernet cfm domain..... 161
3.23.27 show ethernet cfm errors..... 161
3.23.28 show ethernet cfm maintenance-points local..... 162
3.23.29 show ethernet cfm maintenance-points remote..... 164
3.23.30 show ethernet cfm maintenance-points remote detail..... 164
3.23.31 show ethernet cfm mpdb..... 165
3.23.32 show ethernet cfm service..... 166
3.23.33 show ethernet cfm statistic..... 167
3.23.34 show ethernet cfm status..... 168
3.23.35 show ethernet cfm traceroute-reply auto..... 168
3.23.36 show ethernet cfm vlan table..... 169
3.23.37 switchport ulpp group <group-id> track cfm cc level <level-value>..... 169
3.23.38 traceroute ethernet..... 170
3.23.39 traceroute ethernet auto..... 171

Chapter 4 Commands for IP Services..... 172
4.1 Layer 3 Interface..... 172
4.1.1 Bandwidth..... 172
4.1.2 description..... 172
4.1.3 description (VRF mode)..... 172
4.1.4 interface loopback..... 173
4.1.5 interface vlan..... 173
4.1.6 ip vrf..... 173
4.1.7 ip vrf forwarding vrfName..... 174
4.1.8 no interface IFNAME..... 174
4.1.9 rd..... 174
4.1.10 route-target..... 175
4.1.11 show ip route..... 175
4.1.12 show ip route vrf..... 176
4.1.13 show ip vrf..... 176
4.1.14 shutdown..... 177
4.2 Network Management Port..... 177
4.2.1 interface ethernet..... 177
4.2.2 ip address..... 177
4.2.3 shutdown..... 178

4.3 IP Configuration....178
4.3.1 clear ip traffic....178
4.3.2 clear ipv6 neighbor....178
4.3.3 debug ip icmp....178
4.3.4 debug ip packet....179
4.3.5 debug ipv6 packet....179
4.3.6 debug ipv6 icmp....180
4.3.7 debug ipv6 nd....180
4.3.8 debug ipv6 tunnel packet....181
4.3.9 description....181
4.3.10 ip address....181
4.3.11 ipv6 address....182
4.3.12 ipv6 route....182
4.3.13 ipv6 redirect....183
4.3.14 ipv6 nd dad attempts....183
4.3.15 ipv6 nd ns-interval....183
4.3.16 ipv6 nd suppress-ra....184
4.3.17 ipv6 nd ra-lifetime....184
4.3.18 ipv6 nd min-ra-interval....184
4.3.19 ipv6 nd max-ra-interval....184
4.3.20 ipv6 nd prefix....185
4.3.21 ipv6 nd ra-hoplimit....185
4.3.22 ipv6 nd ra-mtu....185
4.3.23 ipv6 nd reachable-time....186
4.3.24 ipv6 nd retrans-timer....186
4.3.25 ipv6 nd other-config-flag....186
4.3.26 ipv6 nd managed-config-flag....186
4.3.27 ipv6 neighbor....186
4.3.28 interface tunnel....187
4.3.29 show ip interface....187
4.3.30 show ip traffic....187
4.3.31 show ipv6 interface....189
4.3.32 show ipv6 route....190
4.3.33 show ipv6 neighbors....191
4.3.34 show ipv6 traffic....191
4.3.35 show ipv6 redirect....192
4.3.36 show ipv6 tunnel....192
4.3.37 tunnel source....193
4.3.38 tunnel destination....193
4.3.39 tunnel nexthop....193
4.3.40 tunnel mode....194
4.4 IP Forwarding....194
4.4.1 ip fib optimize....194
4.5 URPF....194
4.5.1 debug urpf....194
4.5.2 show urpf....195
4.5.3 urpf enable....195
4.6 ARP....195
4.6.1 arp....195
4.6.2 clear arp-cache....196
4.6.3 clear arp traffic....196
4.6.4 debug arp....196
4.6.5 clear ip arp dynamic....196
4.6.6 clear ipv6 nd dynamic....197
4.6.7 ip proxy-arp....197
4.6.8 show arp....197
4.6.9 show arp traffic....198
4.7 Hardware Tunnel Capacity....198
4.7.1 hardware tunnel-capacity....198
4.8 ARP Scanning Prevention....199
4.8.1 anti-arpscan enable [ip|port]....199

4.8.2 anti-arpscan port-based threshold....199
4.8.3 anti-arpscan ip-based threshold....199
4.8.4 anti-arpscan trust....200
4.8.5 anti-arpscan trust ip....200
4.8.6 anti-arpscan recovery enable....201
4.8.7 anti-arpscan recovery time....201
4.8.8 anti-arpscan log enable....201
4.8.9 anti-arpscan trap enable....201
4.8.10 anti-arpscan FFP max-num <num>....202
4.8.11 debug anti-arpscan....202
4.8.12 show anti-arpscan....202
4.8.13 show anti-arpscan ip-based attack-list [history]....203
4.8.14 show anti-arpscan ip-based running-config....204
4.9 Preventing ARP Spoofing....204
4.9.1 ip arp-security updateprotect....204
4.9.2 ip arp-security learnprotect....205
4.9.3 ip arp-security convert....205
4.10 ARP GUARD....205
4.10.1 arp-guard ip....205
4.11 ARP Local Proxy....206
4.11.1 ip local proxy-arp....206
4.12 Gratuitous ARP....206
4.12.1 ip gratuitous-arp....206
4.12.2 show ip gratuitous-arp....207
4.13 Keepalive Gateway....207
4.13.1 keepalive gateway....207
4.13.2 show ip interface....207
4.13.3 show keepalive gateway....208
4.14 Dynamic ARP Inspection....208
4.14.1 ip arp inspection....208
4.14.2 ip arp inspection port....208
4.14.3 ip arp inspection trust....209
4.14.4 ip arp inspection limit-rate....209
4.15 DHCP....210
4.15.1 DHCP Server....210
4.15.2 DHCP Relay....220
4.16 DHCP Option 82....222
4.16.1 debug ip dhcp relay packet....222
4.16.2 ip dhcp relay information option....222
4.16.3 ip dhcp relay information option delimiter....222
4.16.4 ip dhcp relay information option remote-id....223
4.16.5 ip dhcp relay information option remote-id format....223
4.16.6 ip dhcp relay information option self-defined remote-id....224
4.16.7 ip dhcp relay information option self-defined remote-id format....224
4.16.8 ip dhcp relay information option self-defined subscriber-id....224
4.16.9 ip dhcp relay information option self-defined subscriber-id format....225
4.16.10 ip dhcp relay information option subscriber-id....225
4.16.11 ip dhcp relay information option subscriber-id format....225
4.16.12 ip dhcp relay information policy....226
4.16.13 ip dhcp server relay information enable....227
4.16.14 show ip dhcp relay information option....227
4.17 DHCP Snooping....227
4.17.1 debug ip dhcp snooping binding....227
4.17.2 debug ip dhcp snooping event....228
4.17.3 debug ip dhcp snooping packet....228
4.17.4 debug ip dhcp snooping packet interface....228
4.17.5 debug ip dhcp snooping ha....228
4.17.6 debug ip dhcp snooping update....228
4.17.7 ip dhcp snooping....229
4.17.8 ip dhcp snooping action....229
4.17.9 ip dhcp snooping action MaxNum....229

4.17.10 ip dhcp snooping binding....230
4.17.11 ip dhcp snooping binding arp....230
4.17.12 ip dhcp snooping binding dot1x....230
4.17.13 ip dhcp snooping binding user....231
4.17.14 ip dhcp snooping binding user-control....231
4.17.15 ip dhcp snooping binding user-control max-user....232
4.17.16 ip dhcp snooping information enable....232
4.17.17 ip dhcp snooping information option allow-untrusted (replace|)....233
4.17.18 ip dhcp snooping information option delimiter....233
4.17.19 ip dhcp snooping information option remote-id....233
4.17.20 ip dhcp snooping information option self-defined remote-id....234
4.17.21 ip dhcp snooping information option self-defined remote-id format....234
4.17.22 ip dhcp snooping information option self-defined subscriber-id....234
4.17.23 ip dhcp snooping information option self-defined subscriber-id format....235
4.17.24 ip dhcp snooping information option subscriber-id format....235
4.17.25 ip dhcp snooping timeout detection....236
4.17.26 ip dhcp snooping timeout quiet....236
4.17.27 ip dhcp snooping trust....236
4.17.28 ip dhcp snooping vlan....237
4.17.29 ip user helper-address....237
4.17.30 show ip dhcp snooping....238
4.17.31 show ip dhcp snooping binding all....240
4.18 DHCP option 60 and option 43....240
4.18.1 option 43 ascii LINE....240
4.18.2 option 43 hex WORD....241
4.18.3 option 43 ip A.B.C.D....241
4.18.4 option 60 ascii LINE....241
4.18.5 option 60 hex WORD....242
4.18.6 option 60 ip A.B.C.D....242

Chapter 5 Commands for Routing Protocols....243

5.1 Routing Protocol Overview....243
5.1.1 ip prefix-list description....243
5.1.2 ip prefix-list seq....243
5.1.3 ip prefix-list sequence-number....244
5.1.4 match as-path....244
5.1.5 match community....244
5.1.6 match interface....245
5.1.7 match ip....245
5.1.8 match ipv6 address....245
5.1.9 match ipv6 next-hop....246
5.1.10 match metric....246
5.1.11 match origin....246
5.1.12 match route-type....247
5.1.13 match tag....247
5.1.14 route-map....247
5.1.15 set aggregator....248
5.1.16 set as-path....248
5.1.17 set atomic-aggregate....248
5.1.18 set comm-list....249
5.1.19 set community....249
5.1.20 set extcommunity....249
5.1.21 set ip next-hop....250
5.1.22 set local-preference....250
5.1.23 set metric....250
5.1.24 set metric-type....251
5.1.25 set origin....251
5.1.26 set originator-id....251
5.1.27 set tag....252
5.1.28 set vpnv4 next-hop....252
5.1.29 set weight....252

5.1.30 show ip prefix-list <list-name>....253
5.1.31 show ip prefix-list <detail | summary>....253
5.1.32 show route-map....254
5.1.33 show router-id....254
5.2 Static Route....254
5.2.1 ip route....254
5.2.2 ip route vrf....255
5.2.3 show ip route....256
5.2.4 show ip route vrf....257
5.3 RIP....257
5.3.1 accept-lifetime....257
5.3.2 address-family ipv4....258
5.3.3 clear ip rip route....258
5.3.4 debug rip....259
5.3.5 debug rip redistribute message send....259
5.3.6 debug rip redistribute route receive....259
5.3.7 default-information originate....260
5.3.8 default-metric....260
5.3.9 distance....260
5.3.10 distribute-list....261
5.3.11 exit-address-family....261
5.3.12 ip rip aggregate-address....261
5.3.13 ip rip authentication key-chain....262
5.3.14 ip rip authentication mode....262
5.3.15 ip rip authentication string....262
5.3.16 ip rip authentication cisco-compatible....263
5.3.17 ip rip receive-packet....263
5.3.18 ip rip receive version....263
5.3.19 ip rip send-packet....264
5.3.20 ip rip send version....264
5.3.21 ip rip split-horizon....264
5.3.22 key....265
5.3.23 key chain....265
5.3.24 key-string....265
5.3.25 maximum-prefix....266
5.3.26 neighbor....266
5.3.27 network....266
5.3.28 offset-list....267
5.3.29 passive-interface....267
5.3.30 recv-buffer-size....267
5.3.31 redistribute....268
5.3.32 route....268
5.3.33 router rip....269
5.3.34 send-lifetime....269
5.3.35 show debugging rip....270
5.3.36 show ip protocols rip....270
5.3.37 show ip rip....271
5.3.38 show ip rip database....271
5.3.39 show ip rip database vrf....271
5.3.40 show ip rip interface....272
5.3.41 show ip rip interface vrf....272
5.3.42 show ip rip aggregate....272
5.3.43 show ip rip redistribute....273
5.3.44 show ip vrf....273
5.3.45 timers basic....274
5.3.46 version....274
5.4 OSPF....274
5.4.1 area authentication....274
5.4.2 area default-cost....275
5.4.3 area filter-list....275
5.4.4 area nssa....276

5.4.5 area range....276
5.4.6 area stub....277
5.4.7 area virtual-link....277
5.4.8 auto-cost reference-bandwidth....278
5.4.9 compatible rfc1583....278
5.4.10 clear ip ospf process....278
5.4.11 debug ospf events....279
5.4.12 debug ospf ifsm....279
5.4.13 debug ospf lsa....279
5.4.14 debug ospf nfsm....279
5.4.15 debug ospf nsm....280
5.4.16 debug ospf packet....280
5.4.17 debug ospf route....280
5.4.18 debug ospf redistribute message send....280
5.4.19 debug ospf redistribute route receive....281
5.4.20 default-information originate....281
5.4.21 default-metric....281
5.4.22 distance....282
5.4.23 distribute-list....282
5.4.24 filter-policy....283
5.4.25 host area....283
5.4.26 ip ospf authentication....284
5.4.27 ip ospf authentication-key....284
5.4.28 ip ospf cost....284
5.4.29 ip ospf database-filter....285
5.4.30 ip ospf dead-interval....285
5.4.31 ip ospf disable all....285
5.4.32 ip ospf hello-interval....286
5.4.33 ip ospf message-digest-key....286
5.4.34 ip ospf mtu....286
5.4.35 ip ospf mtu-ignore....287
5.4.36 ip ospf network....287
5.4.37 ip ospf priority....287
5.4.38 ip ospf retransmit-interval....288
5.4.39 ip ospf transmit-delay....288
5.4.40 key....289
5.4.41 key chain....289
5.4.42 log-adjacency-changes detail....289
5.4.43 max-concurrent-dd....290
5.4.44 neighbor....290
5.4.45 network area....290
5.4.46 ospf abr-type....291
5.4.47 ospf router-id....291
5.4.48 overflow database....292
5.4.49 overflow database external....292
5.4.50 passive-interface....292
5.4.51 redistribute....293
5.4.52 redistribute ospf....293
5.4.53 router ospf....294
5.4.54 show ip ospf....294
5.4.55 show ip ospf border-routers....295
5.4.56 show ip ospf database....295
5.4.57 show ip ospf interface....296
5.4.58 show ip ospf neighbor....296
5.4.59 show ip ospf redistribute....297
5.4.60 show ip ospf route....297
5.4.61 show ip ospf virtual-links....298
5.4.62 show ip route process-detail....298
5.4.63 show ip protocols....299
5.4.64 summary-address....299
5.4.65 timers spf....300
5.5 BGP....300

5.5.1 address-family....300
5.5.2 aggregate-address....301
5.5.3 bgp aggregate-nexthop-check....301
5.5.4 bgp always-compare-med....301
5.5.5 bgp asnotation asdot....302
5.5.6 bgp bestpath as-path ignore....302
5.5.7 bgp bestpath compare-confed-aspath....302
5.5.8 bgp bestpath compare-routerid....303
5.5.9 bgp bestpath med....303
5.5.10 bgp client-to-client reflection....303
5.5.11 bgp cluster-id....304
5.5.12 bgp confederation identifier....304
5.5.13 bgp confederation peers....305
5.5.14 bgp dampening....305
5.5.15 bgp default....305
5.5.16 bgp deterministic-med....306
5.5.17 bgp enforce-first-as....306
5.5.18 bgp fast-external-failover....306
5.5.19 bgp inbound-route-filter....307
5.5.20 bgp inbound-max-route-num....307
5.5.21 bgp log-neighbor-changes....307
5.5.22 bgp network import-check....308
5.5.23 bgp rfc1771-path-select....308
5.5.24 bgp rfc1771-strict....308
5.5.25 bgp router-id....308
5.5.26 bgp scan-time....309
5.5.27 clear ip bgp....309
5.5.28 clear ip bgp dampening....309
5.5.29 clear ip bgp flap-statistics....310
5.5.30 debug bgp....310
5.5.31 debug bgp redistribute message send....310
5.5.32 debug bgp redistribute route receive....311
5.5.33 distance....311
5.5.34 distance bgp....311
5.5.35 exit-address-family....312
5.5.36 import map....312
5.5.37 ip as-path access-list....313
5.5.38 ip community-list....313
5.5.39 ip extcommunity-list....313
5.5.40 neighbor activate....314
5.5.41 neighbor advertisement-interval....314
5.5.42 neighbor allowas-in....314
5.5.43 neighbor as-override....315
5.5.44 neighbor attribute-unchanged....315
5.5.45 neighbor capability....316
5.5.46 neighbor capability orf prefix-list....316
5.5.47 neighbor collide-established....317
5.5.48 neighbor default-originate....317
5.5.49 neighbor description....317
5.5.50 neighbor distribute-list....318
5.5.51 neighbor dont-capability-negotiate....318
5.5.52 neighbor ebgp-multihop....319
5.5.53 neighbor enforce-multihop....319
5.5.54 neighbor filter-list....319
5.5.55 neighbor interface....320
5.5.56 neighbor maximum-prefix....320
5.5.57 neighbor next-hop-self....321
5.5.58 neighbor override-capability....321
5.5.59 neighbor passive....322
5.5.60 neighbor peer-group (Creating)....322
5.5.61 neighbor peer-group (Configuring group members)....322
5.5.62 neighbor port....323

5.5.63 neighbor prefix-list....323
5.5.64 neighbor remote-as....324
5.5.65 neighbor remove-private-AS....324
5.5.66 neighbor route-map....324
5.5.67 neighbor route-reflector-client....325
5.5.68 neighbor route-server-client....325
5.5.69 neighbor send-community....326
5.5.70 neighbor shutdown....326
5.5.71 neighbor soft-reconfiguration inbound....327
5.5.72 neighbor soo....327
5.5.73 neighbor strict-capability-match....327
5.5.74 neighbor timers....328
5.5.75 neighbor timers connect....328
5.5.76 neighbor unsuppress-map....329
5.5.77 neighbor update-source....329
5.5.78 neighbor version 4....329
5.5.79 neighbor weight....330
5.5.80 network (BGP)....330
5.5.81 redistribute (BGP)....330
5.5.82 redistribute ospf....331
5.5.83 router bgp....331
5.5.84 show ip bgp....332
5.5.85 show ip bgp attribute-info....332
5.5.86 show ip bgp community....332
5.5.87 show ip bgp community-info....333
5.5.88 show ip bgp community-list....333
5.5.89 show ip bgp dampening....334
5.5.90 show ip bgp filter-list....334
5.5.91 show ip bgp inconsistent-as....335
5.5.92 show ip bgp neighbors....335
5.5.93 show ip bgp paths....336
5.5.94 show ip bgp prefix-list....336
5.5.95 show ip bgp quote-regexp....337
5.5.96 show ip bgp regexp....337
5.5.97 show ip bgp route-map....338
5.5.98 show ip bgp scan....338
5.5.99 show ip bgp summary....338
5.5.100 show ip bgp view....339
5.5.101 show ip bgp view neighbors....339
5.5.102 show ip bgp vrf....340
5.5.103 show ip bgp vpnv4....341
5.5.104 timers bgp....341
5.6 IPv4 Black Hole Routing....342
5.6.1 ip route null0....342
5.7 GRE....342
5.7.1 debug gre....342
5.7.2 ip address....342
5.7.3 ip route....343
5.7.4 ipv6 address....343
5.7.5 ipv6 route....343
5.7.6 loopback-group (Global)....344
5.7.7 loopback-group (Port)....344
5.7.8 loopback-group (Tunnel Interface)....344
5.7.9 show gre tunnel....344
5.7.10 show interface tunnel....345
5.7.11 tunnel destination....345
5.7.12 tunnel mode gre ip....345
5.7.13 tunnel source....346
5.8 ECMP....346
5.8.1 load-balance....346
5.8.2 maximum-paths....346

5.8.3 load-balance hash-shift....347
5.9 BFD....347
5.9.1 bfd authentication key....347
5.9.2 bfd authentication key md5|sm3....348
5.9.3 bfd authentication key text....348
5.9.4 bfd echo....348
5.9.5 bfd echo-source-ip....349
5.9.6 bfd echo-source-ipv6....349
5.9.7 bfd enable....349
5.9.8 bfd interval....350
5.9.9 bfd min-echo-recv-interval....350
5.9.10 bfd mode....351
5.9.11 debug bfd....351
5.9.12 ip ospf bfd enable....351
5.9.13 ip route bfd....352
5.9.14 ipv6 ospf bfd enable....352
5.9.15 ipv6 ospf bfd enable instance-id....352
5.9.16 ipv6 rip bfd enable....352
5.9.17 ipv6 route bfd....353
5.9.18 neighbor....353
5.9.19 rip bfd enable....354
5.9.20 show bfd neighbor....354
5.10 BGP GR....355
5.10.1 bgp graceful-restart....355
5.10.2 bgp graceful-restart restart-time....355
5.10.3 bgp graceful-restart stale-path-time....355
5.10.4 bgp selection-deferral-time....356
5.10.5 neighbor capability graceful-restart....356
5.11 OSPF GR....356
5.11.1 capability restart graceful....356
5.11.2 debug ospf events gr....357
5.11.3 ospf graceful-restart grace-period....357
5.11.4 ospf graceful-restart helper max-grace-period....357
5.11.5 ospf graceful-restart helper never....357
5.11.6 show ip ospf....358
5.11.7 show ip ospf graceful-restart....358

Chapter 6 Commands for Multicast Protocol....360

6.1 Multicast....360
6.1.1 show ip mroute....360
6.2 PIM-DM....360
6.2.1 debug pim timer sat....360
6.2.2 debug pim timer srt....361
6.2.3 ip mroute....361
6.2.4 ip pim bsr-border....361
6.2.5 ip pim dense-mode....362
6.2.6 ip pim dr-priority....362
6.2.7 ip pim exclude-genid....362
6.2.8 ip pim hello-holdtime....363
6.2.9 ip pim hello-interval....363
6.2.10 ip pim multicast-routing....364
6.2.11 ip pim neighbor-filter....364
6.2.12 ip pim scope-border....364
6.2.13 ip pim state-refresh origination-interval....365
6.2.14 show ip pim interface....365
6.2.15 show ip pim mroute dense-mode....365
6.2.16 show ip pim neighbor....366
6.2.17 show ip pim nexthop....367
6.3 PIM-SM....367
6.3.1 clear ip pim bsr rp-set....367
6.3.2 debug pim event....368

6.3.3 debug pim mfc..... 368
6.3.4 debug pim mib..... 368
6.3.5 debug pim nexthop..... 369
6.3.6 debug pim nsm..... 369
6.3.7 debug pim packet..... 369
6.3.8 debug pim state..... 369
6.3.9 debug pim timer..... 370
6.3.10 ip mroute..... 371
6.3.11 ip multicast unresolved-cache aging-time..... 371
6.3.12 ip pim accept-register..... 371
6.3.13 ip pim bsr-border..... 372
6.3.14 ip pim bsr-candidate..... 372
6.3.15 ip pim cisco-register-checksum..... 373
6.3.16 ip pim dr-priority..... 373
6.3.17 ip pim exclude-genid..... 373
6.3.18 ip pim hello-holdtime..... 374
6.3.19 ip pim hello-interval..... 374
6.3.20 ip pim ignore-rp-set-priority..... 374
6.3.21 ip pim jp-timer..... 375
6.3.22 ip pim multicast-routing..... 375
6.3.23 ip pim neighbor-filter..... 375
6.3.24 ip pim register-rate-limit..... 376
6.3.25 ip pim register-rp-reachability..... 376
6.3.26 ip pim register-source..... 376
6.3.27 ip pim register-suppression..... 377
6.3.28 ip pim rp-address..... 377
6.3.29 ip pim rp-candidate..... 377
6.3.30 ip pim rp-register-kat..... 378
6.3.31 ip pim scope-border..... 378
6.3.32 ip pim sparse-mode..... 379
6.3.33 show ip pim bsr-router..... 379
6.3.34 show ip pim interface..... 379
6.3.35 show ip pim mroute sparse-mode..... 380
6.3.36 show ip pim neighbor..... 381
6.3.37 show ip pim nexthop..... 381
6.3.38 show ip pim rp-hash..... 382
6.3.39 show ip pim rp mapping..... 382
6.4 MSDP..... 383
6.4.1 cache-sa-holdtime..... 383
6.4.2 cache-sa-maximum..... 383
6.4.3 cache-sa-state..... 383
6.4.4 clear msdp peer..... 384
6.4.5 clear msdp sa-cache..... 384
6.4.6 clear msdp statistics..... 384
6.4.7 connect-source..... 385
6.4.8 debug msdp all..... 385
6.4.9 debug msdp events..... 385
6.4.10 debug msdp filter..... 386
6.4.11 debug msdp fsm..... 386
6.4.12 debug msdp keepalive..... 386
6.4.13 debug msdp nsm..... 386
6.4.14 debug msdp packet..... 387
6.4.15 debug msdp peer..... 387
6.4.16 debug msdp timer..... 387
6.4.17 default-rpf-peer..... 388
6.4.18 description..... 388
6.4.19 exit-peer-mode..... 388
6.4.20 mesh-group..... 389
6.4.21 originating-rp..... 389
6.4.22 peer..... 389
6.4.23 redistribute..... 390
6.4.24 remote-as..... 390

6.4.25 router msdp....390
6.4.26 sa-filter....391
6.4.27 sa-request....391
6.4.28 sa-request-filter....392
6.4.29 show msdp global....392
6.4.30 show msdp local-sa-cache....393
6.4.31 show msdp peer....393
6.4.32 show msdp sa-cache....394
6.4.33 show msdp sa-cache summary....394
6.4.34 show msdp statistics....395
6.4.35 show msdp summary....396
6.4.36 shutdown....396
6.4.37 ttl-threshold....397
6.5 ANYCAST RP....397
6.5.1 debug pim anycast-rp....397
6.5.2 ip pim anycast-rp....397
6.5.3 ip pim anycast-rp....398
6.5.4 ip pim anycast-rp self-rp-address....398
6.5.5 ip pim rp-candidate....399
6.5.6 show debugging pim....399
6.5.7 show ip pim anycast-rp first-hop....399
6.5.8 show ip pim anycast-rp non-first-hop....400
6.5.9 show ip pim anycast-rp status....400
6.6 PIM-SSM....401
6.6.1 ip multicast ssm....401
6.7 DVMRP....402
6.7.1 debug dvmrp....402
6.7.2 ip dvmrp enable....402
6.7.3 ip dvmrp metric....402
6.7.4 ip dvmrp multicast-routing....403
6.7.5 ip dvmrp output-report-delay....403
6.7.6 ip dvmrp reject-non-pruners....403
6.7.7 ip dvmrp tunnel....404
6.7.8 show ip dvmrp....404
6.7.9 show ip dvmrp interface....405
6.7.10 show ip dvmrp neighbor....405
6.7.11 show ip dvmrp prune....405
6.7.12 show ip dvmrp route....406
6.8 Multicast Source and Destination Control....407
6.8.1 access-list (Multicast Destination Control)....407
6.8.2 access-list (Multicast Source Control)....408
6.8.3 ip multicast destination-control....408
6.8.4 ip multicast destination-control access-group (sip)....409
6.8.5 ip multicast destination-control access-group (vmac)....409
6.8.6 ip multicast policy....409
6.8.7 ip multicast source-control....410
6.8.8 ip multicast source-control access-group....410
6.8.9 multicast destination-control....411
6.8.10 profile-id (Multicast Destination Control Rule List)....411
6.8.11 show ip multicast destination-control....412
6.8.12 show ip multicast destination-control access-list....412
6.8.13 show ip multicast destination-control filter-profile-list....412
6.8.14 show ip multicast policy....413
6.8.15 show ip multicast source-control....413
6.8.16 show ip multicast source-control access-list....413
6.9 IGMP....414
6.9.1 clear ip igmp group....414
6.9.2 debug igmp event....414
6.9.3 debug igmp snooping all/packet/event/timer/mfc/authentication/ha....414
6.9.4 ip igmp access-group....415
6.9.5 ip igmp immediate-leave....415

6.9.6 ip igmp join-group....415
6.9.7 ip igmp last-member-query-interval....416
6.9.8 ip igmp limit....416
6.9.9 ip igmp query-interval....416
6.9.10 ip igmp query-max-response-time....417
6.9.11 ip igmp query-timeout....417
6.9.12 ip igmp robust-variable....417
6.9.13 ip igmp static-group....418
6.9.14 ip igmp version....418
6.9.15 show ip igmp groups....418
6.9.16 show ip igmp interface....419
6.10 IGMP Snooping....420
6.10.1 clear ip igmp snooping vlan....420
6.10.2 clear ip igmp snooping vlan <1-4094> mrouter-port....420
6.10.3 debug igmp snooping all/packet/event/timer/mfc....420
6.10.4 ip igmp snooping....421
6.10.5 ip igmp snooping proxy....421
6.10.6 ip igmp snooping vlan....421
6.10.7 ip igmp snooping vlan immediate-leave....421
6.10.8 ip igmp snooping vlan <id> immediately-leave mac-based....422
6.10.9 ip igmp snooping vlan l2-general-querier....422
6.10.10 ip igmp snooping vlan l2-general-querier-source....422
6.10.11 ip igmp snooping vlan l2-general-querier-version....423
6.10.12 ip igmp snooping vlan limit....423
6.10.13 ip igmp snooping vlan interface (ethernet | port-channel|) IFNAME limit....424
6.10.14 ip igmp snooping vlan mrouter-port interface....424
6.10.15 ip igmp snooping vlan mrouter-port learnpim....425
6.10.16 ip igmp snooping vlan mrpt....425
6.10.17 ip igmp snooping vlan query-interval....425
6.10.18 ip igmp snooping vlan query-mrsp....426
6.10.19 ip igmp snooping vlan query-robustness....426
6.10.20 ip igmp snooping vlan report source-address....426
6.10.21 ip igmp snooping vlan specific-query-mrsp....427
6.10.22 ip igmp snooping vlan static-group....427
6.10.23 ip igmp snooping vlan passthrough-group....427
6.10.24 ip igmp snooping vlan not-forward....428
6.10.25 ip igmp snooping vlan suppression-query-time....428
6.10.26 show ip igmp snooping....428
6.11 IGMP Proxy....429
6.11.1 clear ip igmp proxy agggroup....429
6.11.2 debug igmp proxy all....430
6.11.3 debug igmp proxy event....430
6.11.4 debug igmp proxy mfc....430
6.11.5 debug igmp proxy packet....430
6.11.6 debug igmp proxy timer....431
6.11.7 ip igmp proxy....431
6.11.8 ip igmp proxy aggregate....431
6.11.9 ip igmp proxy downstream....431
6.11.10 ip igmp proxy limit....432
6.11.11 ip igmp proxy multicast-source....432
6.11.12 ip igmp proxy unsolicited-report interval....432
6.11.13 ip igmp proxy unsolicited-report robustness....433
6.11.14 ip igmp proxy upstream....433
6.11.15 ip multicast ssm....433
6.11.16 ip pim bsr-border....434
6.11.17 show debugging igmp proxy....434
6.11.18 show ip igmp proxy....434
6.11.19 show ip igmp proxy mroute....435
6.11.20 show ip igmp proxy upstream groups....435
6.12 Multicast VLAN....436
6.12.1 multicast-vlan....436

6.12.2 multicast-vlan association....436
6.12.3 multicast-vlan association interface....436
6.12.4 multicast-vlan mode....437
6.12.5 switchport association multicast-vlan....437

Chapter 7 Commands for Security Function....439

7.1 ACL....439
7.1.1 absolute-periodic/periodic....439
7.1.2 absolute start....439
7.1.3 access-list deny-preemption....440
7.1.4 access-list (ip extended)....441
7.1.5 access-list (ip standard)....442
7.1.6 access-list(mac extended)....442
7.1.7 access-list(mac-ip extended)....444
7.1.8 access-list(mac standard)....445
7.1.9 clear access-group....446
7.1.10 firewall....446
7.1.11 ip access extended....446
7.1.12 ip access standard....446
7.1.13 ipv6 access-list....447
7.1.14 ipv6 access standard....448
7.1.15 ipv6 access extended....448
7.1.16 {ip|ipv6|mac|mac-ip} access-group....448
7.1.17 mac access extended....449
7.1.18 mac-ip access extended....449
7.1.19 permit | deny (ip extended)....450
7.1.20 permit | deny(ip standard)....451
7.1.21 permit | deny(ipv6 extended)....451
7.1.22 permit | deny(ipv6 standard)....452
7.1.23 permit | deny(mac extended)....453
7.1.24 permit | deny(mac-ip extended)....454
7.1.25 show access-lists....455
7.1.26 show access-group....456
7.1.27 show firewall....456
7.1.28 show ipv6 access-lists....457
7.1.29 show time-range....457
7.1.30 time-range....457
7.2 Self-defined ACL....458
7.2.1 userdefined-access-list standard offset....458
7.2.2 userdefined-access-list standard....458
7.2.3 vacl userdefined access-group....459
7.3 802.1x....459
7.3.1 debug dot1x detail....459
7.3.2 debug dot1x error....460
7.3.3 debug dot1x fsm....460
7.3.4 debug dot1x packet....460
7.3.5 dot1x accept-mac....461
7.3.6 dot1x eapor enable....461
7.3.7 dot1x enable....461
7.3.8 dot1x guest-vlan....462
7.3.9 dot1x macfilter enable....462
7.3.10 dot1x macbased guest-vlan....463
7.3.11 dot1x macbased port-down-flush....463
7.3.12 dot1x max-req....464
7.3.13 dot1x user allow-movement....464
7.3.14 dot1x user free-resource....464
7.3.15 free-resource destination....465
7.3.16 dot1x max-user macbased....465
7.3.17 dot1x max-user userbased....465
7.3.18 dot1x portbased mode single-mode....466
7.3.19 dot1x port-control....466

7.3.20 dot1x port-method....466
7.3.21 dot1x re-authenticate....467
7.3.22 dot1x re-authentication....467
7.3.23 dot1x timeout quiet-period....467
7.3.24 dot1x timeout re-authperiod....468
7.3.25 dot1x timeout tx-period....468
7.3.26 dot1x unicast enable....468
7.3.27 free-mac....469
7.3.28 show dot1x....469
7.3.29 show dot1x user....470
7.3.30 clear dot1x all....470
7.4 Number Limitation of MAC and IP Addresses on Ports and VLANs....471
7.4.1 debug ip arp count....471
7.4.2 debug ipv6 nd count....471
7.4.3 debug switchport arp count....472
7.4.4 debug switchport mac count....472
7.4.5 debug switchport nd count....472
7.4.6 debug vlan mac count....473
7.4.7 ip arp dynamic maximum....473
7.4.8 ipv6 nd dynamic maximum....474
7.4.9 mac-address query timeout....474
7.4.10 show arp-dynamic count....474
7.4.11 show mac-address dynamic count....475
7.4.12 show nd-dynamic count....475
7.4.13 switchport arp dynamic maximum....476
7.4.14 switchport mac-address dynamic maximum....476
7.4.15 switchport mac-address violation....477
7.4.16 switchport nd dynamic maximum....477
7.4.17 vlan mac-address dynamic maximum....478
7.5 AM....478
7.5.1 am enable....478
7.5.2 am port....478
7.5.3 am ip-pool....479
7.5.4 am mac-ip-pool....479
7.5.5 no am all....479
7.5.6 show am....480
7.6 Security Feature....480
7.6.1 dosattack-check srcip-equal-dstip enable....480
7.6.2 dosattack-check tcp-flags enable....480
7.6.3 dosattack-check srcport-equal-dstport enable....481
7.6.4 dosattack-check icmp-attacking enable....481
7.6.5 invalid-dip-drop....481
7.7 TACACS+....482
7.7.1 tacacs-server authentication host....482
7.7.2 tacacs-server key....482
7.7.3 tacacs-server nas-ipv4....483
7.7.4 tacacs-server timeout....483
7.7.5 debug tacacs-server....483
7.8 RADIUS....484
7.8.1 aaa enable....484
7.8.2 aaa-accounting enable....484
7.8.3 aaa-accounting update....484
7.8.4 debug aaa packet....485
7.8.5 debug aaa detail attribute....485
7.8.6 debug aaa detail connection....485
7.8.7 debug aaa detail event....486
7.8.8 debug aaa error....486
7.8.9 radius nas-ipv4....486
7.8.10 radius nas-ipv6....486
7.8.11 radius-server accounting host....487
7.8.12 radius-server authentication host....488

7.8.13 radius-server dead-time....488
7.8.14 radius-server key....489
7.8.15 radius-server retransmit....489
7.8.16 radius-server timeout....489
7.8.17 radius-server accounting-interim-update timeout....490
7.8.18 show aaa authenticated-user....490
7.8.19 show aaa authenticating-user....490
7.8.20 show aaa config....491
7.8.21 show radius authenticated-user count....491
7.8.22 show radius authenticating-user count....492
7.8.23 show radius count....492
7.8.24 Radius Escaping....492
7.9 SSL....493
7.9.1 ip http secure-server....493
7.9.2 ip http secure-port....493
7.9.3 ip http secure- ciphersuite....494
7.9.4 show ip http secure-server status....494
7.9.5 debug ssl....494
7.10 VLAN-ACL....495
7.10.1 clear vacl statistic vlan....495
7.10.2 show vacl vlan....495
7.10.3 vacl ip access-group....496
7.10.4 vacl ipv6 access-group....496
7.10.5 vacl mac access-group....497
7.10.6 vacl mac-ip access-group....497
7.11 Captive Portal Authentication....498
7.11.1 Authentication....498
7.11.2 Free-resource....509
7.11.3 Automatic Page Pushing after Successful Authentication....510
7.11.4 Portal Escaping....511
7.12 MAB....512
7.12.1 authentication mab....512
7.12.2 clear mac-authentication-bypass binding....512
7.12.3 debug mac-authentication-bypass....512
7.12.4 mac-authentication-bypass binding-limit....513
7.12.5 mac-authentication-bypass enable....513
7.12.6 mac-authentication-bypass guest-vlan....513
7.12.7 mac-authentication-bypass timeout linkup-period....514
7.12.8 mac-authentication-bypass timeout offline-detect....514
7.12.9 mac-authentication-bypass timeout quiet-period....514
7.12.10 mac-authentication-bypass timeout reauth-period....515
7.12.11 mac-authentication-bypass timeout stale-period....515
7.12.12 mac-authentication-bypass username-format....515
7.12.13 show mac-authentication-bypass....516
7.13 PPPoE Intermediate Agent....517
7.13.1 debug pppoe packet {receive | send} interface ethernet <interface-name>....517
7.13.2 pppoe intermediate-agent....517
7.13.3 pppoe intermediate-agent (Port)....517
7.13.4 pppoe intermediate-agent circuit-id....518
7.13.5 pppoe intermediate-agent delimiter....518
7.13.6 pppoe intermediate-agent format....518
7.13.7 pppoe intermediate-agent remote-id....519
7.13.8 pppoe intermediate-agent trust....519
7.13.9 pppoe intermediate-agent type self-defined circuit-id....519
7.13.10 pppoe intermediate-agent type self-defined remoteid....520
7.13.11 pppoe intermediate-agent type tr-101 circuit-id access-node-id....520
7.13.12 pppoe intermediate-agent type tr-101 circuit-id identifier-string option delimiter....521
7.13.13 pppoe intermediate-agent vendor-tag strip....521
7.13.14 show pppoe intermediate-agent access-node-id....522
7.13.15 show pppoe intermediate-agent identifier-string option delimiter....522
7.13.16 show pppoe intermediate-agent info....522

7.14 QoS....523
7.14.1 accounting....523
7.14.2 class....523
7.14.3 class-map....523
7.14.4 clear mls qos statistics....524
7.14.5 drop....524
7.14.6 match....524
7.14.7 mls qos aggregate-policy....525
7.14.8 mls qos cos....526
7.14.9 mls qos internal-priority....527
7.14.10 mls qos map....527
7.14.11 mls qos queue weight....528
7.14.12 mls qos trust....529
7.14.13 pass-through-cos....529
7.14.14 pass-through-dscp-exp....529
7.14.15 policy....530
7.14.16 policy aggregate....531
7.14.17 policy-map....531
7.14.18 service-policy input....532
7.14.19 service-policy input vlan....532
7.14.20 set....533
7.14.21 show class-map....533
7.14.22 show policy-map....534
7.14.23 show mls qos interface....534
7.14.24 show mls qos in {interface <interface-name> policy | vlan <vlan-id>....536
7.14.25 show mls qos maps....536
7.14.26 show mls qos vlan....538
7.14.27 show mls qos aggregate-policy....538
7.14.28 transmit....538
7.15 Flow-based Redirection....539
7.15.1 access-group redirect to interface ethernet....539
7.15.2 match vlan <1-4096> redirect interface (ethernet|) IFNAME....539
7.15.3 port-redirect match vlan <1-4094> source-port interface (ethernet|) IFNAME destination-port interface (ethernet|) IFNAME....539
7.15.4 show flow-based-redirect....540
7.15.5 vlan-port-redirect vlan maximum <1-1000>....540
7.16 Egress QoS....540
7.16.1 mls qos egress green remark....540
7.16.2 mls qos map....541
7.16.3 service-policy output....542
7.16.4 service-policy output vlan....543
7.16.5 set....543
7.16.6 show mls qos egress green remark....544
7.16.7 show mls qos maps....544
7.17 Flexible QinQ....544
7.17.1 Add....544
7.17.2 Match....545
7.17.3 service-policy....545
7.17.4 set....546

Chapter 8 Commands for Reliability....547

8.1 MSTP....547
8.1.1 MSTP....547
8.1.2 Monitor and Debug....559
8.1.3 MSTP Spanning-tree Process....561
8.2 VRRP....562
8.2.1 advertisement-interval....562
8.2.2 circuit-failover....562
8.2.3 debug vrrp....563
8.2.4 disable....563
8.2.5 enable....563

8.2.6 interface....564
8.2.7 preempt-mode....564
8.2.8 priority....564
8.2.9 router vrrp....564
8.2.10 show vrrp....565
8.2.11 virtual-ip....565
8.2.12 vrrp track....566
8.3 MRPP....566
8.3.1 control-vlan....566
8.3.2 clear mrpp statistics....567
8.3.3 debug mrpp....567
8.3.4 enable....567
8.3.5 errp domain....568
8.3.6 fail-timer....568
8.3.7 hello-timer....568
8.3.8 mrpp eaps compatible....569
8.3.9 mrpp enable....569
8.3.10 mrpp errp compatible....569
8.3.11 mrpp poll-time....570
8.3.12 mrpp ring....570
8.3.13 mrpp ring primary-port....570
8.3.14 mrpp ring secondary-port....570
8.3.15 node-mode....571
8.3.16 show mrpp....571
8.3.17 show mrpp statistics....571
8.4 ULPP....572
8.4.1 clear ulpp flush counter interface....572
8.4.2 control vlan....572
8.4.3 debug ulpp error....572
8.4.4 debug ulpp event....572
8.4.5 debug ulpp flush {send | receive} interface....573
8.4.6 description....573
8.4.7 flush disable arp....573
8.4.8 flush disable mac....574
8.4.9 flush disable mac-vlan....574
8.4.10 flush enable arp....574
8.4.11 flush enable mac....574
8.4.12 flush enable mac-vlan....575
8.4.13 preemption delay....575
8.4.14 preemption mode....575
8.4.15 protect vlan-reference-instance....576
8.4.16 show ulpp flush counter interface....576
8.4.17 show ulpp flush-receive-port....576
8.4.18 show ulpp group....577
8.4.19 ulpp control vlan....577
8.4.20 ulpp flush disable arp....577
8.4.21 ulpp flush disable mac....578
8.4.22 ulpp flush disable mac-vlan....578
8.4.23 ulpp flush enable arp....578
8.4.24 ulpp flush enable mac....578
8.4.25 ulpp flush enable mac-vlan....579
8.4.26 ulpp group....579
8.4.27 ulpp group master....579
8.4.28 ulpp group slave....580
8.5 ULSM....580
8.5.1 debug ulsm event....580
8.5.2 show ulsm group....580
8.5.3 ulsm group....581
8.5.4 ulsm group {uplink | downlink}....581
8.6 ERPS....581
8.6.1 ethernet tcn-propagation erps to {erps | stp}....581

8.6.2 erps-ring <ring-name>....582
8.6.3 version {v1 | v2}....582
8.6.4 open-ring....583
8.6.5 raps-virtual-channel {with | without}....583
8.6.6 erps-ring <ring-name> port0 [port1-none]....584
8.6.7 erps-ring <ring-name> port1....585
8.6.8 failure-detect {cc | physical-link-or-cc} domain <domain-name> service {< ma-name > | number < ma-num > | pvlan < vlan-id >} mep <mep-id> rmep<rmep-id>....586
8.6.9 erps-instance <instance-id>....586
8.6.10 description....587
8.6.11 ring-id <ring-id>....587
8.6.12 rpl {port0 | port1} {owner | neighbour}....588
8.6.13 non-revertive....589
8.6.14 guard-timer <guard-times>....589
8.6.15 holdoff-timer < holdoff-times>....590
8.6.16 wtr-timer <wtr-times>....590
8.6.17 protected-instance....591
8.6.18 raps-mel <level-value>....591
8.6.19 control-vlan <vlan-id>....592
8.6.20 forced-switch {port0 | port1}....593
8.6.21 manual-switch {port0 | port1}....593
8.6.22 clear command....594
8.6.23 show erps ring {<ring-name> | brief}....595
8.6.24 show erps instance [ring <ring-name> [instance <instance-id>]]....596
8.6.25 show erps status [ring <ring-name> [instance <instance-id>]]....597
8.6.26 show erps statistics [ring <ring-name> [instance <instance-id>]]....597
8.6.27 clear erps statistics [ring <ring-name> [instance <instance-id>]]....598
8.6.28 debug erps....598
8.6.29 debug erps error....599
8.6.30 debug erps event....599
8.6.31 no debug all....599
8.6.32 show debugging....599

Chapter 9 Commands for Debugging and Diagnosis....600

9.1 Monitor and Debug....600
9.1.1 clear history all-users....600
9.1.2 history all-users max-length....600
9.1.3 ping....600
9.1.4 ping6....601
9.1.5 show boot-files....602
9.1.6 show debugging....603
9.1.7 show fan....603
9.1.8 show flash....603
9.1.9 show history....604
9.1.10 show history all-users....604
9.1.11 show memory usage....604
9.1.12 show running-config....605
9.1.13 show running-config current-mode....605
9.1.14 show startup-config....605
9.1.15 show switchport interface....606
9.1.16 show tcp....606
9.1.17 show tcp ipv6....606
9.1.18 show telnet login....607
9.1.19 show temperature....607
9.1.20 show tech-support....607
9.1.21 show udp....608
9.1.22 show udp ipv6....608
9.1.23 show version....608
9.1.24 traceroute....608
9.1.25 traceroute6....609
9.2 Logging....609

9.2.1 logging executed-commands....609
9.2.2 show logging executed-commands state....609
9.3 Reload Switch after Specified Time....610
9.3.1 reload after....610
9.3.2 reload cancel....610
9.3.3 show reload....610
9.4 Debugging and Diagnosis for Packets Received and Sent by CPU....611
9.4.1 clear cpu-rx-stat protocol....611
9.4.2 cpu-rx-limitnotify enable interval....611
9.4.3 cpu-rx-limitnotify protocol (all|WORD)(enable|disable)....611
9.4.4 cpu-rx-ratelimit enhanced....612
9.4.5 cpu-rx-ratelimit protocol....612
9.4.6 cpu-rx-ratelimit total....612
9.4.7 debug driver....613
9.4.8 protocol filter....613
9.4.9 show cpu-rx protocol....613
9.5 CPU-Protect....614
9.5.1 cpu-protect enable....614
9.5.2 cpu-protect log enable....614
9.5.3 cpu-protect trap enable....614
9.5.4 cpu-protect interval....615
9.5.5 cpu-protect recovery-time....615
9.5.6 cpu-protect threshold....615
9.5.7 cpu-protect limit-speed....616
9.5.8 show cpu-protect attack-list....616
9.5.9 show cpu-protect running-config....617
9.6 Info-Center....617
9.6.1 info-center enable....617
9.6.2 info-center prefix....617
9.6.3 info-center match....618
9.6.4 info-center output-enable....619
9.6.5 info-center record-cmd....619
9.6.6 info-center loghost....620
9.6.7 info-center logfile....620
9.6.8 info-center clear....621
9.6.9 show info-center config....621
9.6.10 show info-center logbuffer....622
9.6.11 show info-center trapbuffer....622
9.6.12 show info-center logfile....623
9.6.13 info-center list all disk....624
9.6.14 info-center save all....624
9.7 Mirror....625
9.7.1 monitor session source interface....625
9.7.2 monitor session source interface access-list....625
9.7.3 monitor session destination interface....626
9.7.4 show monitor....626
9.8 RSPAN....626
9.8.1 remote-span....626
9.8.2 monitor session remote vlan....627
9.8.3 monitor session reflector-port....627
9.9 ERSPAN....628
9.9.1 monitor session destination tunnel....628
9.10 sFlow....628
9.10.1 sflow agent-address....628
9.10.2 sflow analyzer....628
9.10.3 sflow counter-interval....629
9.10.4 sflow data-len....629
9.10.5 sflow destination....629
9.10.6 sflow header-len....630
9.10.7 sflow priority....630
9.10.8 sflow rate....630

9.10.9 sflow version....631
9.10.10 show sflow....631
9.11 NQA....632
9.11.1 nqa agent....632
9.11.2 nqa entry type icmp-echo....632
9.11.3 nqa entry type icmp-jitter....633
9.11.4 nqa entry type udp-echo....633
9.11.5 nqa entry type udp-jitter....634
9.11.6 nqa entry type tcp....634
9.11.7 nqa entry type dhcp....634
9.11.8 nqa entry description....635
9.11.9 nqa entry frequency....635
9.11.10 nqa entry probe-count....635
9.11.11 nqa entry probe-timeout....636
9.11.12 nqa entry datasize....636
9.11.13 nqa entry ttl....636
9.11.14 nqa entry tos....637
9.11.15 nqa entry fail-percent....637
9.11.16 nqa entry records-result....637
9.11.17 nqa entry probe-threshold....638
9.11.18 nqa entry start....638
9.11.19 nqa alarm enable....638
9.11.20 nqa traps enable....639
9.11.21 nqa entry alarm enable....639
9.11.22 nqa entry traps enable....639
9.11.23 nqa server....639
9.11.24 nqa server tcp-port....640
9.11.25 nqa server udp-port....640
9.11.26 track nqa....640
9.11.27 track list boolean....641
9.11.28 ip route track....641
9.11.29 rip track....641
9.11.30 ospf track....642
9.11.31 bgp track....642
9.11.32 show nqa results....642
9.11.33 show track status....643

Chapter 10 Commands for Network Time Management....644

10.1 NTP....644
10.1.1 clock timezone....644
10.1.2 debug ntp adjust....644
10.1.3 debug ntp authentication....644
10.1.4 debug ntp events....645
10.1.5 debug ntp packet....645
10.1.6 debug ntp sync....645
10.1.7 ntp access-group....645
10.1.8 ntp authenticate....646
10.1.9 ntp authentication-key....646
10.1.10 ntp broadcast client....646
10.1.11 ntp broadcast server count....646
10.1.12 ntp disable....647
10.1.13 ntp enable....647
10.1.14 ntp ipv6 multicast client....647
10.1.15 ntp multicast client....648
10.1.16 ntp server....648
10.1.17 ntp syn-interval....648
10.1.18 ntp trusted-key....649
10.1.19 show ntp status....649
10.1.20 show ntp session....649
10.2 SNTP....650
10.2.1 clock timezone....650

10.2.2 debug sntp....650
10.2.3 sntp polltime....650
10.2.4 sntp server....651
10.2.5 show sntp....651
10.3 DNSv4/v6....651
10.3.1 clear dynamic-host....651
10.3.2 debug dns....652
10.3.3 dns-server....652
10.3.4 dns lookup....653
10.3.5 show dns name-server....653
10.3.6 show dns domain-list....653
10.3.7 show dns hosts....653
10.3.8 show dns config....654
10.3.9 show dns client....654
10.3.10 ip domain-lookup....654
10.3.11 ip domain-list....655
10.3.12 ip dns server....655
10.3.13 ip dns server queue maximum....655
10.3.14 ip dns server queue timeout....655
10.4 Summer Time....656
10.4.1 clock summer-time absolute....656
10.4.2 clock summer-time recurring....656
10.4.3 clock summer-time recurring....657

Chapter 11 Commands for Virtualization....658
11.1 VSF....658
11.1.1 Basic VSF....658
11.1.2 Configuration and Debugging of VSF Conflict Detection....662
11.1.3 VSF Debugging....664

Chapter 12 Commands for DataCenter....672
12.1 Commands for MC-LAG....672
12.1.1 evpn nve mac-address....672
12.1.2 mac-address....672
12.1.3 mclag....672
12.1.4 mclag domain-id....673
12.1.5 mclag priority....673
12.1.6 mclag enable....673
12.1.7 mclag group....673
12.1.8 mclag local-ip....674
12.1.9 mclag peer-ip....674
12.1.10 ip address....674
12.1.11 ipv6 address....675
12.1.12 mclag dad link....675
12.1.13 error-down exclude....675
12.1.14 mclag up-delay....676
12.1.15 mclag probe-interval....676
12.1.16 show mclag....676
12.1.17 show mclag group....677
12.1.18 switchport mclag data link....677
12.1.19 virtual-equipment-group ID....677
12.1.20 virtual-equipment-group ID....677
12.1.21 virtual-equipment-group ID....678
12.2 Commands for NETCONF....678
12.2.1 netconf server enable....678
12.2.2 show netconf session....678
12.2.3 show netconf tcp....679
12.3 Commands for Telemetry....679
12.3.1 Telemetry....679
12.3.2 grpc server....679
12.3.3 destination-group....680

12.3.4 destination-group ipv4-address....680
12.3.5 sensor-group....680
12.3.6 sensor-group path memoryInfo....681
12.3.7 sensor-group path cpuInfo....681
12.3.8 sensor-group path ifStatistics....681
12.3.9 subscription....682
12.3.10 subscription destination-group....682
12.3.11 subscription sensor-group....683
12.3.12 tun interface vlan....683
12.3.13 show telemetry subscription....683
12.3.14 show telemetry dynamic-subscription....684
12.4 VXLAN Commands....685
12.4.1 arp proxy-answer enable....685
12.4.2 arp suppression enable....685
12.4.3 arp suppress-drop....685
12.4.4 arp suppression table kat....685
12.4.5 clear nvi statistics....686
12.4.6 description....686
12.4.7 description....686
12.4.8 destination....686
12.4.9 flooding disable....687
12.4.10 interface nve....687
12.4.11 interface nvi-interface....687
12.4.12 ip address....688
12.4.13 ipv6 address....688
12.4.14 join nvi....688
12.4.15 mac-address....689
12.4.16 mac-address-table static address nvi....689
12.4.17 nd proxy-answer enable....689
12.4.18 nd suppression enable....689
12.4.19 nd suppress-drop....690
12.4.20 nd suppression table kat....690
12.4.21 nve mode....690
12.4.22 nvi....691
12.4.23 remote ip....691
12.4.24 show interface nve....691
12.4.25 show interface nvi-interface....692
12.4.26 show ipv6 interface nvi-interface....692
12.4.27 show nvi arp suppression....693
12.4.28 show nvi detail....693
12.4.29 show nvi nd suppression....694
12.4.30 show nvi nve tunnel....694
12.4.31 show nvi statistics....695
12.4.32 show virtual-equipment-group ID....695
12.4.33 show virtual-equipment-group ID service....696
12.4.34 show vxlan mac-address-table....696
12.4.35 show vxlan mac-address-table count....697
12.4.36 source....697
12.4.37 source ip....697
12.4.38 virtual-equipment-group ID....698
12.4.39 vxlan remote arp-learning disable....698
12.4.40 vxlan remote mac-address-learning disable....698
12.4.41 vxlan remote nd-learning disable....698
12.4.42 vxlan udp destination-port-number....699
12.4.43 vxlan-id....699
12.4.44 xconnect nvi....699
12.5 EVPN Commands....700
12.5.1 address-family l2vpn evpn....700
12.5.2 distributed-gateway enable....700
12.5.3 dup-addr-detection....700
12.5.4 enable/disable....700

12.5.5 esi....701
12.5.6 evpn....701
12.5.7 evpn nve source-address....701
12.5.8 evpn nvi-vlan-mapping-monitor disable....702
12.5.9 evpn timer df-delay....702
12.5.10 evpn-exit....702
12.5.11 exit-address-family....702
12.5.12 ip vrf forwarding....703
12.5.13 l3-vni....703
12.5.14 rd....703
12.5.15 route-target....704
12.5.16 neighbor activate....704
12.5.17 neighbor route-reflector-client....704
12.5.18 show evpn es....705
12.5.19 show evpn mac-ip....705
12.5.20 show evpn mac-mobility....706
12.5.21 show evpn nvi....706
12.5.22 show ip bgp evpn....707

Chapter 13 Commands for IPv6....709

13.1 DHCPv6....709
13.1.1 clear ipv6 dhcp binding....709
13.1.2 clear ipv6 dhcp conflict....709
13.1.3 clear ipv6 dhcp statistics....709
13.1.4 debug ipv6 dhcp client packet....710
13.1.5 debug ipv6 dhcp detail....710
13.1.6 debug ipv6 dhcp relay packet....710
13.1.7 debug ipv6 dhcp server....710
13.1.8 dns-server....711
13.1.9 domain-name....711
13.1.10 excluded-address....711
13.1.11 ipv6 address....711
13.1.12 ipv6 dhcp client pd....712
13.1.13 ipv6 dhcp client pd hint....712
13.1.14 ipv6 dhcp pool....713
13.1.15 ipv6 dhcp relay destination....713
13.1.16 ipv6 dhcp server....714
13.1.17 ipv6 general-prefix....714
13.1.18 ipv6 local pool....714
13.1.19 lifetime....715
13.1.20 network-address....715
13.1.21 prefix-delegation....716
13.1.22 prefix-delegation pool....716
13.1.23 service dhcpv6....717
13.1.24 show ipv6 dhcp....717
13.1.25 show ipv6 dhcp binding....717
13.1.26 show ipv6 dhcp conflict....718
13.1.27 show ipv6 dhcp interface....718
13.1.28 show ipv6 dhcp pool....718
13.1.29 show ipv6 dhcp statistics....718
13.1.30 show ipv6 general-prefix....720
13.1.31 show ipv6 local pool....720
13.2 DHCPv6 option37, 38....720
13.2.1 Commands for DHCPv6 option37, 38....720
13.2.2 Commands for Monitoring and Debugging....728
13.3 Prevent ND Spoofing....730
13.3.1 ipv6 nd-security updateprotect....730
13.3.2 ipv6 nd-security learnprotect....730
13.3.3 ipv6 nd-security convert....730
13.4 RIPng....731
13.4.1 clear ipv6 route....731

13.4.2 default-information originate....731
13.4.3 default-metric....731
13.4.4 distance....732
13.4.5 distribute-list....732
13.4.6 debug ipv6 rip....733
13.4.7 debug ipv6 rip redistribute message send....733
13.4.8 debug ipv6 rip redistribute route receive....733
13.4.9 ipv6 rip aggregate-address....734
13.4.10 ipv6 rip split-horizon....734
13.4.11 ipv6 router rip....734
13.4.12 neighbor....735
13.4.13 offset-list....735
13.4.14 passive-interface....735
13.4.15 redistribute....736
13.4.16 redistribute ospf....736
13.4.17 route....736
13.4.18 router ipv6 rip....737
13.4.19 show debugging ipv6 rip....737
13.4.20 show ipv6 rip interface....737
13.4.21 show ipv6 rip redistribute....738
13.4.22 show ipv6 protocols rip....738
13.4.23 show ipv6 rip....739
13.4.24 show ipv6 rip database....739
13.4.25 show ipv6 rip aggregate....739
13.4.26 timers basic....740
13.5 OSPFv3....740
13.5.1 area authentication-mode....740
13.5.2 area default cost....741
13.5.3 area range....741
13.5.4 area stub....741
13.5.5 area virtual-link....742
13.5.6 abr-type....742
13.5.7 default-metric....743
13.5.8 debug ipv6 ospf events....743
13.5.9 debug ipv6 ospf ifsm....743
13.5.10 debug ipv6 ospf lsa....744
13.5.11 debug ipv6 ospf nfsm....744
13.5.12 debug ipv6 ospf nsm....744
13.5.13 debug ipv6 ospf packet....744
13.5.14 debug ipv6 ospf redistribute message send....744
13.5.15 debug ipv6 ospf redistribute route receive....745
13.5.16 debug ipv6 ospf route....745
13.5.17 ipv6 ospf authentication-mode....745
13.5.18 ipv6 ospf cost....746
13.5.19 ipv6 ospf dead-interval....746
13.5.20 ipv6 ospf display route single-line....746
13.5.21 ipv6 ospf hello-interval....747
13.5.22 ipv6 ospf priority....747
13.5.23 ipv6 ospf retransmit-interval....748
13.5.24 ipv6 ospf transmit-delay....748
13.5.25 ipv6 router ospf....748
13.5.26 max-concurrent-dd....749
13.5.27 passive-interface....749
13.5.28 redistribute....749
13.5.29 redistribute ospf....750
13.5.30 router-id....750
13.5.31 router ipv6 ospf....751
13.5.32 show ipv6 ospf....751
13.5.33 show ipv6 ospf database....751
13.5.34 show ipv6 ospf interface....752
13.5.35 show ipv6 ospf neighbor....753
13.5.36 show ipv6 ospf route....754

13.5.37 show ipv6 ospf redistribute....754
13.5.38 show ipv6 ospf topology....755
13.5.39 show ipv6 ospf virtual-links....755
13.5.40 show ipv6 route process-detail....755
13.5.41 timers spf....756
13.6 MBGP4+....756
13.6.1 debug ipv6 bgp redistribute message send....756
13.6.2 debug ipv6 bgp redistribute route receive....756
13.6.3 redistribute ospf (MBGP4+)....757
13.6.4 show ipv6 bgp redistribute....757
13.7 Black Hole Routing....757
13.7.1 ipv6 route null0....757
13.8 IPv6 Multicast Protocol....758
13.8.1 Multicast....758
13.8.2 PIM-DM6....759
13.8.3 PIM-SM6....765
13.8.4 ANYCAST RP v6....780
13.8.5 PIM-SSM6....784
13.8.6 IPv6 Multicast Source and Destination Control....784
13.8.7 MLD....790
13.8.8 MLD Snooping....796
13.9 IPv6 Security RA....802
13.9.1 ipv6 security-ra enable....802
13.9.2 ipv6 security-ra enable....802
13.9.3 show ipv6 security-ra....802
13.9.4 debug ipv6 security-ra....803
13.10 SAVI....803
13.10.1 Commands for SAVI....803
13.10.2 Commands for Monitor and Debug....808
13.11 IPv6 VRRPv3....810
13.11.1 advertisement-interval....810
13.11.2 circuit-failover....811
13.11.3 debug ipv6 vrrp....811
13.11.4 disable....811
13.11.5 enable....812
13.11.6 preempt-mode....812
13.11.7 priority....812
13.11.8 router ipv6 vrrp....813
13.11.9 show ipv6 vrrp....813
13.11.10 virtual-ipv6 interface....814

Chapter 14 Commands for VPN....815

14.1 MPLS....815
14.1.1 mpls egress-ttl....815
14.1.2 mpls enable....815
14.1.3 mpls ingress-ttl....815
14.1.4 mpls local-packet-handling....816
14.1.5 mpls mtu....816
14.1.6 show mpls....816
14.1.7 show mpls enable....817
14.1.8 show mpls forwarding-table....817
14.1.9 show mpls ftn-table brief....817
14.1.10 show mpls ftn-table detail....818
14.1.11 show mpls ilm-table....819
14.1.12 show mpls vrf-table....819
14.2 LDP....820
14.2.1 advertisement-mode....820
14.2.2 clear ldp adjacency....821
14.2.3 clear ldp session....821
14.2.4 clear ldp statistics....821
14.2.5 control-mode....822

14.2.6 debug ldp all....822
14.2.7 debug ldp dsm....822
14.2.8 debug ldp error....823
14.2.9 debug ldp events....823
14.2.10 debug ldp fsm....823
14.2.11 debug ldp hexdump....823
14.2.12 debug ldp nsm....824
14.2.13 debug ldp packet....824
14.2.14 debug ldp timer....824
14.2.15 debug ldp tsm....825
14.2.16 debug ldp usm....825
14.2.17 ldp {enable|disable}....825
14.2.18 global-merge-capability....825
14.2.19 hello-interval....826
14.2.20 hold-time....826
14.2.21 import-bgp-routes....827
14.2.22 keepalive-interval....827
14.2.23 keepalive-timeout....827
14.2.24 label-retention-mode....828
14.2.25 label-switching....828
14.2.26 ldp advertisement-mode....829
14.2.27 ldp hello-interval....829
14.2.28 ldp hold-time....829
14.2.29 ldp keepalive-interval....830
14.2.30 ldp keepalive-timeout....830
14.2.31 ldp label-retention-mode....831
14.2.32 ldp multicast-hellos....831
14.2.33 ldp targeted-peer-hello-interval....831
14.2.34 ldp targeted-peer-hold-time....832
14.2.35 loop-detection....832
14.2.36 loop-detection-count....832
14.2.37 multicast-hellos....833
14.2.38 propagate-release....833
14.2.39 request-retry....833
14.2.40 request-retry-timeout....834
14.2.41 router ldp....834
14.2.42 router-id....834
14.2.43 show ldp....835
14.2.44 show ldp adjacency....836
14.2.45 show ldp downstream....836
14.2.46 show ldp fec....837
14.2.47 show ldp interface....837
14.2.48 show ldp lsp....837
14.2.49 show ldp session....838
14.2.50 show ldp statistics....838
14.2.51 show ldp targeted-peers....839
14.2.52 show ldp upstream....839
14.2.53 show mpls ldp discovery....839
14.2.54 show mpls ldp fec....840
14.2.55 show mpls ldp neighbor....840
14.2.56 show mpls ldp parameter....840
14.2.57 show mpls ldp session....842
14.2.58 targeted-hello-accept....842
14.2.59 targeted-peer....842
14.2.60 targeted-peer-hello-interval....842
14.2.61 targeted-peer-hold-time....843
14.2.62 transport-address....843
14.3 MPLS VPN....844
14.3.1 address-family ipv4....844
14.3.2 address-family vpnv4....844
14.3.3 aggregate-address....844
14.3.4 clear ip bgp....845

14.3.5 debug bgp mpls....845
14.3.6 debug bgp update....845
14.3.7 description....846
14.3.8 import map....846
14.3.9 ip route vrf....846
14.3.10 ip vrf....847
14.3.11 ip vrf forwarding vrfName....847
14.3.12 neighbor remote-as....847
14.3.13 neighbor as-override....848
14.3.14 neighbor soo....848
14.3.15 rd....849
14.3.16 route-target....849
14.3.17 show ip bgp vpnv4....849
14.3.18 show ip route vrf....850
14.3.19 show ip vrf....850
14.4 VPLS and VPWS....851
14.4.1 clear mac-address-table....851
14.4.2 debug vpls packet....851
14.4.3 description....851
14.4.4 encapsulation....852
14.4.5 l2-vc....852
14.4.6 mac-address-table limit....852
14.4.7 mac-address-table static address....853
14.4.8 mtu....853
14.4.9 peer....854
14.4.10 pw-class....854
14.4.11 show mpls l2-vc....854
14.4.12 show pw-class....855
14.4.13 show vpls....855
14.4.14 show vpls fib....855
14.4.15 show vfi mac-address-table....856
14.4.16 show vfi mac-address-table count....856
14.4.17 show vpls peer....856
14.4.18 transport-mode....857
14.4.19 ptag....857
14.4.20 vfi....858
14.4.21 vfi vfi-name....858
14.4.22 xconnect l2-vc....858
14.4.23 xconnect vfi....859

Chapter 1 Commands for Basic Switch

1.1 Basic Switch

1.1.1 Basic Configuration

1.1.1.1 authentication line login

Command: authentication line {console | vty | web} login {local | radius | tacacs}
no authentication line {console | vty | web} login

Function: Configures the authentication method priority for VTY (Telnet and SSH), Web, and Console logins. The **no** form of this command restores the default authentication method.

Default: No authentication method is configured for Console logins. Local authentication is enabled for VTY and Web logins.

Command Mode: Global Mode.

Usage Guidelines: You can configure a separate authentication method for Console, VTY, and Web logins. The authentication method can be Local, RADIUS, TACACS, or any combination of them. When multiple methods are configured, they take precedence from left to right. Once a user passes one authentication method, the methods with lower precedence are ignored. If the switch receives an accept or reject response from the server of the current method, it does not try the next method; if it receives no response, it tries the next method. Exception: if local authentication fails, the switch tries the next method. Configure the AAA function and a RADIUS server before you use RADIUS authentication, and configure a TACACS server before you use TACACS authentication. The **authentication line console login** command and the **login** command are mutually exclusive. The **authentication line console login** command configures the authentication method for Console logins, while the **login** command makes Console logins use the password configured with the **password** command.

If local authentication is configured but no local users exist, users can log in to the switch through the Console port.

Example: Configure RADIUS authentication for Telnet and SSH logins.

```
Switch(config)# authentication line vty login radius
```

Related Commands: aaa enable, radius-server authentication host, tacacs-server authentication host, tacacs-server key

1.1.1.2 banner

Command: banner motd <LINE>
no banner motd

Function: Configures the message displayed after a Telnet or Console user successfully passes login authentication. The **no** form of this command removes the message.

Parameters: <LINE>: The message displayed after successful authentication, from 1 to 256 characters.

Default: No message is displayed after successful authentication.

Command Mode: Global Mode.

Example:

```
Switch(config)#banner motd Welcome
```

1.1.1.3 boot img

Command: `boot img <img-file-url> {primary | backup}`

Function: Configures the primary and backup image (IMG) files used the next time the switch boots.

Parameters: primary specifies the primary IMG file; **backup** specifies the backup IMG file. **<img-file-url>** is the full path of the boot IMG file, in the following format:

1. The file path consists of two parts: a device prefix used as the root directory (flash:/) and the file name. Spaces are not allowed within either part or between the two parts.
2. All file names must have the .img extension.
3. The full file path cannot exceed 128 characters, and the file name cannot exceed 80 characters.

Command Mode: Admin Mode.

Default: By factory default, only the primary boot IMG file is specified (nos.img in flash). No backup boot IMG file is specified.

Example:

1. Set flash:/nos.img as the backup boot IMG file for the next system boot.

```
Switch#boot img flash:/nos.img backup
```

2. Set flash:/5.4.128.0_nos.img as the primary boot IMG file for the next system boot.

```
Switch#boot img flash:/5.4.128.0_nos.img primary
```

1.1.1.4 boot startup-config

Command: `boot startup-config {NULL | <file-url> }`

Function: Configures the configuration (CFG) file used the next time the switch boots.

Parameters: The **NULL** keyword specifies that the factory default configuration is used at the next boot. Setting the next-boot CFG file to NULL is equivalent to running the **set default** and **write** commands. **<file-url>** is the full path of the CFG file used at the next boot, in the following format:

1. The file path consists of two parts: a device prefix used as the root directory (flash:/) and the file name. Spaces are not allowed within either part or between the two parts.
2. All file names must have the .cfg extension.
3. The full file path cannot exceed 128 characters, and the file name cannot exceed 80 characters.

Command Mode: Admin Mode.

Default: None.

Example:

1. Set flash:/ startup.cfg as the boot CFG file for the next system boot.

```
Switch# boot startup-config flash:/ startup.cfg
```

2. Set flash:/ test-trunk.cfg as the boot CFG file for the next system boot.

```
Switch#boot startup-config flash:/ test-trunk.cfg
```

1.1.1.5 clock set

Command: `clock set <HH:MM:SS> <YYYY.MM.DD>`

Function: Sets the system date and time.

Parameters: <HH:MM:SS> is the current time, where **HH** ranges from 0 to 23 and **MM** and **SS** range from 0 to 59. **<YYYY.MM.DD>** is the current date, where **YYYY** (year) ranges from 2001 to 2037, **MM** is the month, and **DD** (day) ranges from 1 to 31.

Command Mode: Admin Mode.

Default: At first startup, the system clock defaults to 2006.1.1 0:0:0.

Usage Guidelines: The switch cannot keep time while powered off. Therefore, set the current date and time first in environments that require accurate time.

Example: Set the current date and time of the switch to 2002.8.1 23:0:0.

```
Switch#clock set 23:0:0 2002.8.1
```

Related Commands: show clock

1.1.1.6 config

Command: `config [terminal]`

Function: Enters Global Mode from Admin Mode.

Parameters: terminal specifies terminal configuration.

Command Mode: Admin Mode.

Example:

```
Switch#config
```

1.1.1.7 debug ssh-server

Command: `debug ssh-server`
`no debug ssh-server`

Function: Displays SSH server debugging information. The **no** form of this command stops displaying SSH server debugging information.

Default: Disabled.

Command Mode: Admin Mode.

1.1.1.8 disable

Command: `disable`

Function: Exits Admin Mode.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example:

```
Switch#disable
Switch>
```

1.1.1.9 enable

Command: `enable [<1-15>]`

Function: Enters Admin Mode from User Mode, or changes the user privilege level.

Command Mode: User Mode and Admin Mode.

Default: None.

Usage Guidelines: To prevent unauthorized access by non-admin users, user authentication (the Admin user password) is required to enter Admin Mode from User Mode. If the correct Admin password is entered, access to Admin Mode is granted. If an incorrect password is entered three consecutive times, the user remains in User Mode. When a user changes from a lower privilege level to a higher one, the password for the target level must be authenticated; changing to a lower level does not require a password. Use the **enable password** command in Global Mode to set the Admin user password.

Example:

```
Switch>enable
Switch#
```

1.1.1.10 enable password

Command: enable password [level <1-15>] [0 | 7] <password>
no enable password [level <1-15>]

Function: Configures the password used to enter Admin Mode from User Mode.

The **no enable password** command deletes this password.

Parameters: level <1-15> specifies the privilege level. The default level is 15. **<password>** is the user password. If option 0 is specified, the password is stored unencrypted; if option 7 is specified, the password is stored encrypted.

Command Mode: Global Mode.

Default: No password is configured.

Usage Guidelines: Configure this password to prevent unauthorized access to Admin Mode. We recommend setting this password during the initial switch configuration. We also recommend that administrators exit Admin Mode with the **exit** command before leaving the terminal unattended for a long time.

1.1.1.11 end

Command: end

Function: Exits the current mode and returns to Admin Mode. This command is available in all modes except User Mode and Admin Mode.

Command Mode: All Modes Except User Mode and Admin Mode.

Example: Exit VLAN Mode and return to Admin Mode.

```
Switch(config-vlan1)#end
Switch#
```

1.1.1.12 exec-timeout

Command: exec-timeout <minutes> [<seconds>]
no exec-timeout

Function: Configures the idle timeout for exiting Admin Mode. The **no** form of this command restores the default value.

Parameters: <minutes> is the timeout in minutes, from 0 to 35791. **<seconds>** is the timeout in seconds, from 0 to 59.

Command Mode: Global Mode.

Default: 10 minutes.

Usage Guidelines: To secure the switch and prevent unauthorized users from making changes, the timer starts from the administrator's last operation. When the timer expires, the system exits Admin Mode, and the user must enter the Admin password again to return to Admin Mode. Setting the timeout to 0 disables the timer.

Example: Set the Admin Mode timeout to 6 minutes.

```
Switch(config)#exec-timeout 6
```

Set the Admin Mode timeout to 5 minutes and 30 seconds.

```
Switch(config)#exec-timeout 5 30
```

1.1.1.13 exit

Command: `exit`

Function: Exits the current mode and returns to the previous mode.

Command Mode: All Modes.

Usage Guidelines: Use this command to exit the current mode and return to the previous mode.

Example: Exit the current mode and return to the previous mode.

```
Switch#exit
Switch#
```

1.1.1.14 help

Command: `help`

Function: Displays a brief description of the CLI help system.

Command Mode: All Configuration Modes.

Usage Guidelines: The switch provides instant online help. The **help** command describes the help system, including full help and partial help. You can enter "?" at any time to get online help.

Example:

```
switch(config)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.
If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)
```

1.1.1.15 hostname

Command: `hostname <hostname>`
`no hostname`

Function: Sets the prompt of the switch CLI. The **no** form of this command removes the configured prompt.

Parameters: <hostname> is the prompt string, up to 64 characters.

Command Mode: Global Mode.

Default: The default prompt depends on the switch model.

Usage Guidelines: Use this command to customize the CLI prompt of the switch.

Example: Set the prompt to "Test".

```
Switch(config)#hostname Test
Test(config)#
```

1.1.1.16 ip host

Command: `ip host <hostname> <ip_addr>`
`no ip host {<hostname>|all}`

Function: Maps a host name to an IP address. The **no ip host** command deletes the mapping.

Parameters: <hostname> is the host name, up to 64 characters. **<ip_addr>** is the IP address mapped to the host name, in dotted decimal notation. **all** specifies all host names.

Command Mode: Global Mode.

Usage Guidelines: The host-to-IP address mapping can be used in commands such as **ping <host>**.

Example: Map the host name "test" to IP address 200.121.1.1.

```
Switch(config)#ip host test 200.121.1.1
```

Related Commands: telnet, ping, traceroute

1.1.1.17 ipv6 host

Command: ipv6 host <hostname> <ipv6_addr>
no ipv6 host { <hostname> | all}

Function: Maps a host name to an IPv6 address. The **no** form of this command deletes the mapping.

Parameters: <hostname> is the host name, up to 64 characters. **<ipv6_addr>** is the IPv6 address mapped to the host name. **all** specifies all host names.

Command Mode: Global Mode.

Usage Guidelines: Configures a static mapping between a host name and an IPv6 address for use in commands such as **traceroute6 <host>**.

Example: Map the host name "test" to IPv6 address 2001:1:2:3::1.

```
Switch(config)#ipv6 host test 2001:1:2:3::1
```

Related Commands: ping6, traceroute6

1.1.1.18 ip http server

Command: ip http server
no ip http server

Function: Enables Web-based configuration. The **no ip http server** command disables Web-based configuration.

Default: Enabled.

Command Mode: Global Mode.

Usage Guidelines: Web-based configuration provides an intuitive HTTP-based interface for configuring the switch.

Example: Enable the Web server for Web-based configuration.

```
Switch(config)#ip http server
```

1.1.1.19 language

Command: language {chinese | english}

Function: Sets the display language for help information.

Parameters: chinese displays help in Chinese; **english** displays help in English.

Command Mode: Admin Mode and Configuration Mode.

Default: English.

Usage Guidelines: The switch provides help information in two languages, which users can select as needed. After the system restarts, help information is displayed in English again.

1.1.1.20 login

Command: login
no login

Function: Enables password authentication for Console logins. The **no login** command cancels this configuration.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: After this command is configured, users must enter the password set with the **password** command to enter User Mode through the Console port. The **no login** command removes this requirement.

Example: Enable password authentication for Console logins.

```
Switch(config)#login
```

1.1.1.21 password

Command: password [0 | 7] <password>
no password

Function: Configures the password used to enter User Mode through the Console port. The **no password** command deletes this password.

Parameters: <password> is the user password. If option 0 is specified, the password is stored unencrypted; if option 7 is specified, the password is stored encrypted.

Command Mode: Global Mode.

Default: No password is configured.

Usage Guidelines: When both this password and the **login** command are configured, users must enter this password to enter User Mode through the Console port.

Example:

```
Switch(config)#password 0 test
Switch(config)#login
```

1.1.1.22 password feedback

Command: password feedback {none | star}
no password feedback

Function: Sets how password input is echoed during user login. The **no** form of this command restores the default.

Parameters:

none: Nothing is displayed while the user enters the password.

star: An asterisk (*) is displayed for each character the user enters.

Command Mode: Global Mode.

Default: An asterisk (*) is displayed for each password character.

Usage Guidelines: This setting applies to SSH, Telnet, and Console logins.

Example:

```
Switch(config)# password feedback none
```

1.1.1.23 privilege

Command: privilege mode level <1-15> LINE
no privilege mode level <1-15> LINE

Function: Configures the privilege level of a specified command. The **no** form of this command restores the original level of the command.

Parameters: mode: The mode in which the command is registered. Press Tab or enter "?" to list all modes.

<1-15>: The privilege level, from 1 to 15.

LINE: The command to configure. Command abbreviations are supported.

Command Mode: Global Mode.

Usage Guidelines: This function does not change the command itself. **LINE** must be a complete command; abbreviated commands are accepted only if they can be parsed successfully. The configuration fails for incomplete commands, misspelled commands, and abbreviations that cannot be parsed. For a command with parameters, enter any valid parameter values in the required format. The level specified in the **no** form is optional and does not affect the result. When you use the **no** form, **LINE** must match the configured command line, including any parameters. After you change the privilege level of the **enable** command, configure the **authentication line console login local** command and a username and password with the corresponding privilege so that users can still enter Admin Mode. If the Console connection is in User Mode after the configuration is completed through another login method, enter **exit** or **quit**; the switch then prompts for a username and password to enter Admin Mode.

Example: Change the level of the **show ip route** command to 5.

```
Switch(config)#privilege exec level 5 show ip route
```

Change the level of the **peer A.B.C.D** command to 6.

```
Switch(config)#privilege router-msdp level 6 peer 1.2.3.4
```

Restore the original level of the **show ip route** command.

```
Switch(config)#no privilege exec level 5 show ip route
```

Restore the original level of the **peer A.B.C.D** command.

```
Switch(config)#no privilege router-msdp level 6 peer 1.2.3.4
```

1.1.1.24 reload

Command: `reload`

Function: Performs a warm restart of the switch.

Command Mode: Admin Mode.

Usage Guidelines: Use this command to restart the switch without powering it off.

1.1.1.25 service password-encryption

Command: `service password-encryption`
`no service password-encryption`

Function: Encrypts system passwords. The **no service password-encryption** command disables encryption.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: After this command is executed, existing unencrypted passwords and passwords configured later with the **password**, **enable password**, **ip ftp**, and **username** commands are encrypted. The **no service password-encryption** command disables this function, but passwords that are already encrypted remain encrypted.

Example: Encrypt system passwords.

```
Switch(config)#service password-encryption
```

1.1.1.26 service terminal-length

Command: `service terminal-length <0-512>`
`no service terminal-length`

Function: Configures the number of lines displayed per screen on a VTY terminal. The **no service terminal-length** command disables screen paging.

Parameters: The number of lines displayed per screen on a VTY terminal, from 0 to 512.

Command Mode: Global Mode.

Usage Guidelines: Configures the number of lines displayed per screen on the terminal. This setting applies to Telnet and SSH clients and to the Console.

Example: Set the number of lines displayed per screen to 20.

```
Switch(config)#service terminal-length 20
```

1.1.1.27 sysContact

Command: `sysContact <LINE>`
`no sysContact`

Function: Sets the system contact information. The **no sysContact** command restores the factory setting.

Parameters: <LINE> is the contact string, from 0 to 255 characters.

Command Mode: Global Mode.

Default: Factory setting.

Usage Guidelines: Set the contact information according to your deployment.

Example: Set the system contact to "test".

```
Switch(config)#sysContact test
```

1.1.1.28 sysLocation

Command: `sysLocation <LINE>`
`no sysLocation`

Function: Sets the system location information. The **no sysLocation** command restores the factory setting.

Parameters: <LINE> is the location string, from 0 to 255 characters.

Command Mode: Global Mode.

Default: Factory setting.

Usage Guidelines: Set the location information according to your deployment.

Example: Set the system location to "test".

```
Switch(config)#sysLocation test
```

1.1.1.29 set default

Command: `set default`

Function: Restores the switch to factory settings.

Command Mode: Admin Mode.

Usage Guidelines: Restores the switch to factory settings; all user configurations are cleared. After the switch restarts, the prompt is the same as when the switch was powered on for the first time.

Note: After running this command, run the **write** command to save the change. The switch returns to factory settings after it restarts.

Example:

```
Switch#set default
Are you sure? [Y/N] = y
Switch#write
Switch#reload
```

1.1.1.30 setup

Command: `setup`

Function: Enters the Setup Mode of the switch.

Command Mode: Admin Mode.

Usage Guidelines: The switch provides a Setup Mode in which users can configure settings such as IP addresses.

1.1.1.31 show clock

Command: `show clock`

Function: Displays the current system time.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: If the system clock is inaccurate, check the system date and time and adjust them as needed.

Example:

```
Switch#show clock
Current time is TUE AUG 22 11：00：01 2002
```

Related Commands: clock set

1.1.1.32 show cpu usage

Command: `show cpu usage [<slotno>]`

Function: Displays the CPU usage.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Use this command to check the current CPU usage. The **<slotno>** parameter is used only on chassis-based switches to display the CPU usage of the card in the specified slot. If no parameter is specified, the command displays the CPU usage of the current card.

Example: Display the current CPU usage.

```
Switch#show cpu usage
Last  5 second CPU IDLE:  87%
Last 30 second CPU IDLE:  89%
Last  5 minute CPU IDLE:  89%
From  running  CPU IDLE:  89%
```

1.1.1.33 show cpu utilization

Command: `show cpu utilization`

Function: Displays the current CPU utilization.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays the CPU utilization over the last 5 seconds, 30 seconds, and 5 minutes.

Example: Display the CPU utilization.

```
Switch#show cpu utilization
Last  5 second CPU USAGE:   9%
Last 30 second CPU USAGE:  11%
Last  5 minute CPU USAGE:  11%
From  running  CPU USAGE:  11%
```

1.1.1.34 show memory usage

Command: `show memory usage [<slotno>]`

Function: Displays the memory usage.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Use this command to check the current memory usage. The **<slotno>** parameter is used only on chassis-based switches to display the memory usage of the card in the specified slot. If no parameter is specified, the command displays the memory usage of the current card.

Example: Display the current memory usage.

```
Switch#show memory usage
The memory total 128 MB, free 58914872 bytes, usage is 56.10%
```

1.1.1.35 show privilege

Command: `show privilege`

Function: Displays the privilege level of the current user.

Parameters: None.

Command Mode: All Configuration Modes.

Example: Display the privilege level of the current user.

```
Switch(Config)#show privilege
Current privilege level is 15
```

1.1.1.36 show privilege mode LINE

Command: `show privilege mode LINE`

Function: Displays the privilege level of a specified command.

Parameters: mode: The mode in which the command is registered. Press Tab or enter "?" to list all modes.

LINE: The command to query. Command abbreviations are supported.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: LINE must be a complete command; abbreviated commands are accepted only if they can be parsed successfully. The level cannot be displayed for incomplete commands, misspelled commands, or abbreviations that cannot be parsed.

Example: Display the privilege level of the **show ip route** command.

```
Switch(config)#show privilege exec show ip route
The command : show ip route
Privilege is : 15
```

1.1.1.37 show tcam usage

Command: `show tcam usage`

Function: Displays the current ACL (TCAM) resource usage of the switch.

Command Mode: All Modes.

Usage Guidelines: Use this command to display the current ACL resource usage of the switch.

Example:

```
Switch(Config)#show tcam usage
TCAM Total: 1024 extended (2048 standard) entries on unit: 0
     USED:  25   extended entries for l4 function
     FREE:  999  extended entries
```

1.1.1.38 show temperature

Command: `show temperature`

Function: Displays the current CPU temperature of the switch.

Command Mode: All Modes.

Usage Guidelines: Use this command to monitor the CPU temperature of the switch.

Example: Display the current CPU temperature of the switch.

```
Switch(Config)#show temperature
Temperature: 47.0625 ℃
```

1.1.1.39 show tech-support

Command: `show tech-support [no-more]`

Function: Displays operational information and task status of the switch. Technical support engineers use this command to diagnose whether the switch is operating normally.

Parameters: no-more: Displays all output at once without "--More--" paging.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Use this command to collect relevant information when the switch is not operating properly.

Example:

```
Switch#show tech-support
```

1.1.1.40 show version

Command: `show version`

Function: Displays the version information of the switch.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the switch version information, including the hardware and software versions.

Example:

```
Switch#show version.
```

1.1.1.41 username

Command: `username <username> [privilege <privilege>] [password [0 | 7] <password>]`
`no username <username>`

Function: Configures a local login username and password and the user's privilege level.

Parameters: <username> is the username, up to 32 characters. **<privilege>** is the highest privilege level of commands the user can execute, from 1 to 15; the default is 1. **<password>** is the user password. If option 0 is specified, the password is stored unencrypted; if option 7 is specified, the password is entered in encrypted form (a 32-character MD5-encrypted string).

Command Mode: Global Mode.

Usage Guidelines: Commands registered on the switch have one of two privilege levels: 1 or 15. Level 1 applies to commands in User Mode; level 15 applies to commands registered in all other modes. Up to 16 local users can be configured with this command. The maximum password length is not less than 32 characters.

Note: After the user is configured, the user can log in with the configured username and privilege level. Before you configure the **authentication line console login local** command, make sure that at least one user with privilege level 15 is configured, so that you can log in to the switch and make changes in Admin Mode and Global Mode. If no local user with privilege level 15 exists and only local authentication is configured for Console logins, users can log in to the switch without authentication. For HTTP logins, only users with privilege level 15 can log in; users with any other level are denied.

Example: Configure an administrator account named "admin" with privilege level 15 and two normal accounts with privilege level 1, and then enable local authentication.

With this configuration, only the user "admin" can log in to the switch in Admin Mode through Telnet or the Console port; "user1" and "user2" can log in only in User Mode through Telnet or the Console port. For HTTP logins, only "admin" passes authentication; "user1" and "user2" are denied.

```
Switch(config)#username admin privilege 15 password 0 admin
Switch(config)# username user1 privilege 1 password 7
4a7d1ed414474e4033ac29ccb8653d9b (32-character MD5-encrypted password)
Switch(config)# username user2 password 0 user2
Switch(config)# authentication line console login local
```

1.1.1.42 web-auth privilege <1-15>

Command: `web-auth privilege <1-15>`
`no web-auth privilege`

Function: Configures the privilege level required to log in to the switch through the Web interface.

Parameters: <1-15>: The privilege level required for Web login, from 1 to 15.

Command Mode: Global Mode.

Default: 15.

Usage Guidelines: After this level is configured, only users with a privilege level equal to or higher than this level can log in to the switch through the Web interface.

Example: Set the privilege level required for Web login to 10.

```
Switch(config)# web-auth privilege 10
```

1.1.1.43 write

Command: `write`

Function: Saves the current configuration to flash memory.

Command Mode: Admin Mode.

Usage Guidelines: After configuring the required functions, save the settings to the configuration file so that the system automatically restores the saved configuration after an accidental power-off or power failure. This command is equivalent to the **copy running-config startup-config** command.

1.1.1.44 write running-config

Command: `write running-config [<startup-config-file-name>]`

Function: Saves the current running configuration to flash memory as a .cfg file.

Parameters: <startup-config-file-name> is the full path of the .cfg file, in the following format:

1. The file path consists of two parts: a device prefix used as the root directory (flash:/) and the file name. Spaces are not allowed within either part or between the two parts.
2. All file names must have the .cfg extension.
3. The full file path cannot exceed 128 characters, and the file name cannot exceed 121 characters.

Command Mode: Admin Mode.

Usage Guidelines: A configuration file saved in flash memory can be used as the startup configuration file.

Example: Save the current running configuration as a .cfg file named 123.

```
Switch#write running-config 123.cfg
```

1.1.2 Telnet

1.1.2.1 aaa authorization config-commands

Command: `aaa authorization config-commands`
`no aaa authorization config-commands`

Function: Enables command authorization for users who log in through VTY (Telnet and SSH). The **no** form of this command disables this function. Authorization is requested when certain commands are executed only if this command is enabled and a command authorization method is configured.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Commands at the corresponding command level are authorized for VTY users only after this command is enabled and both the command authorization method and its priority are configured for VTY logins.

Example: Enable command authorization for VTY users.

```
Switch(config)# aaa authorization config-commands
```

1.1.2.2 accounting exec

Command: `accounting line {console | vty} exec {start-stop | stop-only | none} method1 [method2…]`
`no accounting line {console | vty} exec`

Function: Configures the accounting method list for users who log in through VTY (Telnet and SSH) and the Console port. The **no** form of this command restores the default accounting method.

Parameters: line specifies the line type: **console** or **vty** (Telnet and SSH). **start-stop** sends an accounting-start record when the user logs in and an accounting-stop record when the user logs out. **stop-only** sends only an accounting-stop record when the user logs out. **none** sends no accounting records. **method** is the accounting method list; only the **tacacs** keyword is supported, which uses a remote TACACS+ server for accounting.

Default: No accounting is configured.

Command Mode: Global Mode.

Usage Guidelines: You can configure a separate accounting method for **console** and **vty** logins. Currently, only the TACACS+ accounting method is supported.

Example: Configure login accounting for Telnet users.

```
Switch(config)#accounting line vty exec start-stop tacacs
```

1.1.2.3 authentication enable

Command: `authentication enable method1 [method2…]`
`no authentication enable`

Function: Configures the authentication method list for entering Admin Mode with the **enable** command. The **no** form of this command restores the default authentication method.

Parameters: method is the authentication method list, which can include the keywords **local**, **tacacs**, and **radius**. **local** uses the local database; **tacacs** uses a remote TACACS+ authentication server; **radius** uses a remote RADIUS authentication server.

Default: Local authentication.

Command Mode: Global Mode.

Usage Guidelines: The enable authentication method can be Local, RADIUS, TACACS, or any combination of them. When multiple methods are configured, they take precedence from left to right. Once a user passes one authentication method, the methods with lower precedence are ignored. If the switch receives an accept or reject response from the server of the current method, it does not try the next method; if it receives no response, it tries the next method. Exception: if local authentication fails, the switch tries the next method. Configure the AAA function and a RADIUS server before you use RADIUS authentication, and configure a TACACS server before you use TACACS authentication.

Example: Configure TACACS and local authentication for the enable password.

```
Switch(config)#authentication enable tacacs local
```

1.1.2.4 authentication ip access-class

Command: `authentication ip access-class {<num-std>|<name>}`
`no authentication ip access-class`

Function: Binds a standard IP ACL to Telnet, SSH, and Web logins. The **no** form of this command removes the ACL binding.

Parameters: <num-std> is the number of a numbered standard ACL, from 1 to 299. **<name>** is the name of a named standard ACL, from 1 to 64 characters.

Default: No ACL is bound to Telnet, SSH, or Web logins.

Command Mode: Global Mode.

Example: Bind standard IP ACL 1 to Telnet, SSH, and Web logins.

```
Switch(config)#authentication ip access-class 1 in
```

1.1.2.5 authentication ipv6 access-class

Command: `authentication ipv6 access-class {<num-std>|<name>} in`
`no authentication ipv6 access-class`

Function: Binds a standard IPv6 ACL to Telnet, SSH, and Web logins. The **no** form of this command removes the ACL binding.

Parameters: <num-std> is the number of a numbered standard IPv6 ACL, from 500 to 599. **<name>** is the name of a named standard ACL, from 1 to 64 characters.

Default: No ACL is bound to Telnet, SSH, or Web logins.

Command Mode: Global Mode.

Example: Bind standard IPv6 ACL 500 to Telnet, SSH, and Web logins.

```
Switch(config)#authentication ipv6 access-class 500 in
```

1.1.2.6 authentication line login

Command: `authentication line {console | vty | web} login method1 [method2…]`
`no authentication line {console | vty | web} login`

Function: Configures the authentication method list for users who log in through VTY (Telnet and SSH), the Web interface, and the Console port. The **no** form of this command restores the default authentication method.

Parameters: line specifies the login line: **console**, **vty** (Telnet and SSH), or **web**. **method** is the authentication method list, which can include the keywords **local**, **tacacs**, and **radius**. **local** uses the local database; **tacacs** uses a remote TACACS+ authentication server; **radius** uses a remote RADIUS authentication server.

Default: No authentication method is configured for Console logins. Local authentication is enabled for VTY and Web logins.

Command Mode: Global Mode.

Usage Guidelines: You can configure a separate authentication method for Console, VTY, and Web logins. The authentication method can be Local, RADIUS, TACACS, or any combination of them. When multiple methods are configured, they take precedence from left to right. Once a user passes one authentication method, the methods with lower precedence are ignored. If the switch receives an accept or reject response from the server of the current method, it does not try the next method; if it receives no response, it tries the next method. Exception: if local authentication fails, the switch tries the next method. Configure the AAA function and a RADIUS server before you use RADIUS authentication, and configure a TACACS server before you use TACACS authentication.

The **authentication line console login** command and the **login** command are mutually exclusive. The **authentication line console login** command configures the authentication method for Console logins, while the **login** command makes Console logins use the password configured with the **password** command.

If local authentication is configured but no local users exist, users can log in to the switch through the Console port.

Example: Configure remote RADIUS authentication for Telnet and SSH logins.

```
Switch(config)#authentication line vty login radius
```

Related Commands: aaa enable, radius-server authentication host, tacacs-server authentication host, tacacs-server key

1.1.2.7 authentication securityip

Command: `authentication securityip <ip-addr>`
`no authentication securityip <ip-addr>`

Function: Configures a trusted IP address for Telnet and HTTP logins. The **no** form of this command removes the trusted IP address.

Parameters: <ip-addr> is the IP address, in dotted decimal notation, of a client that is allowed to log in to the switch.

Default: No trusted IP address is configured.

Command Mode: Global Mode.

Usage Guidelines: Until a trusted IP address is configured, clients can log in to the switch from any IP address. After a trusted IP address is configured, only clients with a trusted IP address can log in to the switch. Up to 32 trusted IP addresses can be configured.

Example: Configure 192.168.1.21 as a trusted IP address.

```
Switch(config)# authentication securityip 192.168.1.21
```

1.1.2.8 authentication securityipv6

Command: `authentication securityipv6 <ipv6-addr>`
`no authentication securityipv6 <ipv6-addr>`

Function: Configures a trusted IPv6 address for Telnet and HTTP logins. The **no** form of this command removes the specified address.

Parameters: <ipv6-addr> is the IPv6 address of a client that is allowed to log in to the switch.

Default: No trusted IPv6 address is configured.

Command Mode: Global Mode.

Usage Guidelines: Until a trusted IPv6 address is configured, clients can log in to the switch from any IPv6 address. After a trusted IPv6 address is configured, only clients with a trusted IPv6 address can log in to the switch. Up to 32 trusted IPv6 addresses can be configured.

Example: Configure 2001:da8:123:1::1 as a trusted IPv6 address.

```
Switch(config)# authentication securityipv6 2001:da8:123:1::1
```

1.1.2.9 authorization

Command: `authorization line {console | vty | web} exec method [method…]`
`no authorization line {console | vty | web} exec`

Function: Configures the authorization method list for users who log in through VTY (Telnet and SSH), the Web interface, and the Console port. The **no** form of this command restores the default authorization method.

Parameters: line specifies the login line: **console**, **vty** (Telnet and SSH), or **web**. **method** is the authorization method list, which can include the keywords **local**, **tacacs**, and **radius**. **local** uses the local database; **tacacs** uses a remote TACACS+ server; **radius** uses a remote RADIUS server.

Default: No authorization method is configured.

Command Mode: Global Mode.

Usage Guidelines: You can configure a separate authorization method for Console, VTY, and Web logins. The authorization method can be Local, RADIUS, TACACS, or any combination of them. When multiple methods are configured, they take precedence from left to right. Once a user passes one authorization method, the methods with lower precedence are ignored. If the switch receives an accept or reject response from the server of the current method, it does not try the next method; if it receives no response, it tries the next method. Configure the AAA function and a RADIUS server before you use RADIUS authorization, and configure a TACACS server before you use TACACS authorization.

If no authorization method is configured, local users receive the privilege configured with the **username** command, and users who log in through RADIUS or TACACS work in User Mode.

Example: Configure RADIUS authorization for Telnet users.

```
Switch(config)#authorization line vty exec radius
```

1.1.2.10 authorization line vty command

Command: `authorization line vty command <1-15>  {local | radius | tacacs} (none|)`
`no authorization line vty command <1-15>`

Function: Configures the command authorization methods and their priority for users who log in through VTY (Telnet and SSH). The **no** form of this command restores the default.

Default: No command authorization method is configured.

Command Mode: Global Mode.

Usage Guidelines: Configures the authorization method used when a VTY user enters commands. The methods can be any combination of Local, RADIUS, and TACACS, and **none** can be specified as the last method. When multiple methods are configured, the first method has the highest priority and the rest follow in descending order; if a higher-priority method authorizes the command, the command is executed and the remaining methods are ignored. Note: if a method receives an explicit response from the corresponding protocol, whether accept or reject, the next method is not tried; the next method is tried only if no explicit response is received. RADIUS authorization requires the AAA function to be enabled and a RADIUS server to be configured. TACACS authorization requires a TACACS server to be configured. **none** is a fallback method and can only be the last method; it authorizes the command directly so that the command is executed.

Example: Configure TACACS as the command authorization method for level 1 commands of Telnet users.

```
Switch(config)#authorization line vty command 1 tacacs
```

1.1.2.11 clear line vty <0-31>

Command: `clear line vty <0-31>`

Function: Clears the information of the user logged in on the specified line and forcibly disconnects the user logged in through Telnet or SSH.

Command Mode: Admin Mode.

Usage Guidelines: After you enter this command, the switch prompts "Confirm[Y/N]:". Enter "Y" or "y" to clear the line. Enter "N" to cancel; the switch only displays a notice. Any other input also cancels the operation.

1.1.2.12 crypto key clear rsa

Command: `crypto key clear rsa`

Function: Clears the SSH key.

Command Mode: Admin Mode.

1.1.2.13 terminal length

Command: `terminal length <0-512>`
`terminal no length`

Function: Sets the number of lines displayed per screen on the terminal. The **terminal no length** command disables paging so that all output is displayed at once.

Parameters: The number of lines displayed per screen, from 0 to 512. A value of 0 displays output without pausing.

Command Mode: Admin Mode.

Default: 25.

Usage Guidelines: Sets the number of lines displayed per screen on the terminal. When the output exceeds one screen, the "--More--" prompt is displayed; press any key to display the next screen. The default length is 25 lines.

Example: Set the number of lines displayed per screen to 20.

```
Switch#terminal length 20
```

1.1.2.14 terminal monitor

Command: `terminal monitor`
`terminal no monitor`

Function: Displays debugging messages on the current terminal. The **terminal no monitor** command restores the default.

Command Mode: Admin Mode.

Usage Guidelines: Configures whether debugging messages are displayed on the current terminal. If this command is configured on a Telnet or SSH client, debugging messages are sent to that client. By default, debugging messages are displayed on the Console.

Example:

```
Switch#terminal monitor
```

1.1.2.15 telnet

Command: `telnet [vrf <vrf-name>] {<ip-addr> | <ipv6-addr> | host <hostname>} [<port>]`

Function: Logs in to a remote host through Telnet.

Parameters: <vrf-name> is the VRF name. **<ip-addr>** is the IP address of the remote host, in dotted decimal notation. **<ipv6-addr>** is the IPv6 address of the remote host. **<hostname>** is the name of the remote host, up to 64 characters. **<port>** is the port number, from 0 to 65535.

Command Mode: Admin Mode.

Usage Guidelines: Use this command when the switch acts as a Telnet client to log in to and configure a remote host. As a Telnet client, the switch can establish only one TCP connection with a remote host at a time. To connect to another remote host, first disconnect the current TCP connection with the hotkey Ctrl+\. To Telnet to a host name, first configure the mapping between the host name and its IP or IPv6 address with the **ip host** or **ipv6 host** command. If a host name maps to both an IPv4 and an IPv6 address, the IPv6 address is preferred.

Example: Telnet from the switch to a remote host with IP address 20.1.1.1.

```
Switch#telnet 20.1.1.1 23
Connecting Host 20.1.1.1 Port 23...
Service port is 23
Connected to 20.1.1.1
login:123
password:***
router>
```

1.1.2.16 telnet server enable

Command: `telnet server enable`
`no telnet server enable`

Function: Enables the Telnet server on the switch. The **no telnet server enable** command disables the Telnet server.

Default: Enabled.

Command Mode: Global Mode.

Usage Guidelines: This command is available only from the Console. Administrators can use it to allow or deny Telnet client logins to the switch.

Example: Disable the Telnet server on the switch.

```
Switch(config)#no telnet server enable
```

1.1.2.17 telnet-server max-connection

Command: `telnet-server max-connection {<max-connection-number> | default}`

Function: Configures the maximum number of concurrent Telnet connections supported by the switch.

Parameters: <max-connection-number>: The maximum number of Telnet connections, from 1 to 16. **default** restores the default value.

Default: 5.

Command Mode: Global Mode.

Usage Guidelines: None.

Example: Set the maximum number of Telnet connections to 10.

```
Switch(config)#telnet-server max-connection 10
```

1.1.2.18 ssh-server authentication-retries

Command: `ssh-server authentication-retries <authentication-retries>`
`no ssh-server authentication-retries`

Function: Configures the number of SSH authentication retries. The **no ssh-server authentication-retries** command restores the default.

Parameters: <authentication-retries> is the number of authentication retries, from 1 to 10.

Command Mode: Global Mode.

Usage Guidelines: None.

Default: 3.

Example: Set the number of SSH authentication retries to 5.

```
Switch(config)#ssh-server authentication-retries 5
```

1.1.2.19 ssh-server enable

Command: `ssh-server enable`
`no ssh-server enable`

Function: Enables the SSH server on the switch. The **no ssh-server enable** command disables the SSH server.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: For SSH clients to log in to the switch, configure an SSH user and enable the SSH server on the switch.

Example: Enable the SSH server on the switch.

```
Switch(config)#ssh-server enable
```

1.1.2.20 ssh-server host-key create rsa

Command: `ssh-server host-key create rsa [modulus < modulus >]`

Function: Generates a new RSA host key.

Parameters: modulus is the modulus used to compute the host key, from 768 to 2048. The default is 1024.

Command Mode: Global Mode.

Default: The system uses the key generated when the SSH server is first started.

Usage Guidelines: Use this command to generate a new host key, which is then used to authenticate the server when an SSH client logs in. After the new host key is generated and the configuration is saved with the **write** command, the system always uses this key for authentication. Because computing a new key takes a long time and some clients are not compatible with keys generated with a modulus of 2048, we recommend using the default modulus of 1024.

Example: Generate a new host key.

```
Switch(config)#ssh-server host-key create rsa
```

1.1.2.21 ssh-server max-connection

Command: `ssh-server max-connection {<max-connection-number>|default}`

Function: Configures the maximum number of concurrent SSH connections supported by the switch.

Parameters: <max-connection-number>: The maximum number of SSH connections, from 1 to 16. **default** restores the default value.

Default: 5.

Command Mode: Global Mode.

Usage Guidelines: None.

Example: Set the maximum number of SSH connections to 10.

```
Switch(config)#ssh-server max-connection 10
```

1.1.2.22 ssh-server timeout

Command: `ssh-server timeout <timeout>`
`no ssh-server timeout`

Function: Configures the SSH authentication timeout. The **no ssh-server timeout** command restores the default timeout.

Parameters: <timeout> is the timeout value, from 10 to 600 seconds.

Command Mode: Global Mode.

Default: 180 seconds.

Usage Guidelines: Sets the SSH authentication timeout. The default is 180 seconds.

Example: Set the SSH authentication timeout to 240 seconds.

```
Switch(config)#ssh-server timeout 240
```

1.1.2.23 show crypto key

Command: `show crypto key`

Function: Displays the SSH key.

Command Mode: Admin Mode.

1.1.2.24 show ssh-server

Command: `show ssh-server`

Function: Displays the SSH server status and the users currently logged in.

Command Mode: Admin Mode.

Example:

```
Switch#show ssh-server
ssh server is enabled
ssh-server timeout 180s
ssh-server authentication-retries 3
ssh-server max-connection number 6
ssh-server login user number 2
```

1.1.2.25 show telnet login

Command: `show telnet login`

Function: Displays information about Telnet clients currently connected to the switch.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Use this command to check the Telnet clients connected to the switch.

Example:

```
Switch#show telnet login
Authenticate login by local
Login user:
aa
```

1.1.2.26 show users

Command: `show users`

Function: Displays information about users logged in through Telnet or SSH, including the line number, username, and user IP address.

Command Mode: Admin Mode.

Usage Guidelines: Displays information about users logged in through Telnet or SSH, including the line number, username, and user IP address. Up to 16 Telnet users and 16 SSH users are supported: lines vty 0–15 are used for Telnet and lines vty 16–31 are used for SSH.

Example:

```
Switch#show users
Line              User                                Location
vty 16            a                                   192.168.1.1
vty 0             admin                               192.168.1.2
vty 17            mab                                 192.168.1.13
vty 1             test                                192.168.1.40
```

1.1.2.27 who

Command: `who`

Function: Displays the users currently logged in through VTY.

Parameters: None.

Command Mode: All Configuration Modes.

Example: Display the users currently logged in through VTY.

```
Switch#who
Telnet user a login from 192.168.1.20
```

1.1.3 Configuring Switch IP

1.1.3.1 interface vlan

Command: `interface vlan <vlan-id>`
`no interface vlan <vlan-id>`

Function: Enters VLAN Interface Mode. The **no** form of this command deletes the specified VLAN interface.

Parameters: <vlan-id> is the ID of an existing VLAN, from 1 to 4094.

Command Mode: Global Mode.

Usage Guidelines: Make sure the VLAN exists before you configure its interface. Use the **exit** command to return from VLAN Interface Mode to Global Mode.

Example: Enter VLAN Interface Mode for VLAN 1.

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#
```

1.1.3.2 ip address

Command: `ip address <ip-address> <mask> [secondary]`
`no ip address [<ip-address> <mask>] [secondary]`

Function: Sets the IP address and subnet mask of the specified VLAN interface. The **no ip address [<ip-address> <mask>] [secondary]** command deletes the specified IP address.

Parameters: <ip-address> is the IP address in dotted decimal notation. **<mask>** is the subnet mask in dotted decimal notation. **secondary** specifies that the address is a secondary IP address.

Default: No IP address is configured at the factory.

Command Mode: VLAN Interface Mode.

Usage Guidelines: Create a VLAN interface before you assign an IP address to the switch.

Example: Set 10.1.128.1/24 as the IP address of the VLAN 1 interface.

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.128.1 255.255.255.0
Switch(Config-if-Vlan1)#exit
Switch(config)#
```

Related Commands: ip bootp-client enable, ip dhcp-client enable

1.1.3.3 ipv6 address

Command: ipv6 address <ipv6address | prefix-length> [eui-64]
no ipv6 address <ipv6address | prefix-length> [eui-64]

Function: Configures an aggregatable global unicast address, site-local address, or link-local address for the interface.

Parameters: <ipv6address> is the IPv6 address prefix. **<prefix-length>** is the prefix length, from 3 to 128. **eui-64** specifies that the IPv6 address is generated automatically from the EUI-64 interface ID of the interface.

Command Mode: Interface Mode.

Default: None.

Usage Guidelines: The IPv6 address prefix cannot be a multicast address or any other special-purpose IPv6 address. Different Layer 3 VLAN interfaces cannot share the same address prefix. For a global unicast address, the prefix must be in the range 2001:: to 3fff:: and the prefix length must be at least 3. For a site-local or link-local address, the prefix length must be at least 10.

Example: Configure an IPv6 address with prefix 2001:3f:ed8::99 and prefix length 64 on the Layer 3 interface of VLAN 1.

```
Switch(Config-if-Vlan1)#ipv6 address 2001:3f:ed8::99/64
```

1.1.3.4 ip bootp-client enable

Command: ip bootp-client enable
no ip bootp-client enable

Function: Enables the switch to act as a BootP client and obtain an IP address and gateway address through BootP. The **no ip bootp-client enable** command disables the BootP client and releases the IP address obtained through BootP.

Default: Disabled.

Command Mode: VLAN Interface Mode.

Usage Guidelines: BootP, manual configuration, and DHCP are mutually exclusive methods of obtaining an IP address; only one can be enabled at a time. Note: Obtaining an IP address through BootP requires a DHCP server or BootP server on the network.

Example: Obtain an IP address through BootP.

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip bootp-client enable
Switch (Config-if-Vlan1)#exit
Switch(config)#
```

Related Commands: ip address, ip dhcp-client enable

1.1.3.5 ip dhcp-client enable

Command: `ip dhcp-client enable`
`no ip dhcp-client enable`

Function: Enables the switch to act as a DHCP client and obtain an IP address and gateway address through DHCP. The **no ip dhcp-client enable** command disables the DHCP client and releases the IP address obtained through DHCP. Note: Obtaining an IP address through DHCP requires a DHCP server on the network.

Default: Disabled.

Command Mode: VLAN Interface Mode and Interface Mode.

Usage Guidelines: DHCP, manual configuration, and BootP are mutually exclusive methods of obtaining an IP address; only one can be enabled at a time.

Example: Obtain an IP address through DHCP.

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip dhcp-client enable
Switch(Config-if-Vlan1)#exit
Switch(config)#
```

1.1.3.6 ip dhcp-client upgrade enable

Command: `ip dhcp-client upgrade enable`
`no ip dhcp-client upgrade enable`

Function: Enables automatic upgrade of IMG and CFG files through DHCP options 66 and 67. The **no** form of this command disables automatic upgrade through DHCP options 66 and 67.

Default: Disabled.

Command Mode: VLAN Interface Mode and Interface Mode.

Usage Guidelines: Enables the switch to automatically upgrade IMG and CFG files through DHCP options 66 and 67.

Example: Enable DHCP automatic upgrade.

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip dhcp-client enable
Switch(Config-if-Vlan1)#ip dhcp-client upgrade enable
Switch(Config-if-Vlan1)#exit
Switch(config)#
```

Related Commands: ip dhcp-client enable

1.1.3.7 ip dhcp-client upgrade begin

Command: `ip dhcp-client upgrade begin`

Function: Starts automatic upgrade of IMG and CFG files through DHCP options 66 and 67.

Default: Disabled.

Command Mode: VLAN Interface Mode and Interface Mode.

Usage Guidelines: Starts the automatic upgrade of IMG and CFG files through DHCP options 66 and 67.

Example: Start DHCP automatic upgrade.

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip dhcp-client enable
Switch(Config-if-Vlan1)#ip dhcp-client upgrade enable
Switch(Config-if-Vlan1)#ip dhcp-client upgrade begin
Switch(Config-if-Vlan1)#exit
Switch(config)#
```

Related Commands: ip dhcp-client enable, ip dhcp-client upgrade enable

1.1.4 SNMP

1.1.4.1 debug snmp mib

Command: `debug snmp mib`
`no debug snmp mib`

Function: Enables SNMP MIB debugging. The **no debug snmp mib** command disables the debugging.

Command Mode: Admin Mode.

Usage Guidelines: If problems occur when using SNMP, use SNMP debugging to locate the cause.

Example:

```
Switch#debug snmp mib
```

1.1.4.2 debug snmp kernel

Command: `debug snmp kernel`
`no debug snmp kernel`

Function: Enables SNMP kernel debugging. The **no debug snmp kernel** command disables the debugging.

Command Mode: Admin Mode.

Usage Guidelines: If problems occur when using SNMP, use SNMP debugging to locate the cause.

Example:

```
Switch#debug snmp kernel
```

1.1.4.3 rmon enable

Command: `rmon enable`
`no rmon enable`

Function: Enables RMON. The **no rmon enable** command disables RMON.

Command Mode: Global Mode.

Default: Enabled.

Example:

Enable RMON.

```
Switch(config)#rmon enable
```

Disable RMON.

```
Switch(config)#no rmon enable
```

1.1.4.4 show private-mib oid

Command: `show private-mib oid`

Function: Displays the root OID of the private MIB.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Use this command to check the root OID of the private MIB.

Example: Display the root OID of the private MIB.

```
Switch#show private-mib oid
Private MIB OID:1.3.6.1.4.1.6339
```

1.1.4.5 show snmp

Command: show snmp

Function: Displays all SNMP counters.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch#show snmp
0 SNMP packets input
        0 Bad SNMP version errors
        0 Unknownnnnn community name
        0 Illegal operation for community name supplied
        0 Encoding errors
        0 Number of requested variables
        0 Number of altered variables
        0 Get-request PDUs
        0 Get-next PDUs
        0 Set-request PDUs
0 SNMP packets output
        0 Too big errors (Max packet size 1500)
        0 No such name errors
        0 Bad values errors
        0 General errors
        0 Get-response PDUs
        0 SNMP trap PDUs
```

Field	Description
snmp packets input	Total number of SNMP packets received.
bad snmp version errors	Number of packets with an incorrect SNMP version.
unknown community name	Number of packets with an incorrect community name.
illegal operation for community name supplied	Number of packets with an operation not permitted for the community name.
encoding errors	Number of packets with encoding errors.
number of requested variable	Number of variables requested by the NMS.
number of altered variables	Number of variables set by the NMS.
get-request PDUs	Number of get-request packets received.
get-next PDUs	Number of get-next request packets received.
set-request PDUs	Number of set-request packets received.
snmp packets output	Total number of SNMP packets sent.
too big errors	Number of SNMP packets with a "tooBig" error.
maximum packet size	Maximum length of an SNMP packet.
no such name errors	Number of packets requesting nonexistent MIB objects.
bad values errors	Number of SNMP packets with a "badValue" error.
general errors	Number of SNMP packets with a "genErr" error.
response PDUs	Number of response packets sent.
trap PDUs	Number of trap packets sent.

1.1.4.6 show snmp engineid

Command: `show snmp engineid`

Function: Displays the SNMP engine ID.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch#show snmp engineid
SNMP engineID:3138633303f1276c        Engine Boots is:1
```

Field	Description
SNMP engineID	SNMP engine ID
Engine Boots	Number of times the SNMP engine has booted

1.1.4.7 show snmp group

Command: `show snmp group`

Function: Displays SNMP group information.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch#show snmp group
Group Name:initial            Security Level:noAuthnoPriv
Read View:one
Write View:<no writeview specified>
Notify View:one
```

Field	Description
Group Name	Group name
Security Level	Security level
Read View	Read view name
Write View	Write view name
Notify View	Notify view name
<no writeview specified>	No write view is specified

1.1.4.8 show snmp mib

Command: `show snmp mib`

Function: Displays all MIBs supported by the switch.

Command Mode: Admin Mode and Configuration Mode.

1.1.4.9 show snmp status

Command: `show snmp status`

Function: Displays the SNMP configuration.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch#show snmp status
Trap enable
RMON enable
Community Information:
V1/V2c Trap Host Information:
V3 Trap Host Information:
Security IP Information:
```

Field	Description
Community string	Community string

Community access	Community access permission
Trap-rec-address	IP address that receives traps
Trap enable	Whether sending traps is enabled
SecurityIP	IP address of the NMS allowed to access the SNMP agent

1.1.4.10 show snmp user

Command: `show snmp user`

Function: Displays SNMP user information.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch#show snmp user
User name: initialsha
Engine ID: 1234567890
Auth Protocol:MD5    Priv Protocol:DES-CBC
Row status:active
```

Field	Description
User name	User name
Engine ID	Engine ID
Priv Protocol	Encryption (privacy) algorithm used
Auth Protocol	Authentication algorithm used
Row status	User status

1.1.4.11 show snmp view

Command: `show snmp view`

Function: Displays SNMP view information.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch#show snmp view
View Name:readview        1.       -Included    active
                           1.3.      Excluded    active
```

Field	Description
View Name	View name
1. and 1.3.	OID
Included	The view includes the subtree rooted at this OID
Excluded	The view excludes the subtree rooted at this OID
active	Status

1.1.4.12 snmp-server community

Command: `snmp-server community {ro | rw} {0 | 7} <string> [access {<num-std>|<name>}] [ipv6-access {<ipv6-num-std>|<ipv6-name>}] [read <read-view-name>] [write <write-view-name>]`

`no snmp-server community <string> [access {<num-std>|<name>}] [ipv6-access {<ipv6-num-std>|<ipv6-name>}]`

Function: Configures an SNMP community string for the switch. The **no** form of this command deletes the community string.

Parameters: <string> is the community string. If the key option is 0, the community string is stored unencrypted; if it is 7, the community string is stored encrypted.

ro | rw specifies the MIB access mode: **ro** for read-only and **rw** for read-write.

<num-std> is the number of a numbered standard ACL, from 1 to 99.

<name> is the name of a named standard ACL, from 1 to 64 characters.

<ipv6-num-std> is the number of a numbered standard IPv6 ACL, from 500 to 599.

<ipv6-name> is the name of a named standard IPv6 ACL, from 1 to 64 characters.

<read-view-name> is the name of the read view, from 1 to 32 characters.

<write-view-name> is the name of the write view, from 1 to 32 characters.

Command Mode: Global Mode.

Usage Guidelines: The switch supports up to 4 community strings. You can control access for a community by binding the community name to a specific read view or write view.

Example:

Add a read-write community string named "private".

```
Switch(config)#snmp-server community rw 0 private
```

Add a read-only community string named "public".

```
Switch(config)#snmp-server community ro 0 public
```

Change the read-write community string "private" to read-only.

```
Switch(config)# snmp-server community ro 0 private
```

Delete the community string "private".

```
Switch(config)#no snmp-server community 0 private
```

Bind the read-only community string "public" to the read view "pviewr".

```
Switch(config)#snmp-server community ro 0 public read pviewr
```

Bind the read-write community string "private" to the read view "pviewr" and the write view "pvieww".

```
Switch(config)#snmp-server community rw 0 private read pviewr write pvieww
```

1.1.4.13 snmp-server ddm-electronic-hidden

Command: `snmp-server ddm-electronic-hidden { enable | disable }`

Function: Configures whether electrical ports are automatically skipped when DDM information is read through SNMP.

Parameters: enable automatically skips electrical ports; **disable** does not skip electrical ports.

Command Mode: Global Mode.

Default: Electrical ports are not skipped.

Usage Guidelines: When DDM information is read through SNMP, skipping electrical ports speeds up SNMP reads and avoids SNMP timeouts.

Example: Automatically skip electrical ports when DDM information is read through SNMP.

```
Switch(config)# snmp ddm-electronic-hidden enable
```

1.1.4.14 snmp-server ddm-mib

Command: `snmp-server ddm-mib { enable | disable }`

Function: Enables or disables reading DDM information through SNMP.

Parameters: enable enables this function; **disable** disables it.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: Reading DDM information consumes significant CPU resources, so this function is disabled by default.

Example: Enable reading DDM information through SNMP.

```
Switch(config)# snmp ddm-mib enable
```

1.1.4.15 snmp-server dst-port

Command: snmp-server dst-port <port-number>
no snmp-server dst-port

Function: Configures the SNMP UDP destination port number. The **no** form of this command restores the default destination port.

Parameters: <port-number>: from 1025 to 65535.

Command Mode: Global Mode.

Default: 161.

Usage Guidelines: After the SNMP destination port number is configured, SNMP packets sent by the device use the configured value as the source port number, and only SNMP requests with the configured destination port number are processed.

Example: Set the SNMP UDP destination port number to 1400.

```
Switch(config)# snmp-server dst-port 1400
```

1.1.4.16 snmp-server enable

Command: snmp-server enable
no snmp-server enable

Function: Enables the SNMP agent on the switch. The **no snmp-server enable** command disables the SNMP agent.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: To manage the switch with network management software, first enable the SNMP agent with this command.

Example: Enable the SNMP agent on the switch.

```
Switch(config)#snmp-server enable
```

1.1.4.17 snmp-server enable traps

Command: snmp-server enable traps
no snmp-server enable traps

Function: Enables the switch to send trap messages. The **no snmp-server enable traps** command disables sending trap messages.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: When trap messages are enabled, the switch sends trap messages to the NMS configured to receive them when events such as a port or system going down or up occur.

Example:

Enable sending trap messages.

```
Switch(config)#snmp-server enable traps
```

Disable sending trap messages.

```
Switch(config)#no snmp-server enable traps
```

1.1.4.18 snmp-server engineid

Command: `snmp-server engineid <engine-string>`
`no snmp-server engineid`

Function: Configures the SNMP engine ID. The **no** form of this command restores the default engine ID.

Command Mode: Global Mode.

Parameters: <engine-string> is the engine ID, from 1 to 32 hexadecimal characters.

Default: The company ID plus the local MAC address.

Usage Guidelines: None.

Example: Set the engine ID to A66688999F.

```
Switch(config)#snmp-server engineid A66688999F
```

Restore the default engine ID.

```
Switch(config)#no snmp-server engineid
```

1.1.4.19 snmp-server fdbMacInfoTable-mib

Command: `snmp-server fdbMacInfoTable-mib {enable | disable}`

Function: Enables or disables obtaining FDB (MAC address table) statistics through the MIB using SNMP.

Parameters: enable enables this function; **disable** disables it.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: To obtain FDB statistics with network management software, first enable this function with this command.

Example: Enable obtaining FDB statistics through the MIB.

```
Switch(config)# snmp-server fdbMacInfoTable-mib enable
```

1.1.4.20 snmp-server group

Command: `snmp-server group <group-string> {NoauthNopriv | AuthNopriv | AuthPriv} [[read <read-string>] [write <write-string>] [notify <notify-string>]] [access {<num-std>|<name>}] [ipv6-access {<ipv6-num-std>|<ipv6-name>}]`
`no snmp-server group <group-string> {NoauthNopriv | AuthNopriv | AuthPriv} [access {<num-std>|<name>}] [ipv6-access {<ipv6-num-std>|<ipv6-name>}]`

Function: Creates an SNMP group. The **no** form of this command deletes the group.

Command Mode: Global Mode.

Parameters: <group-string> is the group name, from 1 to 32 characters.

NoauthNopriv: Applies the no-authentication, no-encryption security level.

AuthNopriv: Applies the authentication, no-encryption security level.

AuthPriv: Applies the authentication and encryption security level.

<read-string>: The name of the read view, from 1 to 32 characters.

<write-string>: The name of the write view, from 1 to 32 characters.

<notify-string>: The name of the notify (trap) view, from 1 to 32 characters.

<num-std> is the number of a numbered standard ACL, from 1 to 99.

<name> is the name of a named standard ACL, from 1 to 64 characters.

<ipv6-num-std> is the number of a numbered standard IPv6 ACL, from 500 to 599.

<ipv6-name> is the name of a named standard IPv6 ACL, from 1 to 64 characters.

Usage Guidelines: The system has a default view named "v1defaultviewname". We recommend using this view as the notify view. If the read or write view name is empty, the corresponding operation is disabled.

Example: Create a group named "CompanyGroup" with the authentication and encryption security level, a read view named "readview", and writing disabled.

```
Switch (config)#snmp-server group CompanyGroup AuthPriv read readview
```

Delete the group.

```
Switch (config)#no snmp-server group CompanyGroup AuthPriv
```

1.1.4.21 snmp-server host

Command: snmp-server host { <host-ipv4-address> | <host-ipv6-address> } {{v1 | v2c {0 | 7 | }} | {v3 {NoauthNopriv | AuthNopriv | AuthPriv}}} <user-string>

no snmp-server host { <host-ipv4-address> | <host-ipv6-address> } {{v1 | v2c { 0 | 7}} | {v3 {NoauthNopriv | AuthNopriv | AuthPriv}}} <user-string>

Function: For SNMP v1/v2c, configures the IPv4 or IPv6 address of the NMS that receives SNMP trap messages and the trap community string. For SNMP v3, configures the IPv4 or IPv6 address of the receiving NMS, the trap username, and the security level. The **no** form of this command deletes the IPv4 or IPv6 address.

Command Mode: Global Mode.

Parameters: <host-ipv4-address> is the IPv4 address of the NMS that receives trap messages.

<host-ipv6-address> is the IPv6 address of the NMS that receives trap messages.

v1 | v2c | v3 specifies the SNMP version used to send traps.

NoauthNopriv | AuthNopriv | AuthPriv specifies the security level applied to v3 traps: no authentication and no encryption, authentication without encryption, or authentication and encryption.

<user-string> is the community string used to send trap messages in v1/v2c, or the username in v3. If the key option is 0, the community string is stored unencrypted; if it is 7, the community string is stored encrypted.

Usage Guidelines: The community string configured with this command is the default community string of the RMON event group. If no community string is configured for the RMON event group, this community string is used when RMON traps are sent; otherwise, the RMON event group's own community string is used. You can configure both IPv4 and IPv6 addresses of NMSs that receive trap messages, but the total number of v1 and v2c IPv4 and IPv6 addresses must be less than 8.

Example:

Configure an IP address to receive traps.

```
Switch(config)#snmp-server host 1.1.1.5 v1 usertrap
```

Delete an IPv6 address that receives traps.

```
Switch(config)#no snmp-server host 2001::1 v1 usertrap
```

1.1.4.22 snmp-server securityip

Command: snmp-server securityip {<ipv4-address> | <ipv6-address>}

no snmp-server securityip {<ipv4-address> | <ipv6-address>}

Function: Configures a trusted IPv4 or IPv6 address of an NMS that is allowed to access the switch. The **no** form of this command deletes the configured trusted address.

Command Mode: Global Mode.

Parameters: <ipv4-address> is the trusted IPv4 address of the NMS, in dotted decimal notation.

<ipv6-address> is the trusted IPv6 address of the NMS, in colon-hexadecimal notation.

Usage Guidelines: The switch processes SNMP packets from an NMS only if the NMS IPv4 or IPv6 address matches a trusted address configured with this command. This command applies only to SNMP. Fewer than 20 trusted IP addresses can be configured in total.

Example:

Configure a trusted IP address for an NMS.

```
Switch(config)#snmp-server securityip 1.1.1.5
```

Delete a trusted IPv6 address.

```
Switch(config)#no snmp-server securityip 2001::1
```

1.1.4.23 snmp-server securityip

Command: snmp-server securityip {enable | disable}

Function: Enables or disables trusted IP address checking for NMS access.

Command Mode: Global Mode.

Default: Enabled.

Example:

Disable trusted IP address checking.

```
Switch(config)#snmp-server securityip disable
```

1.1.4.24 snmp-server trap-resend-interval

Command: snmp-server trap-resend-interval <6-65535>
no snmp-server trap-resend-interval

Function: Sets the interval for resending trap alarms. The **no** form of this command restores the default interval.

Parameters: <6-65535>: The interval in seconds.

Command Mode: Global Mode.

Default: 300 seconds.

Usage Guidelines: Sets the trap transmission interval to adjust how frequently trap messages are sent.

Example: Set the trap resend interval to 500 seconds.

```
Switch(config)# snmp-server trap-resend-interval 500
```

1.1.4.25 snmp-server trap-source

Command: snmp-server trap-source {<ipv4-address> | <ipv6-address>}
no snmp-server trap-source {<ipv4-address> | <ipv6-address>}

Function: Sets the source IPv4 or IPv6 address used to send trap packets. The **no** form of this command deletes the configuration.

Parameters: <ipv4-address>: The IPv4 address used to send trap packets, in dotted decimal notation.

<ipv6-address>: The IPv6 address used to send trap packets, in colon-hexadecimal notation.

Command Mode: Global Mode.

Usage Guidelines: If no source address is configured, the switch uses the address of the interface that actually sends the trap packet. If a source address is configured, the switch uses it as the source address of trap packets.

Example:

Set the source IP address used to send trap packets.

```
Switch(config)#snmp-server trap-source 1.1.1.5
```

Delete the configured source IPv6 address used to send trap packets.

```
Switch(config)#no snmp-server trap-source 2001::1
```

1.1.4.26 snmp-server trap-threshold

Command: snmp-server trap-threshold {cpu-usage|memory-usage}{<0-100>}
no snmp-server trap-threshold {cpu-usage|memory-usage}

Function: Sets the threshold at which the switch sends a high CPU or memory utilization alarm. The **no** form of this command restores the default threshold.

Parameters: cpu-usage specifies switch CPU utilization; **memory-usage** specifies switch memory utilization; **<0-100>** is the alarm threshold as a percentage.

Command Mode: Global Mode.

Usage Guidelines: This feature is disabled by default.

Example: Set the threshold for sending a high CPU utilization alarm to 70%.

```
Switch(config)# snmp-server trap-threshold cpu-usage 70
```

1.1.4.27 snmp-server user

Command: snmp-server user <use-string> <group-string> [{authPriv {aes|des|3des {0|7} <word>}| authNoPriv} auth {md5 | sha} {0|7} <word>] [access {<num-std>|<name>}] [ipv6-access {<ipv6-num-std>|<ipv6-name>}]
no snmp-server user <user-string> [access {<num-std>|<name>}] [ipv6-access {<ipv6-num-std>|<ipv6-name>}]

Function: Adds a user to an SNMP group. The **no** form of this command deletes the user.

Command Mode: Global Mode.

Parameters: <user-string> is the username, from 1 to 32 characters.

<group-string> is the name of the group to which the user belongs, from 1 to 32 characters.

authPriv: Uses DES, AES, or 3DES to encrypt packets.

authNoPriv: Does not encrypt packets.

auth: Authenticates packets.

md5: Uses the HMAC-MD5 algorithm for packet authentication.

sha: Uses the HMAC-SHA algorithm for packet authentication.

<word>: The user password, from 8 to 32 characters. If the key option is 0, the password is stored unencrypted; if it is 7, the password is stored encrypted.

<num-std> is the number of a numbered standard ACL, from 1 to 99.

<name> is the name of a named standard ACL, from 1 to 64 characters.

<ipv6-num-std> is the number of a numbered standard IPv6 ACL, from 500 to 599.

<ipv6-name> is the name of a named standard IPv6 ACL, from 1 to 64 characters.

Usage Guidelines: If neither encryption nor authentication is selected, the default is no encryption and no authentication. If encryption is selected, authentication must also be configured. When you delete a user, the user is deleted even if the username is correct and the group name is incorrect.

Example:

Add a user named "tester" to "UserGroup" with the encryption security level, HMAC-MD5 authentication, and the password "hellohello".

```
Switch (config)#snmp-server user tester UserGroup authPriv auth md5
hellohello
```

Delete a user.

```
Switch (config)#no snmp-server user tester
```

1.1.4.28 snmp-server view

Command: `snmp-server view <view-string> <oid-string> {include | exclude}`
`no snmp-server view <view-string> [ <oid-string> ]`

Function: Creates or updates an SNMP view. The **no** form of this command deletes the view.

Command Mode: Global Mode.

Parameters: <view-string> is the view name, from 1 to 32 characters.

<oid-string> is the OID or the corresponding node name, from 1 to 255 characters.

include | exclude: Includes or excludes this OID.

Usage Guidelines: The OID can be entered either as a numeric OID string or as a node name.

Example:

Create a view named "readview" that includes the iso node but excludes the iso.3 node.

```
Switch(config)#snmp-server view readview iso include
Switch(config)#snmp-server view readview iso.3 exclude
```

Delete the view.

```
Switch(config)#no snmp-server view readview
```

1.1.4.29 switchport updown notification enable

Command: `[no] switchport updown notification enable`

Function: Enables or disables sending trap messages for port up/down events.

Default: Trap messages are sent for port up/down events.

Command Mode: Port Mode.

Usage Guidelines: Controls whether a trap message is sent when an up/down event occurs on the port. By default, after SNMP traps are enabled, trap messages are sent for up/down events on all ports.

Example: Disable sending trap messages for up/down events on port 1/0/1.

```
Switch(config)#in e 1/0/1
Switch(config-if-ethernet1/0/1)#no switchport updown notification enable
Switch(config-if-ethernet1/0/1)#show running-config current-mode
!
Interface Ethernet1/0/1
no switchport updown notification enable
```

1.1.5 Switch Upgrade

1.1.5.1 copy (FTP)

Command: `copy <source-url> <destination-url> [ascii | binary]`

Function: Transfers files between the switch, acting as an FTP client, and an FTP server.

Parameters: <source-url> is the location of the source file or directory to copy; **<destination-url>** is the destination of the file or directory. The format of **<source-url>** and **<destination-url>** depends on the location of the file or directory. **ascii** specifies ASCII transfer mode; **binary** specifies binary transfer mode (the default). For an FTP address, the URL format is ftp://<username>:<password>@{<ipaddress>|<ipv6address>|<hostname>}/<filename>, where <username> is the FTP username, <password> is the FTP password, <ipaddress>|<ipv6address> is the IPv4 or IPv6 address of the FTP server or client, <hostname> is a host name mapped to an IPv6 address (host names mapped to IPv4 addresses are not supported for file transfer), and <filename> is the name of the file to upload or download.

Special file name keywords:

Keyword	Source or Destination
running-config	Running configuration file
startup-config	The startup configuration file used at next boot (when the copy running-config startup-config command is used)
nos.img	System image file
boot.rom	Boot file
stacking/nos.img	As the destination, upgrades the system image file of the slave in stacking mode
stacking/nos.rom	As the destination, upgrades the boot file of the slave in stacking mode

Command Mode: Admin Mode.

Usage Guidelines: This command supports CLI prompts. If you enter **copy <filename> ftp://** or **copy ftp:// <filename>** and press Enter, the system prompts for the following:

```
ftp server ip/ipv6 address [x.x.x.x]/[x:x::x:x] >
ftp username>
ftp password>
ftp filename>
```

The system prompts for the FTP server address, username, password, and file name.

Example:

(1) Upload the image in flash to the FTP server 10.1.1.1, with username "Switch" and password "superuser".

```
Switch#copy nos.img ftp://Switch:superuser@10.1.1.1/nos.img
```

(2) Download the system file nos.img from the FTP server 10.1.1.1, with username "Switch" and password "superuser".

```
Switch#copy ftp://Switch:superuser@10.1.1.1/nos.img nos.img
```

(3) Upload the image in flash to the FTP server 2004:1:2:3::6.

```
Switch#copy nos.img ftp://username:password@2004:1:2:3::6/ nos.img
```

(4) Download the system file nos.img from the FTP server 2004:1:2:3::6.

```
Switch#copy ftp:// username:password@2004:1:2:3::6/nos.img nos.img
```

(5) Save the running configuration.

```
Switch#copy running-config startup-config
```

Related Commands: write

1.1.5.2 copy (TFTP)

Command: copy <source-url> <destination-url> [ascii | binary]

Function: Transfers files between the switch, acting as a TFTP client, and a TFTP server.

Parameters: <source-url> is the location of the source file or directory to copy; **<destination-url>** is the destination of the file or directory. The format of **<source-url>** and **<destination-url>** depends on the location of the file or directory. **ascii** specifies ASCII transfer mode; **binary** specifies binary transfer mode (the default). For a TFTP address, the URL format is tftp://{<ipaddress>|<ipv6address>|<hostname>}/<filename>, where <ipaddress>|<ipv6address> is the IPv4 or IPv6 address of the TFTP server or client, <hostname> is a host name mapped to an IPv6 address (host names mapped to IPv4 addresses are not supported for file transfer), and <filename> is the name of the file to upload or download.

Special file name keywords:

Keyword	Source or Destination
running-config	Running configuration file
startup-config	The startup configuration file used at next boot (when the copy running-config startup-config command is used)
nos.img	System image file
boot.rom	Boot file

Command Mode: Admin Mode.

Usage Guidelines: This command supports CLI prompts. If you enter **copy <filename> tftp://** or **copy tftp:// <filename>** and press Enter, the system prompts for the following:

```
tftp server ip/ipv6 address[x.x.x.x]/[x:x::x:x]>
tftp filename>
```

The system prompts for the TFTP server address and file name.

Example:

(1) Upload the image in flash to the TFTP server 10.1.1.1.

```
Switch#copy nos.img tftp://10.1.1.1/nos.img
```

(2) Download the system file nos.img from the TFTP server 10.1.1.1.

```
Switch#copy tftp://10.1.1.1/nos.img nos.img
```

(3) Upload the image in flash to the TFTP server 2004:1:2:3::6.

```
Switch#copy nos.img tftp:// 2004:1:2:3::6/ nos.img
```

(4) Download the system file nos.img from the TFTP server 2004:1:2:3::6.

```
Switch#copy tftp:// 2004:1:2:3::6/nos.img nos.img
```

(5) Save the running configuration.

```
Switch#copy running-config startup-config
```

Related Commands: write

1.1.5.3 copy (SFTP)

Command: copy <source-url> <destination-url> [ascii | binary]

Function: Transfers files between the switch, acting as an SFTP client, and an SFTP server.

Parameters: <source-url> is the location of the source file or directory to copy; **<destination-url>** is the destination of the file or directory. The format of **<source-url>** and **<destination-url>** depends on the location of the file or directory. **ascii** specifies ASCII transfer mode; **binary** specifies binary transfer mode (the default). For an SFTP address, the URL format is sftp://<username>:<password>@{<ipaddress>|<hostname>}/<filename>, where <username> is the SFTP username, <password> is the SFTP password, <ipaddress> is the IPv4 address of the SFTP server, <hostname> is a host name mapped to an IP address, and <filename> is the name of the file to upload or download.

Special file name keywords:

Keyword	Source or Destination

running-config	Running configuration file
startup-config	The startup configuration file used at next boot (when the copy running-config startup-config command is used)
nos.img	System image file
boot.rom	Boot file
stacking/nos.img	As the destination, upgrades the system image file of the slave in stacking mode
stacking/nos.rom	As the destination, upgrades the boot file of the slave in stacking mode

Command Mode: Admin Mode.

Usage Guidelines: This command supports CLI prompts. If you enter **copy <filename> sftp://** or **copy sftp:// <filename>** and press Enter, the system prompts for the following:

```
sftp server ip/ipv6 address [x.x.x.x]/[x:x::x:x] >
sftp username>
sftp password>
sftp filename>
```

The system prompts for the SFTP server address, username, password, and file name.

Example:

(1) Upload the image in flash to the SFTP server 10.1.1.1, with username "Switch" and password "superuser".

```
Switch#copy nos.img sftp://Switch:superuser@10.1.1.1/nos.img
```

(2) Download the system file nos.img from the SFTP server 10.1.1.1, with username "Switch" and password "superuser".

```
Switch#copy sftp://Switch:superuser@10.1.1.1/nos.img nos.img
```

(3) Save the running configuration.

```
Switch#copy running-config startup-config
```

Related Commands: write

1.1.5.4 ftp-dir

Command: `ftp-dir <ftp-server-url>`

Function: Lists the files on an FTP server.

Parameters: The format of **<ftp-server-url>** is ftp://<username>:<password>@{<ipv4address>|<ipv6address>}, where <username> is the FTP username, <password> is the FTP password, and {<ipv4address>|<ipv6address>} is the IPv4 or IPv6 address of the FTP server.

Command Mode: Admin Mode.

Example: List the files on the FTP server, with username "Switch" and password "superuser".

```
Switch#ftp-dir ftp://Switch:superuser @10.1.1.1.
```

1.1.5.5 ftp-server enable

Command: `ftp-server enable`
`no ftp-server enable`

Function: Starts the FTP server. The **no ftp-server enable** command shuts down the FTP server and prevents FTP users from logging in.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: When the FTP server is enabled, the switch can still act as an FTP client. The FTP server is disabled by default.

Example: Enable the FTP server.

```
Switch#config
Switch(config)# ftp-server enable
```

Related Commands: ip ftp

1.1.5.6 ftp-server timeout

Command: `ftp-server timeout <seconds>`

Function: Sets the idle timeout for FTP data connections.

Parameters: <seconds> is the idle timeout for FTP connections, in seconds, from 5 to 3600.

Default: 600 seconds.

Command Mode: Global Mode.

Usage Guidelines: When an FTP data connection is idle longer than this limit, the FTP control connection is disconnected.

Example: Change the idle timeout to 100 seconds.

```
Switch#config
Switch(config)#ftp-server timeout 100
```

1.1.5.7 ip ftp

Command: `ip ftp username <username> password [0 | 7] <password>`
`no ip ftp username <username>`

Function: Configures the username and password used to log in to an FTP server. The **no** form of this command deletes both the configured username and password.

Parameters: <username> is the FTP username, up to 32 characters. **<password>** is the FTP password. If option 0 is specified, the password is stored unencrypted; if option 7 is specified, the password is stored encrypted.

Default: Anonymous FTP login is used.

Command Mode: Global Mode.

Example: Configure the username "Switch" and the password "superuser".

```
Switch#
Switch#config
Switch(config)#ip ftp username Switch password 0 superuser
Switch(config)#
```

1.1.5.8 show ftp

Command: `show ftp`

Function: Displays the FTP server settings.

Command Mode: Admin Mode and Configuration Mode.

Default: None.

Example:

```
Switch#show ftp
Timeout : 600
```

Field	Description
Timeout	Timeout value

1.1.5.9 show tftp

Command: `show tftp`

Function: Displays the TFTP server settings.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch#show tftp
timeout     : 60
Retry Times  : 10
```

Field	Description
Timeout	Timeout value
Retry Times	Number of retransmissions

1.1.5.10 tftp-server enable

Command: `tftp-server enable`
`no tftp-server enable`

Function: Starts the TFTP server. The **no tftp-server enable** command shuts down the TFTP server and prevents TFTP users from logging in.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: When the TFTP server is enabled, the switch can still act as a TFTP client. The TFTP server is disabled by default.

Example: Enable the TFTP server.

```
Switch#config
Switch(config)#tftp-server enable
```

Related Commands: tftp-server timeout

1.1.5.11 tftp-server retransmission-number

Command: `tftp-server retransmission-number <number>`

Function: Sets the number of retransmissions for the TFTP server.

Parameters: <number> is the number of retransmissions, from 1 to 20.

Default: 5.

Command Mode: Global Mode.

Example: Set the number of retransmissions to 10.

```
Switch#config
Switch(config)#tftp-server retransmission-number 10
```

1.1.5.12 tftp-server transmission-timeout

Command: `tftp-server transmission-timeout <seconds>`

Function: Sets the transmission timeout for the TFTP server.

Parameters: <seconds> is the timeout value, from 5 to 3600 seconds.

Default: 600 seconds.

Command Mode: Global Mode.

Example: Set the timeout value to 60 seconds.

```
Switch#config
Switch(config)#tftp-server transmission-timeout 60
```

1.1.6 Boot Configuration

1.1.6.1 baudrate

Command: `baudrate <value>`

Function: Configures the baud rate of the switch.

Parameters: <value> is the baud rate. Supported values are 9600, 14400, 19200, 38400, 57600, and 115200.

Default: 115200.

Command Mode: Boot Mode.

Usage Guidelines: Configures the baud rate used to transfer files in XMODEM mode. The baud rate of the switch must match that of the serial port software on the PC.

Example: Set the baud rate of the switch to 115200 for XMODEM file transfer.

```
[Boot]: baudrate 115200
```

1.1.6.2 boot img

Command: `boot img <img-file-url> {primary | backup}`

Function: Configures the primary and backup IMG files used to boot the switch.

Parameters: primary specifies the primary IMG file; **backup** specifies the backup IMG file. **<img-file-url>** is the full path of the boot IMG file.

Command Mode: Boot Mode.

Default: Only the primary boot IMG file is specified (nos.img in flash). No backup boot IMG file is specified.

Usage Guidelines: Use this command to configure the primary and backup IMG files of the switch. If booting from the primary IMG file fails, the system automatically boots from the backup IMG file. The full IMG file path uses the following format:

1. The file path consists of two parts: a device prefix used as the root directory (flash:/) and the file name. Spaces are not allowed within either part or between the two parts.

2. All file names must have the .img extension.

3. The full file path cannot exceed 128 characters, and the file name cannot exceed 80 characters.

Example: Set flash:/nos.img as the primary IMG file of the switch.

```
[Boot]: boot img flash:/nos.img primary
```

1.1.6.3 boot startup-config

Command: `boot startup-config <file-url>`

Function: Configures the CFG file used the next time the switch boots.

Parameters: <file-url> is the full path of the CFG file used at the next boot.

Command Mode: Boot Mode.

Default: NULL.

Usage Guidelines: Use this command to configure the CFG file used at the next boot. The file name must have the .cfg extension. The full path uses the following format:

1. The file path consists of two parts: a device prefix used as the root directory (flash:/) and the file name. Spaces are not allowed within either part or between the two parts.

2. All file names must have the .cfg extension.

3. The full file path cannot exceed 128 characters, and the file name cannot exceed 80 characters.

Example: Set flash:/ startup.cfg as the CFG file used at the next boot.

```
[Boot]: boot startup-config flash:/ startup-config
```

1.1.6.4 clearconfig

Command: `clearconfig`

Function: Restores the bootrom parameters to their defaults.

Parameters: None.

Command Mode: Boot Mode.

Default: None.

Usage Guidelines: Use this command to restore the bootrom parameters to their defaults.

Example: Restore the bootrom parameters to their defaults.

```
[Boot]: clearconfig
Network interface configure OK.
Boot config set Ok.
```

1.1.6.5 Copy

Command: `copy <srcFileName> <desFileName>`

Function: Copies a file in flash.

Parameters: <source-file-url> is the URL of the source file, which can be relative or absolute. **<dest-file-url>** is the URL of the destination file, which must be relative. The destination file must have the same extension as the source file.

Command Mode: Boot Mode.

Default: None.

Usage Guidelines: Use this command to back up IMG or CFG files.

Example: Copy the IMG file "flash:/nos.img".

```
[Boot]: copy nos.img flash:/backup.img
```

Or:

```
[Boot]: copy flash:/nos.img flash:/backup.img .
```

1.1.6.6 dir

Command: `dir`

Function: Displays the list and attributes of files on the switch.

Default: None.

Command Mode: Boot Mode.

Usage Guidelines: Displays the names and sizes of files.

Example: Display the list and attributes of files on the switch. Note: ROM files are not displayed.

```
[[Boot]: dir
  1461094   nos.img.ecc
    91393   mantest.img.ecc
 41559526   nos.img
  2599038   mantest.img
     1547   startup.cfg
5 file(s), 0 dir(s)
Total size:64483328 bytes , used size:45851648 bytes, free size:18631680
bytes
```

1.1.6.7 help

Command: `h`
`help`

Function: Displays the commands supported by the current bootrom and a description of each.

Default: None.

Parameters: None.

Command Mode: Boot Mode.

Usage Guidelines: Displays descriptions of commonly used commands.

Example: Display descriptions of commonly used commands.

```
[Boot]: help
baudrate            - set the baudrate
boot                - select the active bootimg image file or startup-config
file
clearconfig         - set default bootrom configurations
copy <src> <dst>    - copy a file
delete <filename>   - delete a file
dir                 - display the contents of the current directory
h                   - print help list
help                - print help list
load <filename>     - load system image(binary format)
nobootpassword      - no bootpassword for setup
ping <x.x.x.x>      - ping test
reboot              - reboot system
saveconfig          - save bootrom configurations
setbootpassword     - set boot password
setconfig           - set bootrom configurations
show                - show machine info
showconfig          - show bootrom configurations
write <filename>    - write file to flash; file gotten by 'load'
xmodem              - load file by xmodem
```

1.1.6.8 load

Command: `load<filename>`

Function: Downloads a file through TFTP.

Parameters: <filename> is the name of the file to download.

Command Mode: Boot Mode.

Usage Guidelines: Enter **load** followed by the file name to download the file through TFTP.

Example: Download the boot.rom file.

```
[Boot]:load boot.rom
```

1.1.6.9 nobootpassword

Command: `nobootpassword`

Function: Clears the password used to enter the boot menu.

Parameters: None.

Default: None.

Command Mode: Boot Mode.

Usage Guidelines: Use this command to clear the password used to enter the boot menu.

Example: Clear the password used to enter the boot menu.

```
[Boot]: nobootpassword
clear password ok
```

1.1.6.10 ping

Command: `ping <x.x.x.x>`

Function: Tests network connectivity.

Parameters: <x.x.x.x> is the IP address to ping, typically the IP address of a PC.

Command Mode: Boot Mode.

Default: None.

Usage Guidelines: Use this command to test network connectivity. It works like the ping command on a PC but has no optional parameters, and it can only ping a PC from the switch.

Example: Test connectivity to 192.168.0.1.

```
[Boot]:ping 192.168.0.1
```

1.1.6.11 reboot

Command: `reboot`

Function: Restarts the switch.

Parameters: None.

Default: None.

Command Mode: Boot Mode.

Usage Guidelines: Performs a warm restart of the switch.

Example: Restart the switch.

```
[Boot]:reboot
```

1.1.6.12 saveconfig

Command: `saveconfig`

Function: Saves the bootrom configuration.

Parameters: None.

Default: None.

Command Mode: Boot Mode.

Usage Guidelines: Use this command to save the bootrom configuration.

Example: Save the bootrom configuration.

```
[Boot]: saveconfig
change boot params is OK
```

1.1.6.13 setbootpassword

Command: `setbootpassword`

Function: Sets the password used to enter the boot menu.

Parameters: None.

Default: No boot password is configured.

Command Mode: Boot Mode.

Usage Guidelines: Sets the password used to enter the boot menu. The password must be 3 to 32 characters long.

Example: Set the password used to enter the boot menu.

```
[Boot]: setbootpassword
Password:******
Confirm Password:******
Password has been set successfully!
```

1.1.6.14 setconfig

Command: `setconfig`

Function: Sets the bootrom configuration parameters.

Parameters: None.

Default: Host IP 10.1.1.1 and server IP 10.1.1.2.

Command Mode: Boot Mode.

Usage Guidelines: Use this command to set the bootrom configuration parameters. The host IP and server IP parameters currently support only TFTP.

Example: Set the bootrom configuration parameters.

```
[Boot]: setconfig
Host IP Address: [10.1.1.1] 192.168.1.1
Server IP Address: [10.1.1.2] 192.168.1.2
```

1.1.6.15 show

Command: `show [board|config|boot-files|partition]`

Function: Displays switch information and bootrom configuration.

Parameters: board displays switch information such as the model, MAC address, and serial number. **config** displays the current bootrom configuration. **boot-files** displays the primary and backup IMG files and the CFG file. **partition** displays the flash partitions.

Default: None.

Command Mode: Boot Mode.

Usage Guidelines: show board displays switch information such as the model, MAC address, and serial number. **show config** displays the bootrom configuration. **show boot-files** displays the primary and backup IMG files and the CFG file. **show partition** displays the flash partitions.

Example: Display the configured IMG files.

```
[Boot]: show boot-files
The primary img file : flash:/1.img
The backup img file : flash:/nos.img
```

1.1.6.16 showconfig

Command: `showconfig`

Function: Displays the bootrom configuration. This command is equivalent to the **show config** command.

Parameters: None.

Default: None.

Command Mode: Boot Mode.

Usage Guidelines: Displays the user configuration of the bootrom.

Example: Display the bootrom configuration.

```
[Boot]: showconfig
Host IP Address:    192.168.1.1
Server IP Address:  192.168.1.2
```

1.1.6.17 write

Command: `write <filename>`

Function: Writes a previously downloaded file to memory such as flash.

Parameters: <filename> is the name under which the file is written to memory.

Default: None.

Command Mode: Boot Mode.

Usage Guidelines: Writes a previously downloaded file to flash or the bootrom.

Example: Write the boot file to flash with the name boot.rom.

```
[Boot]:write boot.rom
```

1.1.6.18 xmodem

Command: `xmodem`

Function: Transfers files through the XMODEM protocol in the bootrom.

Parameters: None.

Default: None.

Command Mode: Boot Mode.

Usage Guidelines: To improve the transfer rate, we recommend a higher baud rate (see the **baudrate** command). After this command is executed, the switch waits to receive a file through XMODEM. Then start the XMODEM transfer on the PC with software that supports XMODEM.

Example: Put the switch into XMODEM mode.

```
[Boot]: xmodem
## Ready for binary (xmodem) download to 0x04400000 at 9600 bps...
```

1.2 File System

1.2.1 cd

Command: `cd <directory>`

Function: Changes the working directory on the storage device.

Parameters: <directory> is the subdirectory name, from 1 to 80 characters.

Command Mode: Admin Mode.

Default: The default working directory is flash.

Usage Guidelines: After this command is executed, the current working directory changes to the specified directory, which you can display with the **pwd** command.

Example: Change the working directory to flash.

```
Switch#cd flash:
Switch#pwd
flash:/
Switch#
```

1.2.2 copy

Command: `copy <source-file-url > <dest-file-url>`

Function: Copies a specified file on the switch and saves it as a new file.

Parameters: <source-file-url> is the source file; **<dest-file-url>** is the destination file. The source and destination file URLs must use the following formats:

1. The source file URL must begin with one of the following prefixes:

- flash:/
- ftp://username:pass@server-ip/file-name
- tftp://server-ip/file-name

2. The destination file URL must begin with one of the following prefixes:

- flash:/
- ftp://username:pass@server-ip/file-name
- tftp://server-ip/file-name

Command Mode: Admin Mode.

Default: None.

Usage Guidelines:

1. If the source file URL begins with ftp:// or tftp://, the destination file URL cannot begin with either of these prefixes.

2. The source file must exist, and the destination file cannot have the same name as an existing directory or file; otherwise, the switch may report that the copy failed or prompt you to overwrite the existing file.

3. If the source and destination files are in different directories, you can use this command to copy files from another directory into the current directory.

URL example: The URL of a file in the root directory of flash is flash:/nos.img.

Example: Copy the file "flash:/nos.img" and save it as "flash:/nos-6.1.11.0.img".

```
Switch#copy flash:/nos.img flash:/nos-6.1.11.0.img
Copy flash:/nos.img to flash:/nos-6.1.11.0.img? [Y:N] y
Copyed file flash:/nos.img to flash:/nos-6.1.11.0.img.
```

1.2.3 delete

Command: `delete <file-url>`

Function: Deletes the specified file from the storage device.

Parameters: <file-url> is the full path of the file to delete.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: The specified file is deleted after this command is executed.

Example: Delete the file flash:/nos5.img.

```
Switch#delete flash:/nos5.img
Delete file flash:/nos5.img?[Y:N]y
Deleted file flash:/nos.img.
```

1.2.4 dir

Command: `dir [WORD|all]`

Function: Displays information about the specified directory on the storage device.

Parameters: <WORD> is the name of the directory to display, in the format **directory-name** or **flash:/directory-name**. **all** displays the contents of the flash:/ and mmc:/ directories.

Command Mode: Admin Mode and Configuration Mode.

Default: If <WORD> is not specified, the current working directory is displayed.

Usage Guidelines: Displays information about the files and subdirectories in the specified directory.

Note: This command does not display subdirectories recursively.

Example: Display the contents of the directory "flash:/".

```
Switch#dir flash:/
nos.img      2,449,496      1980-01-01 00:01:06   ----
startup-config   2,064      1980-01-01 00:30:12   ----
Total  7, 932, 928 byte(s)  in  4  file(s),  free  4, 966, 400 byte(s)
```

```
Switch#
```

1.2.5 pwd

Command: pwd

Function: Displays the current working directory.

Parameters: None.

Command Mode: Admin Mode.

Default: flash.

Example: Display the current working directory.

```
Switch#pwd
flash:/
Switch#
```

1.2.6 rename

Command: rename <source-file-url> <new-filename >

Function: Renames a specified file on the switch.

Parameters: <source-file-url> is the source file, with or without its path. **<new-filename>** is the new file name, without a path.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: The file is renamed only if the new name is not already used by an existing directory or file; otherwise, the switch reports that the operation failed.

Example: Rename the file "nos5.img" in the current working directory to "nos-6.1.11.0.img".

```
Switch# rename nos5.img nos-6.1.11.0.img
Rename flash:/nos5.img to flash:/nos-6.1.11.0.img ok！
```

1.3 USB

1.3.1 cd usb:

Command: cd usb:

Function: Changes the current directory to the USB drive.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: If a USB flash drive is inserted, the switch changes to the USB drive and displays "Change the current directory to "usb:/"!". If no USB flash drive is inserted, the switch displays "Device "usb:" has not inserted!".

Example:

```
Switch#cd usb：
Change the current directory to “usb:/”！
```

1.3.2 dir

Command: dir

Function: Displays the contents of the USB flash drive.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Lists the files on the USB flash drive. If no USB flash drive is inserted, an error message is displayed.

Example:

```
Switch#dir
drwx    4.0K    7.0tset
-rwx    1.2K    bootex.log
drwx    4.0K    crt
dr-x     4.0K    recycler
drwx    8.0K    reliability
drwx    4.0K    test
-rwx    141.3K  186.pdf
drwx    4.0K     new
Drive : usb:
Size:7.4G Used:227.6M Available:7.2G Use:3%
```

1.3.3 delete

Command: `delete <filename>`

Function: Deletes a file.

Command Mode: Admin Mode.

Default: None.

Example: Delete the file log.txt on the USB drive.

```
Switch#delete log.txt
Delete file, Are you sure? (Y/N)?[N]y
Delete file ok.
```

1.3.4 rename

Command: `rename <source> <destination>`

Function: Renames a file.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: source is the source file name; **destination** is the destination file name. If no USB flash drive is inserted, the switch first checks whether the destination file name is valid and then checks the source file name. If the destination file name is empty, an error message is displayed.

Example: Rename log1.txt to log2.txt.

```
Switch#rename log1.txt log2.txt
Rename log1.txt to log2.txt ok!
```

1.3.5 copy

Command: `copy <source> <destination>`

Function: Copies a source file to a destination file.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: 1) Copy files on the USB flash drive: **copy source.txt destination.txt** copies source.txt on the USB drive to destination.txt.

2) **copy usb:/startup.cfg startup.cfg** updates the switch with startup.cfg from the USB drive.

The reverse direction is also supported: **copy startup.cfg usb:/startup.cfg**

3) **copy usb:/boot.rom boot.rom** updates boot.rom from the USB drive.

The reverse direction is also supported: **copy boot.rom usb:/boot.rom**

4) **copy usb:/nos.img nos.img** updates nos.img from the USB drive.

The reverse direction is also supported: **copy nos.img usb:/nos.img**

5) The commands above support both absolute and relative paths.

Example: If a USB flash drive is inserted, the copy is performed; if no USB flash drive is inserted, error messages such as the following are displayed:

```
Switch#copy usb:/tt.txt usb:/tttt.txt
Device "usb:" has not inserted!
Read local file usb:/tt.txt error.
Switch #copy startup.cfg usb:/startup.cfg
Can't write in non-existent directory "usb:/"!
Write config usb:/startup.cfg error!
Write error.
Switch #
Switch #copy usb:/startup.cfg startup.cfg
Confirm to overwrite the existed destination file?  [Y/N]:y
Get file "startup.cfg" length error!
Read local file usb:/startup.cfg error.
```

1.4 Device Management

1.4.1 debug devsm

Function: Displays debugging information about device management messages sent and received and about card status transitions. The **no** form of this command disables the debugging output.

Parameters: send displays outgoing device management messages.

receive displays received device management messages.

state displays card status transition information.

Default: Disabled.

Command Mode: Admin Mode.

1.4.2 force runcfg-sync

Command: `force runcfg-sync`

Function: Forces immediate synchronization of the running configuration to the standby master (SM) in a VSF system.

Command Mode: Admin Mode.

Usage Guidelines: In stacking mode, the running configuration of the active master (AM) is synchronized to the SM every 5 minutes by default. This command starts synchronization immediately.

1.4.3 force sync software-version

Command: `force {sm|} sync software-version {enable|disable}`

Function: Forces synchronization of the system software (NOS) version to the SM or slave in a VSF system.

Command Mode: Admin Mode.

Usage Guidelines: In a VSF system, the AM checks whether a newly added member runs the same software version as the AM. If the versions differ, the AM synchronizes its own image to the new member.

1.4.4 force switchover

Command: `force switchover`

Function: Forces a switchover from the SM to the AM role.

Command Mode: Admin Mode.

Usage Guidelines: When a standby master exists, executing this command on the active master triggers a master/standby switchover, and the original standby master becomes the new active master.

1.4.5 reset slot

Command: `reset member <memID> slot <slotno>`

Function: Resets the specified card.

Parameters: <memID>: The VSF member ID in stacking mode, from 1 to 16.

Command Mode: Admin Mode.

Usage Guidelines: Only an SM or slave card can be reset; the AM card cannot be reset.

1.4.6 show fan

Command: `show fan`

Function: Displays whether the fan tray is installed, its operating status, and the fan speed.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays the fan operating status. "Fan board Inserted" indicates whether the fan tray is installed; "Status" indicates whether the fan is operating normally; "Speed" indicates the fan speed.

1.4.7 show power

Command: `show power`

Function: Displays whether each power supply is installed and its operating status.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: "Inserted" indicates whether the power supply is installed; "Status" indicates whether it is operating normally.

Example:

```
Switch#show power
System power information:
Power No         Inserted         Status
1                YES              Normal
2                YES              Abnormal
```

1.4.8 show slot

Command: `show [member <member-id>] slot <slot-id>`

Function: Displays basic information about each card.

Parameters: <member-id> is the member device number in VSF mode, from 1 to 16. **<slot-id>** is the number of the slot where the card resides; on box (non-chassis) devices, the slot number is always 1.

Default: If neither member-id nor slot-id is specified, information about all cards is displayed.

Command Mode: Admin Mode.

Usage Guidelines: Displays basic information about all cards. "MCU state" is the state of the microcontroller unit (master or standby); "MCU version" is the version of the microcontroller unit file; "Uptime" is the time since the system booted.

Example:

```
Switch#show member 13 slot 1
--------------------member :13--------------------
Inserted : YES
Module type : Switch
Work mode : STANDBY MASTER
Work state : RUNNING
Software package version : 7.0.3.0(R0075.0011)
Bootrom version : 7.2.2
CPLD version : N/A
Hardware version : 1.0.1
Part number : N110900062
Manufacture date : 2011/03/10
Temperature : 39C/102F
Uptime : 0 weeks, 0 days, 1 hours, 37 minutes
```

Chapter 2 Network Security

2.1 Network Security

2.1.1 default user password macbased

Command: **`service default user password macbased`**
`no service default user password macbased`

Function: Generates the factory default password from the device VLAN MAC address using a specific combination. The **no** form of this command restores the factory default password.

Parameters: None.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: This command is controlled by the vendor. When required, the vendor adds it to the default configuration in a new image file, and it takes effect after the image is upgraded.

Example: None.

2.1.2 first-login change password

Command: **`first-login change password`**
`no first-login change password`

Function: Forces users to change the default password at first login. By default, users are not forced to change the default password.

Parameters: None.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: This command is controlled by the vendor. When required, the vendor adds it to the default configuration in a new image file, and it takes effect after the image is upgraded.

Example: None.

2.1.3 userpassword restriction

Command: **`userpassword restriction {min-length <1-32> | format-mix (<2-4>|)`**
`| max-consecutive-char <2-32> | max-consecutive-identical-char <2-32>}`
`no userpassword restriction {min-length <1-32> | format-mix (<2-4>|)`
`| max-consecutive-char <2-32> | max-consecutive-identical-char <2-32> | }`

Function: Configures password strength checking. The **no** form of this command removes the password strength check.

Parameters: **min-length <1-32>**: The minimum password length, from 1 to 32.

format-mix (<2-4>|): Requires a mix of character types; the number of types is from 2 to 4. If no value is specified, 2 types are required.

max-consecutive-char <2-32>: The maximum number of sequential characters allowed in a password, from 2 to 32.

max-consecutive-identical-char <2-32>: The maximum number of consecutive identical characters allowed in a password, from 2 to 32.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: Configure this command to check user password strength.

Example: Require passwords to be at least 8 characters long, contain at least three character types, and contain no more than 3 consecutive identical characters and no more than 3 sequential characters.

```
Switch#config terminal
Switch(config)#userpassword restriction min-length 8 format-mix 3 max-
consecutive-identical-char 3 max-consecutive-char 3
```

2.1.4 password valid-time

Command: service user password valid-time <0-90>
no service user password valid-time

Function: Configures the user password validity period. The **no** form of this command removes the validity period setting.

Parameters: <0-90>: The validity period in days, from 0 to 90. A value of 0 means the password never expires.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: Configure this command to enforce password expiration.

Example: Set the password validity period to 30 days.

```
Switch#config terminal
Switch(config)#service user password valid-time 30
```

2.1.5 user-login failed msg

Command: user-login failed msg neutral
no user-login failed msg neutral

Function: Displays only a neutral message when user login fails, without the specific reason for the authentication failure (such as an incorrect password or a nonexistent user). The **no** form of this command restores the default message.

Parameters: None.

Default: A neutral login failure message is displayed.

Command Mode: Global Mode.

Usage Guidelines: Configure this command to display a neutral message after a login failure.

Example: Display a neutral message after a user login failure.

```
Switch#config terminal
Switch(config)#user-login failed msg neutral
```

2.1.6 password feedback

Command: password feedback (none|star)
no password feedback

Function: Configures whether the password is hidden or shown as asterisks (*) when the user logs in. The **no** form of this command deletes the rule.

Parameters: none: The password is not echoed.

star: Each password character is displayed as an asterisk (*).

Default: Asterisks (*) are displayed.

Command Mode: Global Mode.

Usage Guidelines: Configure this command to set how passwords are echoed.

Example: Configure the password not to be echoed.

```
Switch#config terminal
Switch(config)#password feedback none
```

2.1.7 password security-config

Command: `userpassword security-config`
`no userpassword security-config`

Function: Enforces secure (hidden) entry of user passwords. The **no** form of this command cancels this requirement.

Parameters: None.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: Configure this command to require secure entry of user passwords.

Example: Enforce secure entry of user passwords.

```
Switch#config terminal
Switch(config)#userpassword security-config
```

After this command is configured, enter passwords as follows:

```
Switch(config)#username user privilege 15 password
Password:*******
```

2.1.8 boot-file security check

Command: `boot (img | startup-config) check enable`
`no boot (img | startup-config) check enable`

Function: Enables security verification of IMG and CFG files. The **no** form of this command disables the verification.

Parameters: img: The IMG file.

startup-config: The CFG file.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: Configure this command to perform security checks on IMG and CFG files. The setting is stored as an environment variable and can be viewed with the **show boot-files** command.

Example: Enable security verification of the IMG file.

```
Switch#config terminal
Switch(config)#boot img check enable
```

2.1.9 ssh-server dst-port

Command: `ssh-server dst-port <port-number>`
`no ssh-server dst-port`

Function: Configures the port number of the SSH server. The **no** form of this command restores the default.

Parameters: <port-number> is the SSH server port number, from 1025 to 65535.

Command Mode: Global Mode.

Default: 22.

Usage Guidelines: The port number can be changed only when SSH is disabled; if SSH is enabled, disable it first. If the SSH server port number is 22, SSH clients do not need to specify the port number; for any other port number, SSH clients must specify the port number when logging in.

Example: Set the SSH server port number to 1200.

```
Switch(config)# ssh-server dst-port 1200
```

2.1.10 telnet-server dst-port

Command: telnet-server dst-port <port-number>
no telnet-server dst-port

Function: Configures the port number of the Telnet server. The **no** form of this command restores the default.

Parameters: <port-number> is the Telnet server port number, from 1025 to 65535.

Command Mode: Global Mode.

Default: 23.

Usage Guidelines: The port number can be changed only when Telnet is disabled; if Telnet is enabled, disable it first. If the Telnet server port number is 23, Telnet clients do not need to specify the port number; for any other port number, Telnet clients must specify the port number.

Example: Set the Telnet server port number to 1300.

```
Switch(config)# telnet-server dst-port 1300
```

2.1.11 snmp-server dst-port

Command: snmp-server dst-port <port-number>
no snmp-server dst-port

Function: Configures the port number used by the SNMP service. The **no** form of this command restores the default.

Parameters: <port-number> is the SNMP service port number, from 1025 to 65535.

Command Mode: Global Mode.

Default: 161.

Usage Guidelines: The port number can be changed only when SNMP is disabled; if SNMP is enabled, disable it first. After the port number is configured, the port number specified on the network management station must match the port configured with the **snmp-server dst-port** command; otherwise, the device cannot be reached.

Example: Set the SNMP service port number to 1400.

```
Switch(config)# snmp-server dst-port 1400
```

2.1.12 ip http secure-ciphersuite

Command: ip http secure-ciphersuite {**aes128-gcm-sha256 | aes128-sha | aes128-sha256 | aes256-sha | aes256-sha256 | ecdhe-rsa-aes128-gcm-sha256 | ecdhe-rsa-aes128-sha | ecdhe-rsa-aes256-sha**}
no ip http secure-ciphersuite

Function: Configures the cipher suites used by SSL. The **no** form of this command restores the default.

Parameters: aes128-gcm-sha256: The AES128-GCM-SHA256 cipher suite.

aes128-sha: The AES128-SHA cipher suite.

aes128-sha256: The AES128-SHA256 cipher suite.

aes256-sha: The AES256-SHA cipher suite.

aes256-sha256: The AES256-SHA256 cipher suite.

ecdhe-rsa-aes128-gcm-sha256: The ECDHE-RSA-AES128-GCM-SHA256 cipher suite.

ecdhe-rsa-aes128-sha: The ECDHE-RSA-AES128-SHA cipher suite.

ecdhe-rsa-aes256-sha: The ECDHE-RSA-AES256-SHA cipher suite.

Command Mode: Global Mode.

Default: Not configured.

Usage Guidelines: If cipher suites are configured with this command, SSL negotiation uses the configured cipher suites. After you change the cipher suites, restart the SSL function for the change to take effect.

Example: Configure SSL to use the aes128-gcm-sha256 cipher suite.

```
Switch(config)# ip http secure- ciphersuite aes128-gcm-sha256
```

2.1.13 ssh-server encryption-algorithm

Command: ssh-server encryption-algorithm (add | remove) {**aes128-cbc | 3des-cbc | aes128-ctr | aes256-ctr | aes256-cbc | 3des-ctr | all**}
no ssh-server encryption-algorithm

Function: Adds or removes encryption algorithms on the SSH server. The **no** form of this command restores the default.

Parameters: add | remove: Adds or removes the algorithm.

aes128-cbc: The AES128-CBC encryption algorithm.

3des-cbc: The 3DES-CBC encryption algorithm.

aes128-ctr: The AES128-CTR encryption algorithm.

aes256-ctr: The AES256-CTR encryption algorithm.

aes256-cbc: The AES256-CBC encryption algorithm.

3des-ctr: The 3DES-CTR encryption algorithm.

all: All encryption algorithms.

Command Mode: Global Mode.

Default: Three algorithms are enabled: aes128-ctr, aes256-ctr, and 3des-ctr.

Usage Guidelines: The SSH server must support at least one of the algorithms used by the SSH client; otherwise, negotiation fails and the connection cannot be established.

Example: Configure the SSH server to use all encryption algorithms.

```
Switch(config)# ssh-server encryption-algorithm add all
```

2.1.14 service password-encryption type user

Command: service password-encryption type user algo (md5|sha256|aes (salt|)|sm4 (salt|))
no service password-encryption type user

Function: Configures the algorithm used to encrypt user passwords in the configuration file to improve device security. A salt value can be added to make encrypted passwords more varied.

Parameters: md5: The MD5 algorithm.

sha256: The SHA-256 algorithm.

sm4: The SM4 block cipher (Chinese national cryptographic standard).

aes: The AES encryption algorithm.

salt: Adds a salt value for double encryption.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: This command takes effect only after the **service password-encryption** command is configured.

Example: Encrypt passwords in the configuration with SM4 and a salt value.

```
Switch(config)# service password-encryption type user algo sm4 salt
```

2.1.15 bfd authentication key md5

Command: bfd authentication key <1-255> md5 (0 WORD |7 WORD|WORD|)
no bfd authentication key <1-255>

Function: Configures the key number and MD5 authentication string for BFD. The **no** form of this command deletes the configured key.

Parameters: <1-255> is the key number. **<WORD>** is the authentication key string, from 1 to 16 bytes. If option 0 is specified, enter the password in plain text; if option 7 is specified, enter the encrypted string; if no option is specified, the password is entered in secure (hidden) mode.

Default: No key or authentication string is configured.

Command Mode: Global Mode.

Usage Guidelines: Configures the MD5 authentication key string used for BFD authentication. After this command is configured, BFD uses the optional authentication field in its messages, and BFD neighbors are established only when the key configuration is the same at both ends.

Example: Configure MD5 authentication with key number 1 and authentication string 123456.

```
s5(config)#in vlan 50
s5(config)#bfd authentication key 1 md5 123456
```

2.1.16 enable password

Command: enable password (level <1-15> |) (0 LINE|7 WORD|LINE|)
no enable password [level <1-15>]

Function: Configures the password used to enter Admin Mode from User Mode.

Parameters: level <1-15> specifies the privilege level; the default is 15. **<WORD>** or **<LINE>** is the password. If option 0 is specified, enter the password in plain text; if option 7 is specified, enter the encrypted string; if no option is specified, the password is entered in secure (hidden) mode.

Command Mode: Global Mode.

Default: No Admin password is configured.

Usage Guidelines: Configuring an Admin password prevents unauthorized access by users without privileges. We recommend that network administrators set this password during the initial switch configuration. We also recommend exiting Admin Mode with the **exit** command before leaving the terminal unattended for a long time.

2.1.17 enable trustview key

Command: enable trustview key (0 WORD|7 WORD|)
no enable trustview key

Function: Configures the DES encryption key for private messages. This command also enables private message encryption and hashing.

Parameters: <WORD> is a string of fewer than 16 characters used as the DES encryption key. Option 0 specifies a plain-text key and option 7 an encrypted key; if no option is specified, the key is entered in secure (hidden) mode.

Command Mode: Global Mode.

Default: No DES encryption key is configured, and private message encryption and hashing are disabled.

Usage Guidelines: The switch exchanges private information with the network security management system through private messages, which are sent in plain text by default. To protect them, you can encrypt the content of private messages; the administrator must configure the same key on the network security management system.

Example: Enable private message encryption and hashing.

```
Switch(config)#enable trustview key 0 test
```

2.1.18 ip ftp

Command: ip ftp username <username>password (0 LINE|7 WORD|LINE|)
no ip ftp username <username>

Function: Configures the username and password used to log in to an FTP server. The **no** form of this command deletes both the configured username and password.

Parameters: <username> is the FTP username, up to 32 characters. **<LINE>** or **<WORD>** is the FTP password. If option 0 is specified, enter the password in plain text (stored unencrypted); if option 7 is specified, enter the encrypted string; if no option is specified, the password is entered in secure (hidden) mode.

Default: Anonymous FTP login is used.

Command Mode: Global Mode.

Example: Configure the username "Switch" and the password "superuser".

```
Switch#
Switch#config
Switch(config)#ip ftp username Switch password 0 superuser
Switch(config)#
```

2.1.19 ntp authentication-key

Command: ntp authentication-key <key-id> md5 (0 WORD | 7 WORD |)
no ntp authentication-key <key-id>

Function: Enables or disables NTP authentication and defines the authentication key used for NTP authentication.

Parameters: <key-id>: The key number, from 1 to 4294967295. **WORD**: The key value, from 1 to 16 ASCII characters. If no option is specified, press Enter to enter the key in secure (hidden) mode.

Default: No NTP authentication key is configured.

Command Mode: Global Mode.

Usage Guidelines: None.

Example: Define an NTP authentication key with key ID 20 and MD5 key "abc".

```
Switch(config)#ntp authentication-key 20 md5 abc
```

2.1.20 password

Command: password (0 LINE|7 WORD|LINE|)
no password

Function: Configures the password used to enter User Mode through the Console port. The **no** form of this command removes the password.

Parameters: <LINE> or **<WORD>** is the user password. If option 0 is specified, enter the password in plain text (stored unencrypted); if option 7 is specified, enter the encrypted string; if no option is specified, the password is entered in secure (hidden) mode.

Command Mode: Global Mode.

Default: No password is configured.

Usage Guidelines: When this password and the **login** command are both configured, users must enter this password to enter User Mode.

Example:

```
Switch(config)#password 0 test
Switch(config)#login
```

2.1.21 radius-server accounting host

Command: radius-server accounting host {{vrf <vrf-name>| }<ipv4-address> | <ipv6-address>} ((port <port number>|) (key (0 WORD|7 WORD| WORD)|) (primary|)|)
no radius-server accounting host {<ipv4-address> | <ipv6-address>}

Function: Configures the IPv4 or IPv6 address and listening port number of a RADIUS accounting server and whether it is the primary server. The **no** form of this command deletes the RADIUS accounting server.

Parameters: <vrf-name> is the VRF name. **{<ipv4-address> | <ipv6-address>}** is the IPv4 or IPv6 address of the server. **<port-number>** is the listening port number of the server, from 0 to 65535. **<WORD>** is the key string. If the key option is 0, specify a plain-text key of up to 64 characters; if the option is 7, specify an encrypted string of up to 64 characters; if no option is specified, the key is entered in secure (hidden) mode. **primary** sets the server as the primary server. Multiple RADIUS servers can be configured. If no primary server is configured, the switch uses the first available RADIUS server in the configured order; if a primary server is configured, that server is used first.

Command Mode: Global Mode.

Default: No RADIUS accounting server is configured.

Usage Guidelines: Use this command to specify the IPv4 or IPv6 address and port number of the RADIUS accounting server used by the switch. The **<port-number>** parameter specifies the accounting port number, which must match the accounting port number on the RADIUS server; the default is 1813. If the port number is set to 0, a random port is used, which may not work. You can run this command multiple times to configure multiple RADIUS servers. The switch sends accounting messages to all configured accounting servers, which back each other up. If **primary** is configured, that RADIUS server is the primary server. Only one primary RADIUS server can be configured, whether it uses an IPv4 or an IPv6 address.

Example: Configure the RADIUS accounting server with IPv6 address 2004:1:2:3::2 and port number 3000 as the primary server.

```
Switch(config)#radius-server accounting host 2004:1:2:3::2 port 3000 primary
```

2.1.22 radius-server authentication host

Command: radius-server authentication host {<ipv4-address> | <ipv6-address>} (port <0-65535>|)(primary|escape-server|) (access-mode (telnet|dot1x)|)(key (0 WORD |7 WORD| WORD|)|)

no radius-server authentication host {<ipv4-address> | <ipv6-address>}

Function: Configures the IPv4 or IPv6 address, listening port number, encryption key, primary server setting, and access mode of a RADIUS authentication server. The **no** form of this command deletes the RADIUS server.

Parameters: {<ipv4-address> | <ipv6-address>} is the IPv4 or IPv6 address of the server.

<port-number> is the listening port number of the server, from 0 to 65535. **<WORD>** is the key string. If the key option is 0, specify a plain-text key of up to 64 characters; if the option is 7, specify an encrypted string of up to 64 characters; if no option is specified, the key is entered in secure (hidden) mode. **primary** sets the server as the primary server. Multiple RADIUS servers can be configured. If no primary server is configured, the switch uses the first available RADIUS server in the configured order; if a primary server is configured, the most recently configured primary server is used first. **access-mode {dot1x | telnet}** restricts the RADIUS server to 802.1X authentication or Telnet remote authentication only. By default, the RADIUS server is available for all services.

Command Mode: Global Mode.

Default: No RADIUS authentication server is configured.

Usage Guidelines: Use this command to specify the IPv4 or IPv6 address, port number, key string, and access mode of the RADIUS authentication server used by the switch. The **<port-number>** parameter specifies the authentication port number, which must match the authentication port number on the RADIUS server; the default is 1812. If the port number is set to 0, the server may not work. You can run this command multiple times to configure multiple RADIUS servers. Servers are queried in the configured order; once a server responds (whether authentication succeeds or fails), the switch does not send the authentication request to the next server. If **primary** is configured, that RADIUS server is the primary server. If no key is configured for the RADIUS server, the global key configured with the **radius-server key** command is used. You can also restrict the RADIUS server to 802.1X authentication or Telnet remote authentication. The **access-mode** option is not configured by default, so the RADIUS server is available for all remote authentication services.

Example: Configure a RADIUS authentication server with IPv6 address 2004:1:2:3::2.

```
Switch(config)#radius-server authentication host 2004:1:2:3::2
```

2.1.23 radius-server key

Command: radius-server key (0 WORD|7 WORD|)

no radius-server key

Function: Configures the key for RADIUS servers (both authentication and accounting). The **no** form of this command deletes the RADIUS server key.

Parameters: <WORD> is the RADIUS server key string. If the key option is 0, specify a plain-text key of up to 64 characters; if the option is 7, specify an encrypted string of up to 64 characters; if no option is specified, the key is entered in secure (hidden) mode.

Command Mode: Global Mode.

Usage Guidelines: The key is used to encrypt packets exchanged between the switch and the RADIUS server. The key must match the key configured on the RADIUS server; otherwise, RADIUS authentication and accounting fail.

Example: Set the RADIUS authentication key to "test".

```
Switch(config)#radius-server key 0 test
```

2.1.24 tacacs-server authentication host

Command: tacacs-server authentication host {{vrf <vrf-name>| } <ip-address>} [port <port-number>][timeout <seconds>][key (0 WORD|7 WORD|WORD|)][primary]

no tacacs-server authentication host <ip-address>

Function: Configures the IP address, listening port number, authentication timeout, and key string of a TACACS+ authentication server. The **no** form of this command deletes the TACACS+ authentication server.

Parameters: <vrf-name> is the VRF name. **<ip-address>** is the IP address of the server. **<port-number>** is the listening port number of the server, from 0 to 65535; 0 means the server is not used for authentication. **<seconds>** is the TACACS+ authentication timeout, from 1 to 60 seconds. **<WORD>** is the key string. If the key option is 0, specify a plain-text key of up to 64 characters; if the option is 7, specify an encrypted string whose plain-text length does not exceed 64 characters; if no option is specified, press Enter to enter the key in secure (hidden) mode. **primary** sets the server as the primary server.

Command Mode: Global Mode.

Default: No TACACS+ authentication server is configured.

Usage Guidelines: Use this command to specify the IP address, port number, authentication timeout, and key string of the TACACS+ server used by the switch for authentication. The **port** parameter specifies the authentication port number, which must match the authentication port number on the TACACS+ server; the default is 49. The **key** and **timeout** parameters set a key and timeout for this server only. If they are not configured, the global settings configured with the **tacacs-server key <string>** and **tacacs-server timeout <seconds>** commands are used. You can run this command multiple times to configure multiple TACACS+ servers; the switch queries authentication servers in the configured order. If **primary** is configured, that TACACS+ server is the primary server.

Example: Configure a TACACS+ authentication server at 192.168.1.2 that uses the globally configured key.

```
Switch(config)#tacacs-server authentication host 192.168.1.2
```

2.1.25 tacacs-server key

Command: tacacs-server key (0 WORD|7 WORD|)

no tacacs-server key

Function: Configures the key for the TACACS+ authentication server. The **no** form of this command deletes the TACACS+ server key.

Parameters: <WORD> is the TACACS+ server key string. If the key option is 0, specify a plain-text key of fewer than 64 characters; if the option is 7, specify an encrypted string whose plain-text length does not exceed 64 characters; if no option is specified, the key is entered in secure (hidden) mode.

Command Mode: Global Mode.

Usage Guidelines: The key is used to encrypt packets exchanged between the switch and the TACACS+ server. The key must match the key configured on the TACACS+ server; otherwise, TACACS+ authentication fails. To protect TACACS+ authentication data, we recommend configuring an authentication server key.

Example: Set the TACACS+ server authentication key to "test".

```
Switch(config)# tacacs-server key 0 test
```

2.1.26 username

Command: username <username> [privilege <privilege>] [password (0 LINE|7 WORD|LINE|)]
no username <username>

Function: Configures users who log in with username and password authentication and their privilege levels.

Parameters: <username> is the username, up to 32 characters. **<privilege>** is the highest command level the user can execute, from 1 to 15; the default is 1. **<LINE>** or **<WORD>** is the user password. If option 0 is specified, enter the password in plain text; if option 7 is specified, enter the encrypted string (a 32-character MD5-encrypted password); if no option is specified, the password is entered in secure (hidden) mode.

Command Mode: Global Mode.

Usage Guidelines: Commands registered in the system currently have two privilege levels: 1 and 15. Level 1 commands are registered in User Mode; level 15 commands are registered in all other modes. This command supports up to 16 local authentication users, with a maximum password length of 32 characters. Note: Before you use the **authentication line console login local** command to enable local user authentication for Console logins, make sure that at least one user with privilege level 15 exists, so that you can log in, enter Admin Mode and Global Mode, and change the system configuration. If no local user has privilege level 15 and only local authentication is configured for Console logins, users can log in to the switch through the Console port without authentication. For HTTP access, users must log in with a level 15 account; users with a lower level are rejected.

Example: Configure an administrator user "admin" with privilege level 15 and two normal users with privilege level 1, and enable local username and password authentication. Only "admin" can enter Admin Mode through Telnet or the Console port; "user1" and "user2" can log in to User Mode only through Telnet or the Console port. For HTTP logins, only "admin" can log in successfully; "user1" and "user2" are denied.

```
Switch(config)#username admin privilege 15 password 0 admin
Switch(config)#username user1 privilege 1 password 7
4a7d1ed414474e4033ac29ccb8653d9b (MD5-encrypted 32-character form of the
password 0000)
Switch(config)#username user2 password 0 user2
Switch(config)#authentication line console login local
```

Chapter 3 Commands for Layer 2 services

3.1 Port Configuration

3.1.1 Bandwidth

Command: `bandwidth control <bandwidth> {transmit | receive | both}`
`no bandwidth control`

Function: Enables bandwidth limiting on the port. The **no** form of this command disables this function.

Parameters: <bandwidth> is the bandwidth limit in kbps, from 1 to 1000000. **both** applies the limit to both received and transmitted traffic; **receive** applies the limit only to traffic received by the switch; **transmit** applies the limit only to transmitted traffic.

Command Mode: Port Mode.

Default: Disabled.

Usage Guidelines: When bandwidth limiting is enabled, the maximum bandwidth of the port is determined by the configured limit rather than by the port speed. If none of **both**, **receive**, or **transmit** is specified, the default is **both**.

Note: The bandwidth limit cannot exceed the maximum physical speed of the port. If the configured bandwidth is not an integer multiple of the chip's bandwidth granularity, it is adjusted automatically. For example, if the chip granularity is 64 kbps and the configured bandwidth is 50 kbps, the bandwidth is adjusted to 64 kbps.

Example: Set the bandwidth limit of ports 1/0/1-8 to 40000 kbps.

```
Switch(config)#interface ethernet 1/0/1-8
Switch(Config-If-Port-Range)#bandwidth control 40000 both
```

3.1.2 clear counters interface

Command: `clear counters [interface {ethernet <interface-list> | vlan <vlan-id> | port-channel <port-channel-number> | <interface-name>}]`

Function: Clears the statistics of the specified port.

Parameters: <interface-list> is the Ethernet port number; **<vlan-id>** is the VLAN interface number; **<port-channel-number>** is the port channel number; **<interface-name>** is the interface name, such as port-channel 1.

Command Mode: Admin Mode.

Default: Port statistics are not cleared.

Usage Guidelines: If no port is specified, the statistics of all ports are cleared.

Example: Clear the statistics of Ethernet port 1/0/1.

```
Switch#clear counters interface ethernet 1/0/1
```

3.1.3 description

Command: `description <string>`
`no description`

Function: Sets a description for the specified port. The **no** form of this command removes the description.

Parameters: <string> is a character string of up to 200 characters.

Command Mode: Port Mode.

Default: No port description is configured.

Usage Guidelines: Port descriptions help users manage the switch. For example, ports 1/0/1-2, used by the finance department, can be described as "financial"; port 1/0/9, used by the engineering department, as "engineering"; and port 1/0/12, connected to a server, as "Server". This makes the port allocation easy to see.

Example: Set the description of ports 1/0/1-2 to "financial".

```
Switch(config)#interface ethernet 1/0/1-2
Switch(Config-If-Port-Range)#description financial
```

3.1.4 flow control

Command: `flow control`
`no flow control`

Function: Enables flow control on the port. The **no flow control** command disables flow control on the port.

Command Mode: Port Mode.

Default: Disabled.

Usage Guidelines: When flow control is enabled and the received traffic exceeds the port buffer capacity, the port notifies the sending device to slow down to prevent packet loss. Ports support IEEE 802.3x flow control. If flow control causes severe head-of-line (HOL) blocking, the switch automatically starts HOL control (discarding some packets in the CoS queue that may cause HOL blocking) to prevent a sharp drop in network performance.

Note: We do not recommend enabling port flow control unless low packet loss is required and lower network speed and performance are acceptable. When port flow control is enabled, the speed and duplex mode at both ends of the link must be the same.

Example: Enable flow control on ports 1/0/1-8.

```
Switch(config)#interface ethernet 1/0/1-8
Switch(Config-If-Port-Range)#flow control
```

3.1.5 interface ethernet

Command: `interface ethernet <interface-list>`

Function: Enters Port Mode for the specified Ethernet ports from Global Mode.

Parameters: <interface-list> is the port number list.

Command Mode: Global Mode.

Usage Guidelines: Run the **exit** command to return from Port Mode to Global Mode.

Example: Enter Port Mode for ports 1/0/1, 1/0/4-5, and 1/0/8.

```
Switch(config)#interface ethernet 1/0/1;1/0/4-5;1/0/8
Switch(Config-If-Port-Range)#
```

3.1.6 loopback

Command: `loopback`
`no loopback`

Function: Enables loopback testing on an Ethernet port. The **no** form of this command disables loopback testing on the port.

Command Mode: Port Mode.

Default: Disabled.

Usage Guidelines: Use loopback testing to verify that an Ethernet port is working normally. When loopback is enabled, the port behaves as if it were connected to itself, and all traffic sent from the port is received on the same port.

Example: Enable loopback testing on Ethernet ports 1/0/1-8.

```
Switch(config)#interface ethernet 1/0/1-8
Switch(Config-If-Port-Range)#loopback
```

3.1.7 port-rate-statistics interval

Command: port-rate-statistics interval <interval-value>

Function: Sets the port rate statistics interval.

Parameters: <interval-value>: The port rate statistics interval in seconds, from 5 to 600, in increments of 5.

Default: Only the 5-second and 5-minute port rate statistics are displayed.

Command Mode: Global Mode.

Usage Guidelines: None.

Example: Set the port rate statistics interval to 20 seconds.

```
Switch(config)#port-rate-statistics interval 20
```

3.1.8 port-scan-mode

Command: port-scan-mode {interrupt | poll}
no port-scan-mode

Function: Configures the port scan mode as interrupt or poll. The **no** form of this command restores the default scan mode.

Parameters: interrupt: Interrupt mode. **poll**: Poll mode.

Command Mode: Global Mode.

Default: Poll mode.

Usage Guidelines: Two modes can be used to detect port up/down events. In interrupt mode, the hardware raises an interrupt to report the up/down change; in poll mode, software polls the ports to detect events. Interrupt mode is faster: with poll mode, the MRPP convergence time is several hundred milliseconds; with interrupt mode, it is less than 50 milliseconds.

Note: The port scan mode is usually set to poll mode. Interrupt mode is used only in environments with good performance; poll mode is more stable.

Example: Configure the port scan mode as interrupt mode.

```
Switch(config)#port-scan-mode interrupt
```

3.1.9 rate-violation

Command: rate-violation <200-2000000> [recovery <0-86400>]
no rate-violation

Function: Sets the maximum packet receive rate of a port. If the received packet rate exceeds this limit, the port is shut down and recovers after the configured recovery time (300 seconds by default). The **no** form of this command disables rate violation control on the port.

The rate counts all packets received on the port per second, regardless of packet type.

Parameters: <200-2000000>: The maximum packet receive rate of the port, in packets per second.

<0-86400>: The recovery interval after shutdown, in seconds.

recovery: After the specified time, a port that was shut down returns to the up state. **<0-86400>** is the recovery timeout. For example, if a port is shut down because its packet receive rate exceeded the limit, the port comes up again when the configured timeout expires. The default timeout is 300 seconds; 0 means the port never recovers automatically.

Command Mode: Interface Mode.

Default: Rate violation control is disabled.

Usage Guidelines: This command is mainly used to detect abnormal port traffic. For example, when a loop generates a large number of broadcast packets that affect the processing of other tasks, the port is shut down to keep the switch operating normally.

Example: Set the rate violation limit of ports 1/0/8-10 to 10000 pps and the port recovery time to 1200 seconds.

```
Switch(config)#interface ethernet 1/0/8-10
Switch(Config-Port-Range)#rate-violation 10000 recovery 1200
```

3.1.10 show interface

Command: show interface [ethernet <interface-number> | port-channel <port-channel-number> | loopback <loopback-id> | vlan <vlan-id> | tunnel <tunnel-id> | <interface-name>] [detail]
show interface ethernet status
show interface ethernet counter {packet | rate}

Function: Displays information about Layer 3 or Layer 2 interfaces on the switch.

Parameters: <vlan-id> is the VLAN interface number, from 1 to 4094. **<tunnel-id>** is the tunnel number, from 1 to 50. **<loopback-id>** is the loopback interface number, from 1 to 1024. **<interface-number>** is the Ethernet port number. **status** displays key information about all Layer 2 ports. **counter {packet | rate}** displays packet count or rate statistics for all Layer 2 ports. **<port-channel-number>** is the port channel number. **<interface-name>** is the interface name, such as port-channel1. **detail** displays detailed port information.

Command Mode: Admin Mode and Configuration Mode.

Default: None.

Usage Guidelines: For a VLAN interface, this command displays the MAC address, IP address, and packet statistics. For a tunnel interface, it displays the tunnel interface status and the statistics of tunnel packets sent and received at the control plane; for statistics of packets sent and received on the physical interface, see the **show interface ethernet** command. For a loopback interface, it displays the IP address and the statistics of packets sent and received. For an Ethernet port, it displays the port speed, duplex mode, flow control status, broadcast storm suppression setting, and packet statistics. For a port channel, it displays the port speed, duplex mode, flow control status, broadcast storm suppression setting, and packet statistics. If no port is specified, information about all ports on the switch is displayed.

Use **detail** to display detailed information about Ethernet ports and port channels; the information displayed depends on the switch and card type.

For Ethernet ports, **status** displays key information about all Layer 2 ports in a list, one port per row, including the port number, link and protocol status, speed, duplex mode, VLAN, port type, and port name. **counter packet** displays packet count statistics for all Ethernet ports, including Layer 2 unicast, broadcast, multicast, and error packets in the input and output directions. **counter rate** displays rate statistics for all Ethernet ports, including input and output packets and bytes over the last 5 minutes and 5 seconds.

Statistic Field	Description
input errors	Total of CRC, undersize, fragments, and jabber errors
CRC	Total number of received packets between 64 and 1518 octets

	long, inclusive, that had either an FCS error or an alignment error
frame alignment	Total number of received packets that had a bad FCS with a non-integral number of octets (alignment error)
undersize	Total number of received packets shorter than 64 octets
jabber	Total number of received packets longer than 1518 octets (excluding framing bits but including FCS octets) that had either a bad FCS with an integral number of octets (FCS error) or a bad FCS with a non-integral number of octets (alignment error)
fragments	Total number of received packets shorter than 64 octets that had either a bad FCS with an integral number of octets (FCS error) or a bad FCS with a non-integral number of octets (alignment error)
pause frame (input)	Number of 802.3x flow control frames received
output errors	Total of collisions and late collisions
collisions	Best estimate of the total number of collisions on this Ethernet segment
late collisions	Number of times a collision is detected on the interface later than one slot time into the transmission of a packet
pause frame (output)	Number of 802.3x flow control frames sent

Example: Display information about VLAN 1.

```
Switch#show interface vlan 1
Vlan1 is up, line protocol is up, dev index is 2005
Device flag 0x1003(UP BROADCAST MULTICAST)
IPv4 address is:
192.168.10.1      255.255.255.0     (Primary)
Hardware is EtherSVI, address is 00-00-00-00-00-01
MTU is 1500 bytes , BW is 0 Kbit
Encapsulation ARPA, loopback not set
5 minute input rate 0 bytes/sec, 0 packets/sec
5 minute output rate 0 bytes/sec, 0 packets/sec
The last 5 second input rate 0 bytes/sec, 0 packets/sec
The last 5 second output rate 0 bytes/sec, 0 packets/sec
Input packets statistics:
Input queue 0/600, 0 drops
0 packets input, 0 bytes, 0 no buffer
0 input errors, 0 CRC, 0 frame alignment, 0 overrun
0 ignored, 0 abort, 0 length error
Output packets statistics:
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 late collisions
```

Display information about loopback 1.

```
Switch#show interface loopback 1
Loopback1 is up, line protocol is up, dev index is 2006
  Device flag 0x100b(UP BROADCAST LOOP MULTICAST)
  IPv4 address is:
    1.1.1.1          255.255.255.255   (Primary)
  MTU is 1500 bytes , BW is 0 Kbit
  5 minute input rate 0 bytes/sec, 0 packets/sec
  5 minute output rate 0 bytes/sec, 0 packets/sec
  The last 5 second input rate 0 bytes/sec, 0 packets/sec
  The last 5 second output rate 0 bytes/sec, 0 packets/sec
  Input packets statistics:
    Input queue 0/600, 0 drops
    0 packets input, 0 bytes, 0 no buffer
    0 input errors, 0 CRC, 0 frame alignment, 0 overrun
    0 ignored, 0 abort, 0 length error
  Output packets statistics:
    0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 late collisions
```

Display information about tunnel 1.

```
Switch#show interface tunnel 1
Tunnel1 is up, line protocol is up, dev index is 2007
  Device flag 0x91(UP P2P NOARP)
  IPv4 address is:
    (NULL)
  5 minute input rate 0 bytes/sec, 0 packets/sec
  5 minute output rate 0 bytes/sec, 0 packets/sec
  The last 5 second input rate 0 bytes/sec, 0 packets/sec
  The last 5 second output rate 0 bytes/sec, 0 packets/sec
  Input packets statistics:
    Input queue 0/600, 0 drops
    0 packets input, 0 bytes, 0 no buffer
    0 input errors, 0 CRC, 0 frame alignment, 0 overrun
    0 ignored, 0 abort, 0 length error
  Output packets statistics:
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 late collisions
```

Display packet count statistics for all Layer 2 ports.

```
Switch#Show interface ethernet counter packet
Interface        Unicast(pkts)   BroadCast(pkts)    MultiCast(pkts)
Err(pkts)
1/0/1       IN    12,345,678     12,345,678,9       12,345,678,9      4,567
        OUT  23,456,789      34,567,890         5,678          0
1/0/2       IN    0           0               0              0
         OUT  0           0              0              0
1/0/3       IN    0           0               0              0
        OUT  0           0              0              0
1/0/4       IN    0           0               0              0
        OUT  0           0              0              0
…
```

Display rate statistics for all Layer 2 ports.

```
Switch#Show interface ethernet counter rate
Interface         IN(pkts/s)       IN(bytes/s)     OUT(pkts/s)
OUT(bytes/s)
1/0/1       5m   13,473         12,345,678       12,345        1,234,567
        5s    135             65,800          245             92,600
1/0/2       5m   0             0              0              0
        5s       0             0              0              0
1/0/3       5m   0             0              0              0
        5s       0             0              0              0
1/0/4       5m   0             0              0              0
        5s       0             0              0              0
```

3.1.11 shutdown

Command: shutdown
no shutdown

Function: Shuts down the specified Ethernet port. The **no** form of this command enables the port.

Command Mode: Port Mode.

Default: Ethernet ports are enabled.

Usage Guidelines: When an Ethernet port is shut down, it does not send data frames, and the port status displayed by the **show interface** command is "down".

Example: Enable ports 1/0/1-8.

```
Switch(config)#interface ethernet1/0/1-8
Switch(Config-If-Port-Range)#no shutdown
```

3.1.12 storm-control

Command: `storm-control {unicast | broadcast | multicast} <packets>`
`no storm-control {unicast | broadcast | multicast}`

Function: Sets the traffic limit for broadcast, multicast, and unknown-destination unicast traffic on the port. The **no** form of this command disables the limit, allowing broadcast, multicast, and unknown-destination unicast traffic to pass at line rate.

Parameters: unicast limits unknown-destination unicast traffic; **multicast** limits multicast traffic; **broadcast** limits broadcast traffic. **<packets>** is the packet limit, from 1 to 1488905. For non-10 Gbps ports, the unit of **<packets>** is packets per second (pps); for 10 Gbps ports, the unit is kpps (the value multiplied by 1000 is the number of packets allowed per second), so the value must be less than 14880.

Command Mode: Port Mode.

Default: No limit is set; broadcast, multicast, and unknown-destination unicast traffic pass at line rate.

Usage Guidelines: If no VLAN is configured, all ports on the switch belong to the same broadcast domain. The switch floods the three types of traffic above to all ports in the broadcast domain, which can cause broadcast storms and severely degrade switch performance. Storm control helps protect the switch from broadcast storms. Note that the unit differs between 10 Gbps ports and other ports: for 10 Gbps ports, a setting of 3 allows 3,120 packets per second and discards the rest, whereas for other ports the same setting allows 3 broadcast packets per second.

3.1.13 switchport discard packet

Command: `switchport discard packet { tag | untag }`
`no switchport discard packet { tag | untag }`

Function: Configures the port to discard tagged or untagged packets. The **no** form of this command removes the restriction, allowing the port to receive tagged or untagged packets again.

Parameters: tag discards tagged packets; **untag** discards untagged packets.

Command Mode: Port Mode.

Default: No restriction.

Usage Guidelines: None.

Example: Configure port 1/0/8 to discard tagged packets.

```
Switch(config)#interface ethernet 1/0/8
Switch(config-if-ethernet1/0/8)#switchport discard packet tag
```

3.2 Port Isolation

3.2.1 isolate-port group

Command: `isolate-port group <WORD>`
`no isolate-port group <WORD>`

Function: Creates a port isolation group, which defines the scope of port isolation. The **no** form of this command deletes the port isolation group and removes all ports from it.

Parameters: <WORD> is the group name, up to 32 characters.

Command Mode: Global Mode.

Default: None.

Usage Guidelines: You can create port isolation groups as needed. For example, to isolate all downlink ports in a VLAN, create a port isolation group and add all downlink ports of the VLAN to it. A

switch can have up to 30 port isolation groups. To change or rebuild a port isolation group, delete the existing group with the **no** form of this command.

Example: Create a port isolation group named "test".

```
Switch>enable
Switch#config
Switch(config)#isolate-port group test
```

3.2.2 isolate-port group switchport interface

Command: `isolate-port group <WORD> switchport interface [ethernet | port-channel] <IFNAME>`
`no isolate-port group <WORD> switchport interface [ethernet | port-channel] <IFNAME>`

Function: Adds one or more ports to a port isolation group, isolating them from the other ports in the group. The **no** form of this command removes the ports from the group, after which they can communicate normally with the ports in that group. If the removed ports still belong to another port isolation group, they remain isolated from the ports in that group. An Ethernet port that is a member of a port channel cannot be added to a port isolation group, and a member of a port isolation group cannot be added to a port channel. A port can be a member of one or more port isolation groups.

Parameters: <WORD> is the group name, up to 32 characters. If no group with the specified name exists, one is created. **ethernet** specifies that the ports to isolate are Ethernet ports, followed by a list of Ethernet ports separated by ";" and "-", for example, "ethernet 1/0/1;3;4-7;8". **port-channel** specifies that the ports to isolate are port channels. **<IFNAME>** is the interface name, such as e1/0/1; if an interface name is used, the **ethernet** keyword is not required.

Command Mode: Global Mode.

Default: None.

Usage Guidelines: You can add Ethernet ports to or remove them from a port isolation group as needed. A port that belongs to multiple port isolation groups is isolated from all ports in all of those groups.

Example: Add Ethernet ports 1/0/1-2 and 1/0/5 to the port isolation group "test".

```
Switch(config)#isolate-port group test switchport interface ethernet 1/0/1-2;
1/0/5
```

3.2.3 isolate-port apply

Command: `isolate-port apply [<l2|l3|all>]`

Function: Applies the port isolation configuration to isolate Layer 2 traffic, Layer 3 traffic, or all traffic.

Parameters: <l2|l3|all> specifies the traffic to isolate: **l2** isolates Layer 2 traffic, **l3** isolates Layer 3 traffic, and **all** isolates all traffic.

Command Mode: Global Mode.

Default: All traffic is isolated.

Usage Guidelines: Apply the port isolation configuration to Layer 2 traffic, Layer 3 traffic, or all traffic as required.

Example: Apply port isolation to Layer 2 traffic only.

```
Switch(config)#isolate-port apply l2
```

3.2.4 show isolate-port group

Command: `show isolate-port group [<WORD>]`

Function: Displays the port isolation configuration, including all configured port isolation groups and the Ethernet ports in each group.

Parameters: <WORD> is the group name, up to 32 characters. If no group is specified, the configuration of all port isolation groups is displayed.

Command Mode: Admin Mode and Global Mode.

Default: The configuration of all port isolation groups is displayed.

Usage Guidelines: Use this command to view the port isolation configuration.

Example: Display the configuration of the port isolation group "test".

```
Switch(config)#show isolate-port group test
Isolate-port group test
    The isolate-port Ethernet1/0/5
The isolate-port Ethernet1/0/2
```

3.3 Port Loopback Detection

3.3.1 debug loopback-detection

Command: `debug loopback-detection`

Function: Enables loopback detection debugging. Debugging information is generated when packets are sent or received and when the state changes.

Parameters: None.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: Use this command to display packet transmission, packet reception, and state changes.

Example:

```
Switch#debug loopback-detection
%Jan 01 00:07:45:106 2006 Send loopback detection probe packet:dev
Ethernet1/0/5, vlan id 1
%Jan 01 00:07:45:107 2006 Send loopback detection probe packet:dev
Ethernet1/0/5, vlan id 1
%Jan 01 00:07:45:110 2006 Loopback detected on port Ethernet1/0/5, VLAN 1
```

3.3.2 loopback-detection control

Command: `loopback-detection control {shutdown |block| learning}`
`no loopback-detection control`

Function: Enables loopback detection control on the port. The **no** form of this command disables the function.

Parameters: shutdown sets the control method to shutdown: the port is shut down when a loopback is detected.

block sets the control method to block: when a loopback is detected, the port is blocked and only BPDUs and loopback detection packets are allowed.

learning disables MAC address learning on the port, stops forwarding traffic, and deletes the MAC addresses learned on the port.

Default: Disabled.

Command Mode: Port Mode.

Usage Guidelines: After control is enabled on a port and a loopback is detected, the port remains in the controlled state. If a recovery timeout is configured, the port returns to normal when the timeout expires. If the control method is block, you must manually configure the mapping between instances and VLAN IDs; pay attention to this when using this method.

Example: Enable loopback detection control on port 1/0/2.

```
Switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)#loopback-detection control shutdown
Switch(Config-If-Ethernet1/0/2)#no loopback-detection control
```

3.3.3 loopback-detection control-recovery timeout

Command: `loopback-detection control-recovery timeout <0-3600>`

Function: Configures the time after which a port in the controlled state (because a loopback was detected) returns to the uncontrolled state.

Parameters: <0-3600> is the recovery time from the controlled state, in seconds. A value of 0 means the port does not recover automatically.

Default: Ports do not recover automatically.

Command Mode: Global Mode.

Usage Guidelines: When a port detects a loopback and enters the controlled state, it remains controlled and does not recover. In shutdown mode, the port does not send detection packets; in block or learning mode, the port continues to send loopback detection packets to check whether the loopback still exists. If a recovery time is configured, the port returns to normal when the timeout expires. The recovery time is useful mainly for the shutdown control mode; because ports continue loopback detection in the other modes, we do not recommend using this command with them.

Example: Configure automatic recovery from the loopback detection controlled state after 30 seconds.

```
Switch(config)#loopback-detection control-recovery timeout 30
```

3.3.4 loopback-detection interval-time

Command: `loopback-detection interval-time <loopback> <no-loopback>`
`no loopback-detection interval-time`

Function: Sets the loopback detection interval. The **no** form of this command restores the default intervals.

Parameters: <loopback> is the detection interval when a loopback is found, from 5 to 300 seconds.

<no-loopback> is the detection interval when no loopback is found, from 1 to 30 seconds.

Default: 5 seconds when a loopback exists and 3 seconds otherwise.

Command Mode: Global Mode.

Usage Guidelines: When no loopback exists, a relatively short detection interval can be used. When a loopback exists, a detection interval that is too short can severely affect the whole network, so a relatively long interval is recommended.

Example: Set the loopback detection intervals to 35 and 15 seconds.

```
Switch(config)#loopback-detection interval-time 35 15
```

3.3.5 loopback-detection trap enable

Command: `loopback-detection trap enable`
`no loopback-detection trap enable`

Function: Enables sending SNMP traps when loopback detection detects a loop. The **no** form of this command disables the function.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: After loopback detection and trap sending are enabled, an SNMP trap is sent when a loop is detected on a port.

Example: Enable loopback detection traps.

```
Switch(config)# loopback-detection trap enable
```

3.3.6 loopback-detection specified-vlan

Command: `loopback-detection specified-vlan <vlan-list>`
`no loopback-detection specified-vlan [<vlan-list>]`

Function: Enables loopback detection on the port and specifies the VLANs to check. The **no** form of this command disables loopback detection on the port or for the specified VLANs.

Parameters: <vlan-list> is the list of VLANs to check. On a trunk port, which carries multiple VLANs, you can specify the VLANs to check with this parameter.

Default: Loopback detection is disabled on the port.

Command Mode: Port Mode.

Usage Guidelines: If the port is a trunk port carrying multiple VLANs, loopback detection can be performed per port and VLAN, that is, on specified VLANs of the port. If the port is an access port, only one VLAN can be checked even if multiple VLANs are configured. This function is not supported on port channels.

Example: Enable loopback detection on port 1/0/2.

```
Switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)#switchport mode trunk
Switch(Config-If-Ethernet1/0/2)#switchport trunk allowed vlan all
Switch(Config-If-Ethernet1/0/2)#loopback-detection specified-vlan 1;3;5-20
Switch(Config-If-Ethernet1/0/2)#no loopback-detection specified-vlan 1;3;5-20
```

3.3.7 loopback-detection send packet number

Command: `loopback-detection send packet number <1-10>`
`no loopback-detection send packet number`

Function: Configures the number of packets the port sends in each detection cycle. The **no** form of this command restores the default.

Parameters: <1-10>: The number of packets.

Default: 1 packet.

Command Mode: Port Mode.

Usage Guidelines: After loopback detection is enabled, the port sends 1 packet per detection cycle by default. If a loop occurs, the port bandwidth may be consumed by a broadcast storm or other traffic, causing loop detection packets to be lost. In this case, increase the number of detection packets so that loops can still be detected promptly despite packet loss.

Example:

```
Switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)# loopback-detection send packet number 2
```

3.3.8 show loopback-detection

Command: show loopback-detection [interface <interface-list>]

Function: Displays the loopback detection state of all ports if no parameter is specified, or the state and result of the specified ports.

Parameters: <interface-list> is the list of ports to display, for example, ethernet 1/0/1.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Use this command to display the loopback detection state and result of ports.

Example: Display the loopback detection state of port 1/0/4.

```
Switch(config)#show loopback-detection interface Ethernet 1/0/4
loopback detection config and state information in the switch!
PortName            Loopback Detection            Control Mode   Is
Controlled
Ethernet1/0/4           Enable                        Shutdown      No
```

3.4 ULDP

3.4.1 debug uldp

Command: debug uldp (hello | probe | echo | unidir | all) [receive | send] interface [ethernet] IFNAME
no debug uldp (hello | probe | echo | unidir | all) [receive | send] interface [ethernet] IFNAME

Function: Enables debugging for the specified ULDP packets, or all ULDP packets, sent and received on a port. After debugging is enabled, information about the packets sent and received is displayed on the terminal. The **no** form of this command disables the debugging.

Parameters: hello: Hello (advertisement) packets, including common advertisement packets, RSY packets, and Flush packets.

probe: Probe (detection) packets.

echo: Echo packets, which are responses to probe packets.

unidir: Unidir packets, which advertise a detected unidirectional link.

all: All ULDP packets.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: For example, use the following command to check the probe packets received on port 1/0/2.

```
Switch#debug uldp probe receive interface ethernet 1/0/2
```

3.4.2 debug uldp error

Command: debug uldp error
no debug uldp error

Function: Enables ULDP error message debugging. The **no** form of this command disables the function.

Parameters: None.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: Use this command to display error messages.

Example: Display error messages.

```
Switch#debug uldp error
```

3.4.3 debug uldp event

Command: **debug uldp event**
no debug uldp event

Function: Enables ULDP event debugging. The **no** form of this command disables the function.

Parameters: None.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: Use this command to display all types of event information.

Example: Display event information.

```
Switch#debug uldp event
```

3.4.4 debug uldp fsm interface ethernet

Command: **debug uldp fsm interface ethernet <IFname>**
no debug uldp fsm interface ethernet <IFname>

Function: Enables ULDP state machine debugging for the specified interface. The **no** form of this command disables the debugging.

Parameters: ***<IFname>*** is the interface name.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: Use this command to display state transitions of the specified interface.

Example: Display state transitions of interface ethernet 1/0/1.

```
Switch#debug uldp fsm interface ethernet 1/0/1
```

3.4.5 debug uldp interface ethernet

Command: **debug uldp {hello|probe|echo|unidir|all} [receive|send]**
interface ethernet <IFname>
no debug uldp {hello|probe|echo|unidir|all} [receive|send]
interface ethernet <IFname>

Function: Enables debugging that displays packet details. After it is enabled, details of the specified packet types on the interface are displayed on the terminal.

Parameters: <IFname>: The interface name.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: For example, use the following command to display details of Hello packets received on interface Ethernet 1/0/1.

```
Switch#debug uldp hello receive interface Ethernet 1/0/1
```

3.4.6 debug uldp packet

Command: `debug uldp packet [receive|send]`
`no debug uldp packet [receive|send]`

Function: Enables debugging for packets sent and received. After it is enabled, the type and interface of packets sent and received are displayed. The **no** form of this command disables the function.

Parameters: None.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: For example, use the following command to display packets received on each interface.

```
Switch#debug uldp packet receive
```

3.4.7 uldp aggressive-mode

Command: `uldp aggressive-mode`
`no uldp aggressive-mode`

Function: Configures ULDP to work in aggressive mode. The **no** form of this command restores normal mode.

Parameters: None.

Command Mode: Global Mode and Port Mode.

Default: Normal mode.

Usage Guidelines: The ULDP working mode can be configured only when ULDP is enabled globally. When ULDP aggressive mode is enabled globally, all existing fiber ports work in aggressive mode. For ports that become available after the configuration, enable aggressive mode in Port Mode.

Example: Enable ULDP aggressive mode globally.

```
Switch(config)#uldp aggressive-mode
```

3.4.8 uldp enable

Command: `uldp enable`

Function: Enables ULDP. In Global Mode, this command enables ULDP globally; in Port Mode, it enables ULDP on the port.

Parameters: None.

Command Mode: Global Mode and Port Mode.

Default: ULDP is not configured.

Usage Guidelines: ULDP can be configured on ports only when ULDP is enabled globally. When ULDP is enabled globally, it takes effect on all existing fiber ports. For ports that become available after ULDP is enabled, run this command in Port Mode to enable ULDP on them.

Example: Enable ULDP in Global Mode.

```
Switch(config)#uldp enable
```

3.4.9 uldp disable

Command: `uldp disable`

Function: Disables ULDP.

Parameters: None.

Command Mode: Global Mode and Port Mode.

Default: ULDP is not configured.

Usage Guidelines: When ULDP is disabled globally, ULDP is disabled on all ports.

Example: Disable ULDP in Global Mode.

```
Switch(config)#uldp disable
```

3.4.10 uldp hello-interval

Command: `uldp hello-interval <integer>`
`no uldp hello-interval`

Function: Configures the interval at which ULDP sends Hello messages. The **no** form of this command restores the default interval.

Parameters: <integer>: The Hello message interval, from 5 to 100 seconds. The default is 10 seconds.

Command Mode: Global Mode.

Default: 10 seconds.

Usage Guidelines: The Hello message interval can be configured only when ULDP is enabled globally. The value ranges from 5 to 100 seconds.

Example: Set the Hello message interval to 12 seconds.

```
Switch(config)#uldp hello-interval 12
```

3.4.11 uldp manual-shutdown

Command: `uldp manual-shutdown`
`no uldp manual-shutdown`

Function: Configures ULDP to work in manual shutdown mode. The **no** form of this command restores automatic mode.

Parameters: None.

Command Mode: Global Mode.

Default: Automatic mode.

Usage Guidelines: This command can be used only when ULDP is enabled globally.

Example: Enable manual shutdown mode globally.

```
Switch(config)#uldp manual-shutdown
```

3.4.12 uldp recovery-time

Command: `uldp recovery-time<integer>`
`no uldp recovery-time`

Function: Configures the ULDP recovery timer. The **no** form of this command restores the default.

Parameters: <integer>: The ULDP recovery timer timeout, from 30 to 86400 seconds.

Command Mode: Global Mode.

Default: 0, which disables automatic recovery.

Usage Guidelines: If an interface is shut down by ULDP and the recovery timer expires, the interface is reset automatically. If the recovery timer is set to 0, the interface is not reset.

Example: Set the recovery timer to 600 seconds.

```
Switch(config)#uldp recovery-time 600
```

3.4.13 uldp reset

Command: `uldp reset`

Function: Resets ports that were shut down by ULDP.

Parameters: None.

Command Mode: Global Mode and Port Mode.

Default: None.

Usage Guidelines: This command takes effect only on interfaces that were shut down by ULDP.

Example: Reset all ports that were shut down by ULDP.

```
Switch(config)#uldp reset
```

3.4.14 show uldp

Command: `show uldp [interface ethernet<interface-name>]`

Function: Displays the global ULDP configuration and the interface status. If <interface-name> is specified, the ULDP configuration and status of the interface and its neighbors are displayed.

Parameters: <interface-name> is the interface name.

Command Mode: Admin Mode and Configuration Mode.

Default: None.

Usage Guidelines: If no parameter is specified, the global ULDP information is displayed. If an interface name is specified, information about the interface and its neighbors is displayed along with the global information.

Example: Display the global ULDP information.

```
Switch(config)#show uldp
```

3.5 LLDP

3.5.1 clear lldp remote-table

Command: `clear lldp remote-table`

Function: Clears the remote table entries on the port.

Parameters: None.

Default: Entries are not cleared.

Command Mode: Port Mode.

Usage Guidelines: Clears the remote table entries on this port.

Example: Clear the remote table entries on this port.

```
Switch(Config-If-Ethernet 1/0/1)# clear lldp remote-table
```

3.5.2 debug lldp

Command: `debug lldp`
`no debug lldp`

Function: Enables LLDP debugging. The **no** form of this command disables LLDP debugging.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: When debugging is enabled, you can check packet transmission and reception and other information.

Example: Enable LLDP debugging on the switch.

```
Switch#debug lldp
```

3.5.3 debug lldp packets

Command: **debug lldp packets interface ethernet <IFNAME>**
no debug lldp packets interface ethernet <IFNAME>

Function: Displays LLDP packet transmission and reception information on the port. The **no** form of this command disables the debugging.

Parameters: **<IFNAME>**: The interface name.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: When debugging is enabled, you can check packet transmission and reception and other information on the port.

Example: Enable LLDP packet debugging on port 1/0/1.

```
Switch#debug lldp packets interface ethernet 1/0/1
%Jan 01 00:02:40 2006 LLDP-PDU-TX   PORT= ethernet 1/0/1
```

3.5.4 lldp enable

Command: **lldp enable**
lldp disable

Function: Enables LLDP globally. The **lldp disable** command disables LLDP globally.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: When LLDP is enabled globally, it is enabled on every port.

Example: Enable LLDP on the switch.

```
Switch(config)#lldp enable
```

3.5.5 lldp enable (Port)

Command: **lldp enable**
lldp disable

Function: Enables LLDP on the port in Port Mode. The **lldp disable** command disables LLDP on the port.

Parameters: None.

Default: LLDP is enabled on ports.

Command Mode: Port Mode.

Usage Guidelines: When LLDP is enabled globally, it is enabled on every port. Use this command to disable LLDP on ports where it is not needed.

Example: Disable LLDP on port ethernet 1/0/5.

```
Switch(config)#in ethernet 1/0/5
Switch(Config-If-Ethernet1/0/5)#lldp disable
```

3.5.6 lldp mode

Command: `lldp mode <send | receive | both | disable>`

Function: Configures the LLDP operating state of the port.

Parameters: send: LLDP only sends packets.

receive: LLDP only receives packets.

both: LLDP both sends and receives packets.

disable: LLDP neither sends nor receives packets.

Default: both.

Command Mode: Port Mode.

Usage Guidelines: Selects the operating state of the LLDP agent on the port.

Example: Set the LLDP operating state of port ethernet 1/0/5 to receive.

```
Switch(config)#in ethernet 1/0/5
Switch(Config-If-Ethernet1/0/5)#lldp mode receive
```

3.5.7 lldp msgTxHold

Command: `lldp msgTxHold <value>`
`no lldp msgTxHold`

Function: Sets the multiplier used to calculate the aging time (TTL) carried in LLDP update messages sent by all LLDP-enabled ports.

Parameters: <value> is the aging time multiplier, from 2 to 10.

Default: 4.

Command Mode: Global Mode.

Usage Guidelines: The aging time is the product of the multiplier and the message transmission interval; its maximum value is 65535 seconds.

Example: Set the aging time multiplier to 6.

```
Switch(config)#lldp msgTxHold 6
```

3.5.8 lldp neighbors max-num

Command: `lldp neighbors max-num <value>`
`no lldp neighbors max-num`

Function: Sets the maximum number of entries that can be stored in the remote MIB.

Parameters: <value> is the maximum number of entries, from 5 to 500.

Default: 100.

Command Mode: Port Mode.

Usage Guidelines: Sets the maximum number of entries stored in the remote MIB.

Example: Set the maximum number of remote entries on port ethernet 1/0/5 to 200.

```
Switch(config)#in ethernet 1/0/5
Switch(Config-If-Ethernet1/0/5)# lldp neighbors max-num 200
```

3.5.9 lldp notification interval

Command: `lldp notification interval <seconds>`
`no lldp notification interval`

Function: Sets the interval at which the system checks whether the remote table has changed; if it has, the system sends a trap to the SNMP manager.

Parameters: <seconds> is the interval, from 5 to 3600 seconds.

Default: 5 seconds.

Command Mode: Global Mode.

Usage Guidelines: After the notification interval is configured, a trap is sent at the end of each interval if the remote table has changed.

Example: Set the trap notification interval to 20 seconds.

```
Switch(config)#lldp notification interval 20
```

3.5.10 lldp tooManyNeighbors

Command: lldp tooManyNeighbors {discard | delete}

Function: Sets the action taken when the remote table is full.

Parameters: discard: Discards the current message.

delete: Deletes the entry with the shortest TTL in the remote table.

Default: Discard.

Command Mode: Port Mode.

Usage Guidelines: When the remote MIB is full, **discard** discards the received message, and **delete** deletes the entry with the shortest TTL in the remote table.

Example: Set the action on port ethernet 1/0/5 to delete.

```
Switch(config)#in ethernet 1/0/5
Switch(Config-If-Ethernet1/0/5)#lldp tooManyNeighbors delete
```

3.5.11 lldp transmit delay

Command: lldp transmit delay <seconds>
no lldp transmit delay

Function: Sets the LLDP transmit delay. Because local information may change frequently as the network changes, many update messages could be sent in a short time; a delay ensures accurate local information statistics.

If the transmit delay is at its default and tx-interval is configured, the transmit delay becomes one quarter of the tx-interval instead of the default of 2 seconds.

Parameters: <seconds> is the delay, from 1 to 8192 seconds.

Default: 2 seconds.

Command Mode: Global Mode.

Usage Guidelines: When messages are sent continuously, a transmit delay prevents remote information from being updated repeatedly because of messages sent at the same time.

Example: Set the transmit delay to 3 seconds.

```
Switch(config)#lldp transmit delay 3
```

3.5.12 lldp transmit optional tlv

Command: lldp transmit optional tlv [portDesc] [sysName] [sysDesc] [sysCap]
no lldp transmit optional tlv

Function: Configures the optional TLVs sent on the port.

Parameters: portDesc: Port description. **sysName**: System name. **sysDesc**: System description. **sysCap**: System capabilities.

Default: No optional TLVs are sent.

Command Mode: Port Mode.

Usage Guidelines: Each optional TLV can appear only once in a message. The **portDesc** TLV carries the local port name; **sysName** carries the local system name; **sysDesc** carries the local system description; **sysCap** carries the local system capabilities.

Example: Configure port ethernet 1/0/5 to send the portDesc and sysCap TLVs.

```
Switch(config)#in ethernet 1/0/5
Switch(Config-If-Ethernet1/0/5)# lldp transmit optional tlv portDesc sysCap
```

3.5.13 lldp trap

Command: `lldp trap <enable | disable>`

Function: Enables or disables LLDP traps on the specified port: **enable** enables traps; **disable** disables traps.

Parameters: None.

Default: Disabled.

Command Mode: Port Mode.

Usage Guidelines: Enables sending trap messages on the port.

Example: Enable LLDP traps on port ethernet 1/0/5.

```
Switch(config)#in ethernet1/0/5
Switch(Config-If-Ethernet1/0/5)#lldp trap enable
```

3.5.14 lldp tx-interval

Command: `lldp tx-interval <integer>`
`no lldp tx-interval`

Function: Sets the interval at which update messages are sent on all LLDP-enabled ports, from 5 to 32768 seconds; the default is 30 seconds.

Parameters: <integer> is the update message interval, from 5 to 32768 seconds.

Default: 30 seconds.

Command Mode: Global Mode.

Usage Guidelines: After the interval is configured, LLDP messages are received only after the configured interval. The interval must be less than or equal to half of the aging time: an interval that is too long causes entries to age out and be rebuilt too often, while an interval that is too short increases network traffic and reduces available port bandwidth. The message aging time is the product of the multiplier and the transmit interval, up to 65535 seconds.

If tx-interval is at its default and the transmit delay is configured, tx-interval becomes four times the transmit delay instead of the default of 40 seconds.

Example: Set the transmit interval to 40 seconds.

```
Switch(config)#lldp tx-interval 40
```

3.5.15 show debugging lldp

Command: `show debugging lldp`

Function: Displays all ports on which LLDP debugging is enabled.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: The **show debugging lldp** command displays all ports on which LLDP debugging is enabled.

Example: Display all ports on which LLDP debugging is enabled.

```
Switch(config)#show debugging lldp
====BEGINNING OF  LLDP DEBUG SETTINGS====
debug lldp
debug lldp packets interface Ethernet1/0/1
debug lldp packets interface Ethernet1/0/2
debug lldp packets interface Ethernet1/0/3
debug lldp packets interface Ethernet1/0/4
debug lldp packets interface Ethernet1/0/5
=============END OF DEBUG SETTINGS===============
```

3.5.16 show lldp

Command: show lldp

Function: Displays the global LLDP configuration, such as the list of LLDP-enabled ports, the update message interval, the aging time setting, the time the transmit module waits before reinitializing, the trap interval, and the limit on remote table entries.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Global Mode.

Usage Guidelines: Use the **show lldp** command to check the global LLDP configuration.

Example: Check the global LLDP configuration after LLDP is enabled on the switch.

```
Switch(config)#show lldp
-----LLDP GLOBAL INFORMATIONS-----
LLDP enabled port : Ethernet 1/0/1
LLDP interval :30
LLDP txTTL :120
LLDP txShutdownWhile :2
LLDP NotificationInterval :5
LLDP txDelay :20
-------------END-----------------
```

3.5.17 show lldp interface ethernet

Command: show lldp interface ethernet <IFNAME>

Function: Displays the LLDP configuration of the port, such as the operating state of the LLDP agent.

Parameters: <IFNAME>: The interface name.

Default: None.

Command Mode: Admin Mode and Global Mode.

Usage Guidelines: Use the **show lldp interface ethernet <IFNAME>** command to check the LLDP configuration of the port.

Example: Check the LLDP configuration of the port after LLDP is enabled on the switch.

```
Switch(config)#show lldp interface ethernet 1/0/1
Port name :   ethernet 1/0/1
 LLDP Agent Adminstatus: Both
 LLDP Operation TLV: portDecs  sysName  sysDesc  sysCap
 LLDP Trap Status: disable
 LLDP maxRemote: 100
 LLDP Overflow handle: discard
LLDP interface remote status : Full
```

3.5.18 show lldp neighbors interface ethernet

Command: show lldp neighbors interface ethernet < IFNAME >

Function: Displays the LLDP neighbor information of the port.

Parameters: <IFNAME>: The interface name.

Default: None.

Command Mode: Admin Mode and Global Mode.

Usage Guidelines: Use the **show lldp neighbors interface ethernet <IFNAME>** command to check the LLDP neighbor information of the port.

Example: Check the LLDP neighbor information of the port after LLDP is enabled on the port.

```
Switch(config)#show lldp neighbors interface ethernet 1/0/1
```

3.5.19 show lldp traffic

Command: show lldp traffic

Function: Displays LLDP packet statistics.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Global Mode.

Usage Guidelines: Use the **show lldp traffic** command to check LLDP packet statistics.

Example: Check LLDP packet statistics after LLDP is enabled on the switch.

```
Switch(config)#show lldp traffic
PortName  Ageouts  FramesDiscarded  FramesInErrors  FramesIn  FramesOut
TLVsDiscarded  TLVsUnrecognized --------------   -------      ---------------
--------------       --------     ---------       -------------
----------------
Ethernet1/0/1    0            0                0             0          7
0               0
```

3.6 LLDP-MED

3.6.1 civic location

Command: civic location {dhcp server | switch | endpointDev} <country-code>
no civic location

Function: Configures the device type and country code of the location in Civic Address LCI format and enters Civic Address LCI Address Mode. The **no** form of this command removes all Civic Address LCI location settings.

Parameters: dhcp server: Sets the device type to DHCP server.

switch: Sets the device type to switch.

endpointDev: Sets the device type to LLDP-MED endpoint.

<country-code>: Sets the two-letter country code, such as DE or US, in accordance with ISO 3166.

Default: No Civic Address LCI location is configured on the port.

Command Mode: Port Mode.

Usage Guidelines: Configures the device type and country code of the Civic Address LCI location and enters Civic Address LCI Address Mode, where you can configure detailed location information.

Example: Configure the device type as switch and the country code as US for the Civic Address LCI location on Ethernet port 1/0/19.

```
Switch(Config-If-Ethernet1/0/19)# civic location switch US
Switch(Med-Civic)#
```

3.6.2 {description-language | province-state | city | county | street | locationNum | location | floor | room | postal | otherInfo}

Command: {description-language | province-state | city | county | street | locationNum | location | floor | room | postal | otherInfo} <address>

no {description-language | province-state | city | county | street | locationNum | location | floor | room | postal | otherInfo}

Function: Configures detailed location information in Civic Address LCI Address Mode of the port.

Parameters: description-language: The language used to describe the location, such as "English".

province-state: State, canton, region, province, or prefecture, such as "clara".

city: City, such as "New York".

county: County or parish, such as "santa clara".

street: Street, such as "1301 Shoreway Road".

locationNum: House number, such as "9".

location: Name and occupant of a location, such as "Carrillo's Holiday Market".

floor: Floor number, such as "13".

room: Room number, such as "1308".

postal: Postal or ZIP code, such as "10027-1234".

otherInfo: Additional location information, such as "South Wing".

<address>: The detailed address information, up to 250 characters.

Default: No detailed Civic Address LCI location information is configured on the port.

Command Mode: Civic Address LCI Address Mode.

Usage Guidelines: Use this command to configure detailed Civic Address LCI location information on the port. Up to 10 address types can be configured.

Example: Configure detailed location information in Civic Address LCI Address Mode.

```
Switch(Med-Civic)# city example
Switch(Med-Civic)# street shangdi
```

3.6.3 ecs location

Command: ecs location <tel-number>

no ecs location

Function: Configures a location in ECS ELIN format on the port. The **no** form of this command removes the configured location.

Parameters: <tel-number>: The location string in ECS ELIN format, such as an emergency telephone number, from 10 to 25 characters.

Default: No ECS ELIN location is configured.

Command Mode: Port Mode.

Usage Guidelines: The ECS ELIN location string must be 10 to 25 characters long.

Example: Configure an ECS ELIN location on port 1/0/19.

```
Switch(Config-If-Ethernet1/0/19)# ecs location 880-445-3381
```

3.6.4 lldp med fast count

Command: `lldp med fast count <value>`
`no lldp med fast count`

Function: Sets the number of LLDP packets with LLDP-MED TLVs sent rapidly when the LLDP-MED fast start mechanism is triggered. The **no** form of this command restores the default.

Parameters: <value>: The number of packets sent rapidly, from 1 to 10.

Default: 4.

Command Mode: Global Mode.

Usage Guidelines: Use this command to set the number of packets sent rapidly.

Example:

```
Switch(config)#lldp med fast count 5
```

3.6.5 lldp med trap

Command: `lldp med trap {enable | disable}`

Function: Enables or disables sending trap messages on the specified port when the LLDP-MED network topology changes.

Parameters: enable: Enables LLDP-MED traps on the port.

disable: Disables LLDP-MED traps on the port.

Default: Disabled.

Command Mode: Port Mode.

Usage Guidelines: Enables or disables LLDP-MED traps on the port.

Example: Enable LLDP-MED traps on port 1/0/19.

```
Switch(Config-If-Ethernet1/0/19)# lldp med trap enable
```

3.6.6 lldp transmit med tlv all

Command: `lldp transmit med tlv all`
`no lldp transmit med tlv all`

Function: Configures the specified port to send all LLDP-MED TLVs. The **no** form of this command disables the function.

Parameters: None.

Default: The port does not send LLDP-MED TLVs.

Command Mode: Port Mode.

Usage Guidelines: After this command is configured, if the port can send LLDP-MED TLVs, its LLDP packets carry all LLDP-MED TLVs supported by the switch. After the **no** form is configured, LLDP packets sent by the port carry no LLDP-MED TLVs.

Example: Enable port 1/0/19 to send LLDP-MED TLVs.

```
Switch(Config-If-Ethernet1/0/19)# lldp transmit med tlv all
```

3.6.7 lldp transmit med tlv capability

Command: `lldp transmit med tlv capability`
`no lldp transmit med tlv capability`

Function: Configures the specified port to send the LLDP-MED Capabilities TLV. The **no** form of this command disables the function.

Parameters: None.

Default: Disabled.

Command Mode: Port Mode.

Usage Guidelines: After this command is configured, if the port can send LLDP-MED TLVs, its LLDP packets carry the LLDP-MED Capabilities TLV. After the **no** form is configured, LLDP packets sent by the port do not carry the LLDP-MED Capabilities TLV. Note: The LLDP-MED Capabilities TLV is the key LLDP-MED TLV; if the port is not first configured to send it, no other LLDP-MED TLVs are sent.

Example: Enable port 1/0/19 to send the LLDP-MED Capabilities TLV.

```
Switch(Config-If-Ethernet1/0/19)# lldp transmit med tlv capability
```

3.6.8 lldp transmit med tlv location

Command: `lldp transmit med tlv location`
`no lldp transmit med tlv location`

Function: Configures the specified port to send the LLDP-MED Location Identification TLV. The **no** form of this command disables the function.

Parameters: None.

Default: Disabled.

Command Mode: Port Mode.

Usage Guidelines: After this command is configured, if the port can send LLDP-MED TLVs, its LLDP packets carry the LLDP-MED Location Identification TLV. After the **no** form is configured, LLDP packets sent by the port do not carry this TLV even if the port can send LLDP-MED TLVs. Note: The port must first be configured to send the LLDP-MED Capabilities TLV. If the device does not support PoE or PoE is disabled on the port, this TLV is not sent.

Example: Enable port 1/0/19 to send the LLDP-MED Location Identification TLV.

```
Switch(Config-If-Ethernet1/0/19)#lldp transmit med tlv location
```

3.6.9 lldp transmit med tlv inventory

Command: `lldp transmit med tlv inventory`
`no lldp transmit med tlv inventory`

Function: Configures the specified port to send the LLDP-MED Inventory Management TLV set, which includes 7 TLVs: Hardware Revision, Firmware Revision, Software Revision, Serial Number, Manufacturer Name, Model Name, and Asset ID. The **no** form of this command disables the function.

Parameters: None.

Default: Disabled.

Command Mode: Port Mode.

Usage Guidelines: After this command is configured, if the port can send LLDP-MED TLVs, its LLDP packets carry the LLDP-MED Inventory Management TLVs. After the **no** form is configured, LLDP packets sent by the port do not carry these TLVs. Note: The port must first be configured to send the LLDP-MED Capabilities TLV; otherwise, the configuration fails.

Example: Enable port 1/0/19 to send the LLDP-MED Inventory Management TLVs.

```
Switch(Config-If-Ethernet1/0/19)# lldp transmit med tlv inventory
```

3.6.10 lldp transmit med tlv networkPolicy

Command: `lldp transmit med tlv networkPolicy`
`no lldp transmit med tlv networkPolicy`

Function: Configures the specified port to send the LLDP-MED Network Policy TLV. The **no** form of this command disables the function.

Parameters: None.

Default: Disabled.

Command Mode: Port Mode.

Usage Guidelines: After this command is configured, if the port can send LLDP-MED TLVs, its LLDP packets carry the LLDP-MED Network Policy TLV. After the **no** form is configured, LLDP packets sent by the port do not carry this TLV. Note: The port must first be configured to send the LLDP-MED Capabilities TLV; otherwise, the configuration fails.

Example: Enable port 1/0/19 to send the LLDP-MED Network Policy TLV.

```
Switch(Config-If-Ethernet1/0/19)# lldp transmit med tlv networkPolicy
```

3.6.11 network policy

Command: `network policy {voice | voice-signaling | guest-voice | guest-voice-signaling | softphone-voice | video-conferencing | streaming-video | video-signaling} [status {enable | disable}] [tag {tagged | untagged}] [vid {<vlan-id> | dot1p}] [cos <cos-value>] [dscp <dscp-value> ]`
`no network policy {voice | voice-signaling | guest-voice | guest-voice-signaling | softphone-voice | video-conferencing | streaming- video | video-signaling}`

Function: Configures the network policy of the port, including the VLAN ID, the supported application types (such as voice and video), the application priority, and the policy used.

Parameters: voice, **voice-signaling**, **guest-voice**, **guest-voice-signaling**, **softphone-voice**, **video-conferencing**, **streaming-video**, and **video-signaling**: The application types supported on the port.

status: Specifies whether the network policy is in use.

enable: The network policy for the application type is defined. This is the default.

disable: The network policy for the application type is unknown; fields such as the VLAN ID, Layer 2 priority, and DSCP are ignored, and the network connectivity device does not send the TLV for this application type.

tag: Specifies whether the application uses **tagged** or **untagged** VLAN mode.

tagged: Traffic of the application is tagged; the VLAN ID, Layer 2 priority, and DSCP fields take effect.

untagged: Traffic of the application is untagged; the VLAN ID and Layer 2 priority fields are ignored and only the DSCP field takes effect. Untagged is the default.

vid: Configures the VLAN ID of the application. When the peer sends traffic of the application, it tags the traffic with the advertised VLAN ID; otherwise, the VLAN ID is 1.

<vlan-id>: The VLAN ID, from 1 to 4094.

dot1p: Tags the application traffic with an 802.1p priority and carries it in VLAN 0.

cos: Configures the Layer 2 (802.1p) priority of the frames.

<cos-value>: The Layer 2 priority value, from 0 to 7. The default is 5.

dscp: Configures the DSCP value.

<dscp-value>: The DSCP value, from 0 to 63. The default is 46.

Default: No network policy is configured on the port.

Command Mode: Port Mode.

Usage Guidelines: You can configure multiple network policies on a port, but each must have a different application type, and each policy corresponds to one LLDP-MED Network Policy TLV. If multiple policies are configured on a port, the LLDP packet carries multiple Network Policy TLVs. If no network policy is configured, no Network Policy TLV is sent.

Example: Configure a network policy for the voice application on port 1/0/19.

```
Switch(Config-If-Ethernet1/0/19)# network policy voice tag tagged vid 2 cos 6
dscp 23
```

3.6.12 show lldp

Command: `show lldp`

Function: Displays the global LLDP and LLDP-MED configuration.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example: Display the global LLDP and LLDP-MED configuration.

```
Switch#show lldp
-----LLDP GLOBAL INFORMATIONS-----
LLDP has been enabled globally.
LLDP enabled port : Ethernet1/0/19
LLDP interval :5
LLDP txTTL :20
LLDP NotificationInterval :5
LLDP txDelay :1
LLDP-MED FastStart Repeat Count :4
-------------END-----------------
```

3.6.13 show lldp [interface ethernet <IFNAME>]

Command: `show lldp [interface ethernet <IFNAME>]`

Function: Displays the LLDP and LLDP-MED configuration of the port.

Parameters: interface ethernet <IFNAME>: The port name.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: None.

Example: Display the LLDP and LLDP-MED configuration of port 1/0/19.

```
Switch#show lldp interface ethernet 1/0/19
 Port name :Ethernet1/0/19
 LLDP Agent Adminstatus : Both
 LLDP Operation TLV : default
 LLDP Trap Status : disable
 LLDP maxRemote :100
 LLDP Overflow handle : discard
 LLDP interface remote status : Free
 MED Optional TLV : capabilities  networkPolicy  location  power  inventory
 MED Trap Status:Enable
 MED TLV Transmit Status:Disable
 MED Fast Transmit Status:Disable
```

3.6.14 show lldp neighbors

Command: show lldp neighbors [interface ethernet <IFNAME>]

Function: Displays the LLDP and LLDP-MED information of the port's neighbors.

Parameters: <IFNAME>: The interface name.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Use this command to check the LLDP and LLDP-MED information of neighbors after the port receives LLDP packets from them.

Example: Display neighbor information on port 1/0/1.

```
Switch #show lldp neighbors interface ethernet 1/0/1
Port name : Ethernet1/0/1
Port Remote Counter : 1
TimeMark :20
ChassisIdSubtype :4
ChassisId :00-03-0f-00-00-02
PortIdSubtype :Local
PortId :3
PortDesc :Ethernet1/0/1
SysName :switch
SysDesc :switch Device, Compiled Feb 12 17:39:53 2011
 SoftWare Version 6.2.30.0
 BootRom Version 4.0.1
 HardWare Version
 Device serial number
 Copyright (C) 2001-2011 by Vendor.
 All rights reserved
```

3.6.15 show lldp traffic

Command: show lldp traffic

Function: Displays statistics of LLDP and LLDP-MED packets sent and received.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: After the port receives LLDP packets from its neighbors, use this command to view statistics of LLDP and LLDP-MED packets sent and received.

Example: View statistics of packets sent and received after LLDP is enabled.

```
Switch(config)#show lldp traffic
PortName Ageouts FramesDiscarded  FramesInErrors   FramesIn   FramesOut
TLVsDiscarded   TLVsUnrecognized
-----------   -------       ---------------        --------------    --------
---------        -------------       ----------------
Ethernet1/0/1   0           0               0           0            7
0                 0
```

3.7 Port Channel

3.7.1 debug port-channel

Command: debug port-channel <port-group-number> {all | event | fsm | packet | timer}
no debug port-channel [<port-group-number>]

Function: Enables port channel debugging.

Parameters: <port-group-number> is the port channel group number, from 1 to 125.

all: All debugging information.

event: Event debugging information.

fsm: State machine debugging information.

packet: LACP packet debugging information.

timer: Timer debugging information.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: Enable debugging to check port channel debugging information.

Example:

(1) Debug the state machine of port group 1.

```
Switch#debug port-channel 1 fsm
```

(2) Debug LACP packets of port group 2.

```
Switch#debug port-channel 2 packet
```

(3) Enable all debugging for port group 1.

```
Switch#debug port-channel 1 all
```

3.7.2 interface port-channel

Command: interface port-channel <port-channel-number>

Function: Enters Port Channel Configuration Mode.

Command Mode: Global Mode.

Usage Guidelines: In Port Channel Configuration Mode, GVRP and spanning tree settings apply to the port channel. If the port channel does not exist (that is, the ports have not been aggregated), an error message is displayed and the configuration is saved; it is applied when the ports are aggregated. This restoration occurs only once: if a port channel is removed and aggregated again, the initial user configuration is not restored. Settings for other modules, such as shutdown, are applied to all member ports of the corresponding port group.

Example: Enter configuration mode for port-channel 1.

```
Switch(config)#interface port-channel 1
Switch(Config-If-Port-Channel1)#
```

3.7.3 lacp port-priority

Command: lacp port-priority <port-priority>
no lacp port-priority

Function: Sets the LACP port priority.

Parameters: <port-priority>: The LACP port priority, from 0 to 65535.

Command Mode: Port Mode.

Default: 32768.

Usage Guidelines: Use this command to change the LACP port priority. The **no** form of this command restores the default.

Example: Set the LACP port priority.

```
Switch(Config-If-Ethernet1/0/1)# lacp port-priority 30000
```

3.7.4 lacp system-priority

Command: **lacp system-priority <system-priority>**
no lacp system-priority

Function: Sets the LACP system priority.

Parameters: <system-priority>: The LACP system priority, from 0 to 65535.

Command Mode: Global Mode.

Default: 32768.

Usage Guidelines: Use this command to change the LACP system priority. The **no** form of this command restores the default.

Example: Set the LACP system priority.

```
Switch(config)#lacp system-priority 30000
```

3.7.5 lacp timeout

Command: **lacp timeout {short | long}**
no lacp timeout

Function: Sets the LACP timeout mode.

Parameters: short or **long** timeout mode.

Command Mode: Port Mode.

Default: Long.

Usage Guidelines: Sets the LACP timeout mode.

Example: Set the LACP timeout mode to short.

```
Switch(Config-If-Ethernet1/0/1)#lacp timeout short
```

3.7.6 load-balance

Command: **load-balance {dst-src-mac | dst-src-ip | dst-src-mac-ip}**

Function: Sets the load-balancing mode of the switch. The setting applies to both port groups and ECMP.

Parameters: dst-src-mac balances load based on the source and destination MAC addresses.

dst-src-ip balances load based on the source and destination IP addresses.

dst-src-mac-ip balances load based on the source and destination MAC addresses and the source and destination IP addresses.

Command Mode: Global Mode.

Default: Load balancing is based on the source and destination MAC addresses.

Usage Guidelines: Port channels or ECMP can be used to balance load; configure the load-balancing mode as required. If the specified mode differs from the current mode, the switch changes to the specified mode; otherwise, it displays a message indicating that the mode is already configured.

Example: Set the load-balancing mode.

```
Switch(config)#load-balance src-mac-ip
```

3.7.8 load-balance hash-random

Command: `load-balance hash-random`

Function: Generates hash factors randomly, independent of packet fields (that is, independent of traffic samples).

Parameters: None.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: Adds a load-balancing mode based on a pseudo-random number generator (PRNG), which generates hash factors randomly, independent of packet fields and traffic samples. The disadvantage is that packet order within a flow is not guaranteed; for example, even a single fixed flow is distributed randomly.

Example:

```
Switch(config)#load-balance hash-random
```

3.7.9 load-balance ingress-port

Command: `load-balance ingress-port`

Function: Uses the ingress port as a hash factor for load sharing.

Parameters: None.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: Uses the ingress port as a hash factor for load sharing.

Example:

```
Switch(config)#load-balance ingress-port
```

3.7.10 load-balance hash-shift

Command: `load-balance hash-shift { ipv4 | ipv6 } { dstip| srcip} value <0-3>`

Function: When load sharing is based on IP fields, specifies the right-shift offset applied to the IP header field.

Parameters: ipv4 | ipv6: The IP version. **dstip | srcip**: The destination or source IP address field. **value <0-3>**: The shift value.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: When load sharing is based on IP fields, this command specifies the right-shift offset applied to the IP header field.

Example:

```
Switch(config)#lload-balance hash-shift  ipv6  dstip value  1
```

3.7.11 port-group

Command: `port-group <port-group-number>`
`no port-group <port-group-number>`

Function: Creates a port group. The **no** form of this command deletes the group.

Parameters: <port-group-number> is the port channel group number, from 1 to 125.

Default: No port group exists.

Command Mode: Global Mode.

Example: Create a port group.

```
Switch(config)# port-group 1
```

Delete a port group.

```
Switch(config)#no port-group 1
```

3.7.12 port-group mode

Command: port-group <port-group-number> mode {active | passive | on}
no port-group

Function: Adds a physical port to a port channel. The **no** form of this command removes the port from the port channel.

Parameters: <port-group-number> is the port channel group number, from 1 to 125. **active** enables LACP on the port in active mode; **passive** enables LACP on the port in passive mode; **on** forces the port to join the port channel without LACP.

Command Mode: Port Mode.

Default: Ports do not belong to any port channel, and LACP is disabled.

Usage Guidelines: All ports added to a port group must have the same speed, configuration, and physical properties. If the specified port group does not exist, an error message is displayed. All ports in a port group must be added in the same mode, that is, the mode used by the first port added. Adding a port in "on" mode forces aggregation: the local port aggregates regardless of information from the remote end, and aggregation succeeds as long as all ports have consistent VLAN information. Adding a port in "active" or "passive" mode enables LACP. The ports on at least one end must be added in "active" mode; if the ports on both ends are added in "passive" mode, they never aggregate.

Example: In Port Mode of Ethernet 1/0/1, add the port to port group 1 in active mode.

```
Switch(Config-If-Ethernet1/0/1)#port-group 1 mode active
```

3.7.13 show port-group

Command: show port-group [<port-group-number>] {brief | detail |}

Function: Displays the configuration of the specified port group or of all configured port channels.

Parameters: <port-group-number> is the port channel group number, from 1 to 125. **brief** displays summary information; **detail** displays detailed information.

Command Mode: All Configuration Modes.

Usage Guidelines: If no port group number is specified, information about all existing port groups is displayed. If the port channel for the specified group number does not exist, an error message is displayed; otherwise, the current information of the specified port channel is displayed.

Example: 1. Display summary information of the port groups.

```
Switch#show port-group brief
ID: port group number; Mode: port group mode such as on active or passive;
Ports: different types of port number of a port group,
the first is selected ports number, the second is standby ports number, and
the third is unselected ports number.
ID  Mode  Partner ID               Ports     Load-balance
------------------------------------------------------------------------
--------
1   active  0x8000,00-12-cf-4d-e1-a1  8,1,1     dst-src-mac
```

```
10  passive 0x8000,00-12-cf-4d-e1-b2  8,2,0     dst-src-ip
20  on                            8,0,0    dst-src-mac-ip
```

2. Display detailed information of port group 1.

```
Switch#show port-group 1 detail
Flags:  A -- LACP_Activity, B -- LACP_timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired
Port-group number: 1,  Mode: active,   Load-balance: dst-src-mac
Port-group detail information:
System ID: 0x8000,00-03-0f-0c-16-6d
Local:
Port             Status      Priority  Oper-Key   Flag
---------------------------------------------------------
Ethernet1/0/1      Selected    32768     1        {ACDEF}
  Ethernet1/0/2      Selected    32768     1        {ACDEF}
  Ethernet1/0/3      Selected    32768     1        {ACDEF}
  Ethernet1/0/4      Selected    32768     1        {ACDEF}
  Ethernet1/0/5      Selected    32768     1        {ACDEF}
  Ethernet1/0/6      Selected    32768     1        {ACDEF}
  Ethernet1/0/7      Selected    32768     1        {ACDEF}
  Ethernet1/0/8      Selected    32768     1        {ACDEF}
  Ethernet1/0/20     Unselected  32768     1        {ACG}
Ethernet1/0/23     Standby     32768     1        {AC}
Remote:
Actor           Partner  Priority  Oper-Key   SystemID                    Flag
---------------------------------------------------------------------------
Ethernet1/0/1     1        32768     1        0x8000,00-03-0f-01-02-04
{CDEF}
  Ethernet1/0/2     2        32768     1        0x8000,00-03-0f-01-02-04
{CDEF}
  Ethernet1/0/3     3        32768     1        0x8000,00-03-0f-01-02-04
{CDEF}
  Ethernet1/0/4     4        32768     1        0x8000,00-03-0f-01-02-04
{CDEF}
  Ethernet1/0/5     5        32768     1        0x8000,00-03-0f-01-02-04
{CDEF}
  Ethernet1/0/6     6        32768     1        0x8000,00-03-0f-01-02-04
{CDEF}
  Ethernet1/0/7     7        32768     1        0x8000,00-03-0f-01-02-04
{CDEF}
  Ethernet1/0/8     8        32768     1        0x8000,00-03-0f-01-02-04
{CDEF}
  Ethernet1/0/23   23       32768     1        0x8000,00-03-0f-01-02-04
{C}
Switch#
```

3.8 MTU

3.8.1 mtu

Command: `mtu [<mtu-value>]`
`no mtu`

Function: Enables receiving jumbo frames (MTU). The **no** form of this command restores the normal frame size range of 64 to 1518 bytes.

Parameters: <mtu-value>: The MTU of frames that can be received, in bytes, from 1500 to 9000. The corresponding frame size is 1518/1522 to 9018/9022 bytes. If this parameter is not specified, the maximum allowed frame size is 9018/9022 bytes.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Configure the MTU on the switches at both ends; otherwise, jumbo frames are dropped by the switch on which the MTU is not configured.

Example: Enable the MTU function on the switch.

```
Switch(config)#mtu
```

3.9 bpdu-tunnel

3.9.1 bpdu-tunnel dmac

Command: bpdu-tunnel dmac <mac>
no bpdu-tunnel dmac

Function: Configures the BPDU tunnel MAC address globally. The **no** form of this command restores the default tunnel MAC address.

Parameters: <mac>: The MAC address.

Command Mode: Global Mode.

Default: The default tunnel MAC address.

Usage Guidelines: Configures the tunnel MAC address globally. The configured MAC address, which must be a multicast MAC address, is used to forward the specified protocol packets across the tunnel.

Example: Configure the tunnel MAC address.

```
Switch(Config)# bpdu-tunnel dmac 01-02-03-04-05-06
```

3.9.2 bpdu-tunnel stp

Command: bpdu-tunnel stp
no bpdu-tunnel stp

Function: Configures the specified port to forward STP packets across the tunnel. The **no** form of this command cancels the configuration.

Parameters: None.

Command Mode: Port Mode.

Default: The port does not forward any protocol packets across the tunnel.

Usage Guidelines: Disable STP on the port before configuring this command.

Example: Configure Ethernet port 1/0/5 to forward STP packets across the tunnel.

```
Switch(Config)#in Ethernet 1/0/5
Switch(Config-if-ethernet  1/0/5)#bpdu-tunnel stp
```

3.9.3 bpdu-tunnel gvrp

Command: bpdu-tunnel gvrp
no bpdu-tunnel gvrp

Function: Configures the specified port to forward GVRP packets across the tunnel. The **no** form of this command cancels the configuration.

Parameters: None.

Command Mode: Port Mode.

Default: The port does not forward any protocol packets across the tunnel.

Usage Guidelines: Disable GVRP on the port before configuring this command.

Example: Configure Ethernet port 1/0/5 to forward GVRP packets across the tunnel.

```
Switch(Config)#in ethernet 1/0/5
Switch(Config-if-ethernet 1/0/5)#bpdu-tunnel gvrp
```

3.9.4 bpdu-tunnel uldp

Command: bpdu-tunnel uldp
no bpdu-tunnel uldp

Function: Configures the specified port to forward ULDP packets across the tunnel. The **no** form of this command cancels the configuration.

Parameters: None.

Command Mode: Port Mode.

Default: The port does not forward any protocol packets across the tunnel.

Usage Guidelines: Disable ULDP on the port before configuring this command.

Example: Configure Ethernet port 1/0/5 to forward ULDP packets across the tunnel.

```
Switch(Config)#in ethernet 1/0/5
Switch(Config-if-ethernet 1/0/5)#bpdu-tunnel uldp
```

3.9.5 bpdu-tunnel lacp

Command: bpdu-tunnel lacp
no bpdu-tunnel lacp

Function: Configures the specified port to forward LACP packets across the tunnel. The **no** form of this command cancels the configuration.

Parameters: None.

Command Mode: Port Mode.

Default: The port does not forward any protocol packets across the tunnel.

Usage Guidelines: Disable LACP on the port before configuring this command.

Example: Configure Ethernet port 1/0/5 to forward LACP packets across the tunnel.

```
Switch(Config)#in ethernet 1/0/5
Switch(Config-if-ethernet 1/0/5)#bpdu-tunnel lacp
```

3.9.6 bpdu-tunnel dot1x

Command: bpdu-tunnel dot1x
no bpdu-tunnel dot1x

Function: Configures the specified port to forward 802.1X (dot1x) packets across the tunnel. The **no** form of this command cancels the configuration.

Parameters: None.

Command Mode: Port Mode.

Default: The port does not forward any protocol packets across the tunnel.

Usage Guidelines: Disable 802.1X on the port before configuring this command.

Example: Configure Ethernet port 1/0/5 to forward 802.1X packets across the tunnel.

```
Switch(Config)#in ethernet  1/0/5
Switch(Config-if-ethernet 1/0/5)#bpdu-tunnel dot1x
```

3.10 DDM

3.10.1 clear transceiver threshold-violation

Command: `clear transceiver threshold-violation [interface ethernet <interface-list>]`

Function: Clears transceiver monitoring threshold violations.

Parameters: interface ethernet <interface-list>: The list of interfaces whose transceiver threshold violations are cleared.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: None.

Example: Clear transceiver threshold violations on ports 1/0/21, 1/0/25, 1/0/26, and 1/0/28.

```
Switch#clear transceiver threshold-violation interface ethernet 1/0/21;25-
26;28
```

3.10.2 debug transceiver

Command: `debug transceiver {on | off}`

Function: Enables or disables DDM debugging.

Parameters: on | off: Enables or disables debugging.

Command Mode: Admin Mode.

Default: Off.

Usage Guidelines: Press Ctrl+O to disable DDM debugging.

Example: Enable DDM debugging.

```
Switch#debug transceiver on
```

3.10.3 show transceiver

Command: `show transceiver [interface ethernet <interface-list>] [detail]`

Function: Displays transceiver monitoring information.

Parameters: interface ethernet <interface-list>: The list of interfaces whose transceiver monitoring information is displayed.

detail: Displays detailed transceiver monitoring information.

Command Mode: User Mode, Admin Mode, and Global Mode.

Default: None.

Usage Guidelines: Temperature is displayed as an integer; other values are displayed to two decimal places. A parameter that exceeds a warning threshold is marked "W+" or "W-"; a parameter that exceeds an alarm threshold is marked "A+" or "A-". Parameters without a mark are normal.

Example: Display brief DDM information for all ports.

```
Switch#show transceiver
Interface  Temp (℃)  Voltage (V)  Bias (mA)   RX Power (dBM)     TX
Power (dBM)
1/0/25    33         3.31         6.11          -30.54(A-)            -6.01
1/0/26    33         5.00 (W+)  6.11          -20.54(W-)            -6.02
```

3.10.4 show transceiver threshold-violation

Command: show transceiver threshold-violation [interface ethernet <interface-list>]

Function: Displays transceiver monitoring threshold violation information.

Parameters: interface ethernet <interface-list>: The list of interfaces whose transceiver monitoring information is displayed.

Command Mode: Admin Mode and Global Mode.

Default: None.

Usage Guidelines: None.

Example: Display transceiver threshold violation information.

```
Switch(config)#show transceiver threshold-violation interface ethernet
1/0/25-26
Ethernet 1/0/25 transceiver threshold-violation information：Transceiver
monitor is enabled. Monitor interval is set to 30 minutes.
The current time is Jan 02 12:30:50 2010.
The last threshold-violation time is Jan 01 1:30:50 2010.
Brief alarm information:
  RX loss of signal
RX power low
Detail diagnostic and threshold information:
                    Diagnostic                                          Threshold
Realtime Value  High Alarm  Low Alarm    High Warn   Low Warn
-----------------   -----------    -----------      ------------   ---------
Temperature (℃)  33            70          0            70          0
Voltage (V)       7.31          10.00        0.00         5.00        0.00
Bias current (mA)  3.11        10.30        0.00         5.00        0.00
RX Power (dBM)  -30.54(A-)     9.00         -25.00 (-34)  9.00        -25.00
TX Power (dBM)  -1.01          9.00        -12.05        9.00        -10.00
Ethernet 1/0/22 transceiver threshold-violation information:
Transceiver monitor is disabled. Monitor interval is set to 30 minutes.
The last threshold-violation doesn’t exist.
```

3.10.5 transceiver-monitoring

Command: transceiver-monitoring {enable | disable}

Function: Enables or disables transceiver monitoring.

Parameters: enable | disable: Enables or disables the function.

Command Mode: Port Mode.

Default: Disabled.

Usage Guidelines: None.

Example: Enable transceiver monitoring on ethernet1/0/1.

```
Switch(config-if-ethernet1/0/1)#transceiver-monitoring enable
```

3.10.6 transceiver-monitoring interval

Command: transceiver-monitoring interval <minutes>
no transceiver-monitoring interval

Function: Sets the transceiver monitoring interval. The **no** form of this command restores the default interval of 15 minutes.

Parameters: <minutes>: The transceiver monitoring interval, in minutes.

Command Mode: Global Mode.

Default: 15 minutes.

Usage Guidelines: None.

Example: Set the transceiver monitoring interval to 1 minute.

```
Switch(config)#transceiver-monitoring interval 1
```

3.10.7 transceiver threshold

Command: `transceiver threshold {default | {temperature | voltage | bias | rx-power | tx-power} {high-alarm | low-alarm | high-warn | low-warn} {<value> | default}}`

Function: Sets user-defined thresholds.

Parameters: default: Restores the manufacturer's default thresholds. If no monitoring parameter is specified, all thresholds are restored; if a monitoring parameter is specified, only its thresholds are restored.

temperature: The temperature monitoring parameter.

voltage: The voltage monitoring parameter.

bias: The bias current monitoring parameter.

rx-power: The receive power monitoring parameter.

tx-power: The transmit power monitoring parameter.

high-alarm: The high alarm threshold; values above it are marked A+.

low-alarm: The low alarm threshold; values below it are marked A-.

high-warn: The high warning threshold; values above it are marked W+.

low-warn: The low warning threshold; values below it are marked W-.

Command Mode: Port Mode.

Default: Thresholds set by the manufacturer.

Usage Guidelines: The threshold ranges for each monitoring parameter are as follows:

Temperature: -128.00 to 128.00 °C

Voltage: 0.00 to 7.00 V

Bias current: 0.00 to 140.00 mA

rx-power: -50.00 to 9.00 dBm

tx-power: -50.00 to 9.00 dBm

A user-configured threshold value can be up to 20 characters long. After a user threshold is configured, the manufacturer's threshold is shown in parentheses when thresholds are displayed, and alarms are raised according to the user configuration.

Example: On ethernet1/0/1, set the low warning threshold of the fiber module transmit power to -12.

```
Switch(config-if-ethernet1/0/1)#transceiver threshold tx-power low-warn -12
```

3.10.8 optician monitor enable|disable

Command: `optician monitor enable|disable`

Function: Enables or disables the optical module monitoring (tsfpmonitor) thread.

Parameters: None.

Command Mode: Global Mode.

Default: Enabled.

Usage Guidelines: None.

Example: Enable the optical module monitoring (tsfpmonitor) thread.

```
Switch(config)#optician monitor enable
```

When an optical module is inserted:

```
%MODULE-1-INSERT: connector of Ethernet1/0/48 is inserted!
```

When an optical module is removed:

```
%MODULE-1-INSERT: connector of Ethernet1/0/48 is removed!
Switch(config)#optician monitor disable
```

After monitoring is disabled, no message is displayed when an optical module is inserted.

3.11 EFM OAM

3.11.1 clear ethernet-oam

Command: `clear ethernet-oam [interface {ethernet |} <IFNAME>]`

Function: Clears OAM packet and link event statistics on the specified port or all ports.

Parameters: <IFNAME>: The name of the port whose OAM statistics are cleared.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: None.

Example: Clear OAM packet and link event statistics on all ports.

```
Switch#clear ethernet-oam
```

3.11.2 debug ethernet-oam error

Command: `debug ethernet-oam error [interface {ethernet |} <IFNAME>]`
`no debug ethernet-oam error [interface {ethernet |} <IFNAME>]`

Function: Enables debugging of OAM error information. The **no** form of this command disables the debugging.

Parameters: <IFNAME>: The name of the port on which debugging is enabled or disabled.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: None.

Example: Enable debugging of OAM error information on ethernet1/0/1.

```
Switch#debug ethernet-oam error interface ethernet1/0/1
```

3.11.3 debug ethernet-oam fsm

Command: `debug ethernet-oam fsm {all | Discovery | Transmit} [interface {ethernet |} <IFNAME>]`
`no debug ethernet-oam fsm {all | Discovery | Transmit} [interface {ethernet |} <IFNAME>]`

Function: Enables debugging of the OAM state machine. The **no** form of this command disables the debugging.

Parameters: <IFNAME>: The name of the port on which debugging is enabled or disabled.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: None.

Example: Enable debugging of the Discovery state machine on ethernet1/0/1.

```
Switch#debug ethernet-oam fsm Discovery interface ethernet1/0/1.
```

3.11.4 debug ethernet-oam packet

Command: debug ethernet-oam packet [detail] {all | send | receive} [interface {ethernet |} <IFNAME>]
no debug ethernet-oam packet [detail] {all | send | receive} interface {ethernet |} <IFNAME>

Function: Enables debugging of packets sent or received by OAM. The **no** form of this command disables the debugging.

Parameters: <IFNAME>: The name of the port on which debugging is enabled or disabled.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: None.

Example: Enable debugging of packets sent and received on ethernet1/0/1.

```
Switch#debug ethernet-oam packet detail all interface ethernet1/0/1
```

3.11.5 debug ethernet-oam timer

Command: debug ethernet-oam timer {all | pdu_timer | local_lost_link_timer} [interface {ethernet |} <IFNAME>]
no debug ethernet-oam timer {all | pdu_timer | local_lost_link_timer} [interface {ethernet | } <IFNAME>]

Function: Enables debugging of timer refresh information for the specified timer or all timers. The **no** form of this command disables the debugging.

Parameters: <IFNAME>: The name of the port on which debugging is enabled or disabled.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: None.

Example: Enable debugging of refresh information for all timers on ethernet1/0/1.

```
Switch#debug ethernet-oam timer all interface ethernet1/0/1
```

3.11.6 ethernet-oam

Command: ethernet-oam
no ethernet-oam

Function: Enables Ethernet OAM on the port. The **no** form of this command disables Ethernet OAM on the port.

Parameters: None.

Command Mode: Port Mode.

Default: Disabled.

Usage Guidelines: None.

Example: Enable Ethernet OAM on Ethernet port 1/0/4.

```
Switch(config)#interface ethernet 1/0/4
Switch(Config-If-Ethernet1/0/4)#ethernet-oam
```

3.11.7 ethernet-oam errored-frame threshold high

Command: `ethernet-oam errored-frame threshold high {<high-frames> | none}`
`no ethernet-oam errored-frame threshold high`

Function: Configures the high threshold for errored frame events. The **no** form of this command restores the default.

Parameters: <high-frames>: The high detection threshold for errored frame events, from 2 to 4294967295.

none: Cancels the high threshold configuration.

Command Mode: Port Mode.

Default: None.

Usage Guidelines: If the number of errored frames within the detection period is greater than or equal to the high threshold, a critical link event is triggered, and the device notifies the peer by sending an Information OAMPDU with the Link Fault flag in the Flags field set to 1. The high threshold cannot be less than the low threshold.

Example: Set the high threshold for errored frame events on Ethernet port 1/0/4 to 3000.

```
Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame threshold high
3000
```

3.11.8 ethernet-oam errored-frame threshold low

Command: `ethernet-oam errored-frame threshold low <low-frames>`
`no ethernet-oam errored-frame threshold low`

Function: Configures the low threshold for errored frame events. The **no** form of this command restores the default.

Parameters: <low-frames>: The low detection threshold for errored frame events, from 1 to 4294967295.

Command Mode: Port Mode.

Default: 1.

Usage Guidelines: If the number of errored frames within the detection period is greater than or equal to the low threshold, an errored frame event is triggered, and the device notifies the peer by sending an Event Notification OAMPDU. The low threshold cannot be greater than the high threshold.

Example: Set the low threshold for errored frame events on Ethernet port 1/0/4 to 100.

```
Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame threshold low 100
```

3.11.9 ethernet-oam errored-frame window

Command: `ethernet-oam errored-frame window <seconds>`
`no ethernet-oam errored-frame window`

Function: Configures the detection period for errored frame events. The **no** form of this command restores the default.

Parameters: <seconds>: The period over which errored frames are counted, from 5 to 300, in units of 200 ms.

Command Mode: Port Mode.

Default: 5.

Usage Guidelines: The number of errored frames on the port is checked at the end of each detection period. If the number of errored frames is greater than or equal to the threshold, the corresponding event is triggered and the peer is notified through an OAMPDU.

Example: Set the detection period for errored frame events on port 1/0/4 to 20 seconds.

```
Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame window 100
```

3.11.10 ethernet-oam errored-frame-period threshold high

Command: ethernet-oam errored-frame-period threshold high {<high-frames> | none}
no ethernet-oam errored-frame-period threshold high

Function: Configures the high threshold for errored frame period events. The **no** form of this command restores the default.

Parameters: <high-frames>: The high detection threshold for errored frame period events, from 2 to 4294967295.

none: Cancels the high threshold configuration.

Command Mode: Port Mode.

Default: None.

Usage Guidelines: If the number of errored frames within the detection period is greater than or equal to the high threshold, a critical link event is triggered, and the device notifies the peer by sending an Information OAMPDU with the Link Fault flag in the Flags field set to 1. The high threshold cannot be less than the low threshold.

Example: Set the high threshold for errored frame period events on port 1/0/4 to 3000.

```
Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame-period threshold
high 3000
```

3.11.11 ethernet-oam errored-frame-period threshold low

Command: ethernet-oam errored-frame-period threshold low <low-frames>
no ethernet-oam errored-frame-period threshold low

Function: Configures the low threshold for errored frame period events. The **no** form of this command restores the default.

Parameters: <low-frames>: The low detection threshold for errored frame period events, from 1 to 4294967295 frames.

Command Mode: Port Mode.

Default: 1.

Usage Guidelines: If the number of errored frames within the detection period is greater than or equal to the low threshold, an errored frame period event is triggered, and the device notifies the peer by sending an Event Notification OAMPDU. The low threshold cannot be greater than the high threshold.

Example: Set the low threshold for errored frame period events on port 1/0/4 to 100.

```
Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame-period threshold
low 100
```

3.11.12 ethernet-oam errored-frame-period window

Command: ethernet-oam errored-frame-period window <seconds>
no ethernet-oam errored-frame-period window

Function: Configures the detection period for errored frame period events. The **no** form of this command restores the default.

Parameters: <seconds>: The period over which errored frames are counted, from 1 to 300, in units of 200 ms.

Command Mode: Port Mode.

Default: 5.

Usage Guidelines: Errored frames on the port are checked at the end of each detection period. If the number of errored frames is greater than or equal to the threshold, the corresponding event is triggered and the device notifies the peer through an OAMPDU. When packets are sent, the window field of the errored frame period event is filled with the maximum number of frames, calculated as follows: maximum number of frames = interface bandwidth × detection period (seconds) ÷ (64 × 8), where the detection period is the window value configured, in seconds.

Example: Set the detection period for errored frame period events on port 1/0/4 to 10 seconds.

```
Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame-period window 50
```

3.11.13 ethernet-oam errored-frame-seconds threshold high

Command: ethernet-oam errored-frame-seconds threshold high {<high-seconds> | none}
no ethernet-oam errored-frame-seconds threshold high

Function: Configures the high threshold for errored frame seconds events. The **no** form of this command restores the default.

Parameters: <high-seconds>: The high detection threshold for errored frame seconds events, from 2 to 65535 seconds.

none: Cancels the high threshold configuration.

Command Mode: Port Mode.

Default: None.

Usage Guidelines: If the number of errored frame seconds within the detection period is greater than or equal to the high threshold, a critical link event is triggered, and the device notifies the peer by sending an Information OAMPDU with the Link Fault flag in the Flags field set to 1. The high threshold cannot be less than the low threshold. An errored frame second is a second in which at least one errored frame is received.

Example: Set the high threshold for errored frame seconds events on port 1/0/4 to 3000.

```
Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame-seconds threshold
high 3000
```

3.11.14 ethernet-oam errored-frame-seconds threshold low

Command: ethernet-oam errored-frame-seconds threshold low <low-seconds>
no ethernet-oam errored-frame-seconds threshold low

Function: Configures the low threshold for errored frame seconds events. The **no** form of this command restores the default.

Parameters: <low-seconds>: The low detection threshold for errored frame seconds events, from 1 to 65535 seconds.

Command Mode: Port Mode.

Default: 1.

Usage Guidelines: If the number of errored frame seconds within the detection period is greater than or equal to the low threshold, an errored frame seconds event is triggered, and the device notifies the peer by sending an Event Notification OAMPDU. The low threshold cannot be greater than the high threshold. An errored frame second is a second in which at least one errored frame is received.

Example: Set the low threshold for errored frame seconds events on port 1/0/4 to 100.

```
Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame-seconds threshold
low 100
```

3.11.15 ethernet-oam errored-frame-seconds window

Command: `ethernet-oam errored-frame-seconds window <seconds>`
`no ethernet-oam errored-frame-seconds window`

Function: Configures the detection period for errored frame seconds events. The **no** form of this command restores the default.

Parameters: <seconds>: The detection period, from 50 to 4500, in units of 200 ms.

Command Mode: Port Mode.

Default: 300.

Usage Guidelines: Errored frame seconds on the port are checked at the end of each detection period. If the number of errored frame seconds is greater than or equal to the threshold, the corresponding event is triggered and the device notifies the peer through an OAMPDU.

Example: Set the detection period for errored frame seconds events on port 1/0/4 to 120 seconds.

```
Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame-seconds window 600
```

3.11.16 ethernet-oam errored-symbol-period threshold high

Command: `ethernet-oam errored-symbol-period threshold high {<high-symbols> | none}`
`no ethernet-oam errored-symbol-period threshold high`

Function: Configures the high threshold for errored symbol period events. The **no** form of this command restores the default.

Parameters: <high-symbols>: The high detection threshold for errored symbol period events, from 2 to 18446744073709551615 symbols.

none: Cancels the high threshold configuration.

Command Mode: Port Mode.

Default: None.

Usage Guidelines: If the number of errored symbols within the detection period is greater than or equal to the high threshold, a critical link event is triggered, and the device notifies the peer by sending an Information OAMPDU with the Link Fault flag in the Flags field set to 1. The high threshold cannot be less than the low threshold.

Example: Set the high threshold for errored symbol period events on port 1/0/4 to none.

```
Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-symbol-period threshold
high none
```

3.11.17 ethernet-oam errored-symbol-period threshold low

Command: `ethernet-oam errored-symbol-period threshold low <low-symbols>`
`no ethernet-oam errored-symbol-period threshold low`

Function: Configures the low threshold for errored symbol period events. The **no** form of this command restores the default.

Parameters: <low-symbols>: The low threshold for errored symbol period events, from 1 to 18446744073709551615 symbols.

Command Mode: Port Mode.

Default: 1.

Usage Guidelines: If the number of errored symbols within the detection period is greater than or equal to the low threshold, an errored symbol period event is triggered, and the device notifies the peer by sending an Event Notification OAMPDU. The low threshold cannot be greater than the high threshold.

Example: Set the low threshold for errored symbol period events on port 1/0/4 to 5.

```
Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-symbol-period threshold
low 5
```

3.11.18 ethernet-oam errored-symbol-period window

Command: ethernet-oam errored-symbol-period window <seconds>
no ethernet-oam errored-symbol-period window

Function: Configures the detection period for errored symbol period events. The **no** form of this command restores the default.

Parameters: <seconds>: The period over which errored symbols are counted, from 5 to 300, in units of 200 ms.

Command Mode: Port Mode.

Default: 5.

Usage Guidelines: Errored symbols on the port are checked at the end of each detection period. If the number of errored symbols is greater than or equal to the threshold, the corresponding event is triggered and the device notifies the peer through an OAMPDU.

Example: Set the detection period for errored symbol period events on port 1/0/4 to 2 seconds.

```
Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-symbol-period window 10
```

3.11.19 ethernet-oam link-monitor

Command: ethernet-oam link-monitor
no ethernet-oam link-monitor

Function: Enables link monitoring. The **no** form of this command disables the function.

Parameters: None.

Command Mode: Port Mode.

Default: Enabled.

Usage Guidelines: Enables OAM to monitor local link errors. Link monitoring is normally enabled when OAM is enabled on the port. When OAM link monitoring is disabled, local link errors are not monitored, but Event Notification OAMPDUs from the peer are still received and processed normally.

Example: Enable link monitoring on port 1/0/4.

```
Switch(Config-If-Ethernet1/0/4)#ethernet-oam link-monitor
```

3.11.20 ethernet-oam mode

Command: ethernet-oam mode {active | passive}
no ethernet-oam mode

Function: Configures the OAM mode. The **no** form of this command restores the default.

Parameters: active: Active mode.

passive: Passive mode.

Command Mode: Port Mode.

Default: Active mode.

Usage Guidelines: At least one of the two connected OAM entities must be in active mode. After OAM is enabled, the OAM mode cannot be changed; to change it, disable OAM first.

Example: Set the OAM mode of ethernet 1/0/4 to passive.

```
Switch(Config-If-Ethernet1/0/4)#ethernet-oam mode passive
```

3.11.21 ethernet-oam period

Command: `ethernet-oam period <seconds>`
`no ethernet-oam mode`

Function: Configures the transmission period of Information OAMPDUs. The **no** form of this command restores the default.

Parameters: <seconds>: The transmission period, from 1 to 2 seconds.

Command Mode: Port Mode.

Default: 1 second.

Usage Guidelines: Use this command to configure the interval at which Information OAMPDUs are sent to maintain the OAM connection.

Example: Set the Information OAMPDU transmission interval of ethernet 1/0/4 to 2 seconds.

```
Switch(Config-If-Ethernet1/0/4)# ethernet-oam period 2
```

3.11.22 ethernet-oam remote-failure

Command: `ethernet-oam remote-failure`
`no ethernet-oam remote-failure`

Function: Enables OAM remote failure indication. The **no** form of this command disables the function.

Parameters: None.

Command Mode: Port Mode.

Default: Enabled.

Usage Guidelines: When remote failure indication is enabled and a critical event or link fault occurs locally, the device notifies the peer by sending an Information OAMPDU, logs the fault, and sends an SNMP trap. When remote failure indication is disabled, local critical events and link faults are not reported, but failure indications from the peer are still received and processed normally.

Example: Enable remote failure indication on ethernet 1/0/4.

```
Switch(Config-If-Ethernet1/0/4)#ethernet-oam remote-failure
```

3.11.23 ethernet-oam remote-loopback

Command: `ethernet-oam remote-loopback`
`no ethernet-oam remote-loopback`

Function: Sends a remote loopback request from the local OAM entity so that the remote end enters OAM loopback mode. The **no** form of this command disables remote loopback.

Parameters: None.

Command Mode: Port Mode.

Default: Disabled.

Usage Guidelines: Only OAM entities in active mode can initiate remote loopback requests; entities in passive mode cannot. When the remote OAM entity is in loopback mode, all packets except OAMPDUs are returned to the local port along their original paths (normal communication is not possible in OAM loopback mode), and network administrators can measure link delay, jitter, and throughput. Remote loopback is possible only after an OAM connection is established, and loopback is canceled automatically if the OAM connection is lost during the loopback. This command is mutually exclusive with the **ethernet-oam remote-loopback supported** command.

Example: Make the remote OAM entity of ethernet 1/0/4 enter remote loopback mode.

```
Switch(Config-If-Ethernet1/0/4)# ethernet-oam remote-loopback
```

```
Normal forwarding will be suspended during the remote-loopback, are you sure
to start remote-loopback? [Y/N]
```

3.11.24 ethernet-oam remote-loopback supported

Command: ethernet-oam remote-loopback supported
no ethernet-oam remote-loopback supported

Function: Enables OAM loopback support on the port. The **no** form of this command disables it.

Parameters: None.

Command Mode: Port Mode.

Default: Disabled.

Usage Guidelines: Only ports with remote loopback support enabled can accept OAM loopback requests and enter loopback mode. Therefore, make sure that loopback support is configured on the remote end before you put it into OAM loopback mode. This command is mutually exclusive with the **ethernet-oam remote-loopback** command.

Example: Enable OAM loopback support on ethernet 1/0/4.

```
Switch(Config-If-Ethernet1/0/4)#ethernet-oam remote-loopback supported
```

3.11.25 ethernet-oam timeout

Command: ethernet-oam timeout <seconds>
no ethernet-oam timeout

Function: Configures the OAM connection timeout. The **no** form of this command restores the default.

Parameters: <seconds>: The timeout, from 5 to 10 seconds.

Command Mode: Port Mode.

Default: 5 seconds.

Usage Guidelines: The OAM connection is disconnected if no OAMPDU is received within the specified timeout.

Example: Set the OAM connection timeout of ethernet 1/0/4 to 6 seconds.

```
Switch(Config-If-Ethernet1/0/4)#ethernet-oam timeout 6
```

3.11.26 show ethernet-oam

Command: show ethernet-oam [{local | remote} interface {ethernet |}
<IFNAME>]

Function: Displays the Ethernet OAM connections of the specified port or all ports.

Parameters: If no parameter is specified, overview information of all Ethernet OAM connections is displayed.

local: Displays detailed information about the local OAM connection.

remote: Displays detailed information about the remote OAM connection.

<IFNAME>: The port whose OAM connection information is displayed.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: None.

Example: Display overview information of Ethernet OAM connections.

```
Switch#show ethernet-oam
Remote-Capability codes: L - Link Monitor,  R - Remote Loopback
```

```
                      U - Unidirection,  V - Variable Retrieval
--------------------------------------------------------------------------------
-----------------------------------
Interface Local-Mode Local-Capability Remote-MAC-Addr Remote-Mode Remote-
Capability
1/0/1     active       L  R        0003.0f02.2e5d      active          L  R
1/0/2     active       L  R        0003.0f19.3a3e      avtive          L  R
1/0/4     active       L  R        0003.0f26.480c      passive         L  R
1/0/5     active       L  R        0003.0f28.020a      active          L  R
```

Field	Description
Interface	Port on which Ethernet OAM is enabled
Local-Mode	OAM working mode of the local port
Local-Capability	OAM functions supported by the local port L - Link Monitor, R - Remote Loopback U - Unidirection, V - Variable Retrieval
Remote-MAC-Addr	MAC address of the peer
Remote-Mode	OAM working mode of the peer
Remote-Capability	OAM functions supported by the peer L - Link Monitor, R - Remote Loopback U - Unidirection, V - Variable Retrieval

Display detailed information about the local OAM entity of ethernet 1/0/2.

```
Switch#show ethernet-oam local interface ethernet1/0/2
Ethernet1/0/2 oam local Information：
oam_status=enable
local _mode=active
period=1s
timeout=8s
Loopback Supported=YES
Unidirectional Support=YES
Link Events=YES
Remote Failure=YES
local_pdu=INFO
local_mux_action=FWD
local_par_action=DISCARD
Max_OAMPDU_Size=1518
--------------------------------------------------------------------------------
OAM_local_flags_field：
Link Fault=0     Dying Gasp=0    Critical Events=0
--------------------------------------------------------------------------------
Packet statistic：
Packets             Send              Receive
OAMPDU           553                21
Information          552                21
Event Notification     1                  0
Loopback Control     0                  0
--------------------------------------------------------------------------------
```

Field	Description
oam_status	Ethernet OAM status: enable: OAM is enabled. disable: OAM is disabled.
local _mode	Ethernet OAM working mode: active: The port is in active mode. passive: The port is in passive mode.
Period	Packet transmission period
Timeout	Connection timeout
local_pdu	How the local end processes Ethernet OAMPDUs: RX_INFO: The port only receives Information OAMPDUs and does not send any Ethernet OAMPDUs.

	LF_INFO: The port sends only Information OAMPDUs without Information TLVs and with the link error flag bits set. INFO: The port sends and receives only Information OAMPDUs. ANY: The port sends and receives all types of OAMPDUs.
local_mux_action	Operating mode of the local transmitter: FWD: The port can send any packets. DISCARD: The port sends only OAMPDUs and discards all other packets.
local_par_action	Operating mode of the local receiver: FWD: The port can receive any packets. DISCARD: The port receives only OAMPDUs and discards all other packets. LB: OAM remote loopback is enabled on the port. All packets received, except OAMPDUs, are returned to their sources along the paths on which they arrived.
Loopback Supported	Whether remote loopback is supported: YES or NO.
Unidirectional Support	Whether unidirectional transmission is supported: YES or NO.
Link Events	Whether general link events are supported: YES or NO.
Remote Failure	Whether critical link events (remote failure indication) are supported: YES or NO.
Link Fault	Whether a Link Fault event has occurred: 0 for no, 1 for yes.
Dying Gasp	Whether a Dying Gasp event has occurred: 0 for no, 1 for yes.
Critical Event	Whether a Critical Event has occurred: 0 for no, 1 for yes.
Max_OAMPDU_Size	The maximum supported OAMPDU length.
OAMPDU	The number of OAMPDUs sent and received (the sum of the three packet types below).
Information	The number of Information OAMPDUs sent and received.
Event Notification	The number of Event Notification OAMPDUs sent and received.
Loopback Control	The number of Loopback Control OAMPDUs sent and received.

Display detailed information about the remote OAM entity of Ethernet port 1/0/2.

```
Switch#show ethernet-oam remote interface ethernet1/0/2
Ethernet1/0/2 oam remote Information：
Remote_Mac_Address=0003.0f19.3a3e
local _mode=active
------------------------------------------------------------------------------
local_pdu=INFO
local_mux_action=FWD
local_par_action=DISCARD
Loopback Supported=YES
Unidirectional Support=NO
Link Events=YES
Remote Failure=YES
Max_OAMPDU_Size=1518
------------------------------------------------------------------------------
OAM Remote Flags Field：
Link Fault=0     Dying Gasp=0     Critical Event=0
```

Field	Description
Remote_Mac_Address	MAC address of the remote OAM entity
local _mode	Ethernet OAM working mode: active: The port is in active mode. passive: The port is in passive mode.
local_pdu	How the local end processes Ethernet OAMPDUs: RX_INFO: The port only receives Information OAMPDUs and does not send any Ethernet OAMPDUs.

	LF_INFO: The port sends only Information OAMPDUs without Information TLVs and with the link error flag bits set. INFO: The port sends and receives only Information OAMPDUs. ANY: The port sends and receives all types of OAMPDUs.
local_mux_action	Operating mode of the local transmitter: FWD: The port can send any packets. DISCARD: The port sends only OAMPDUs and discards all other packets.
local_par_action	Operating mode of the local receiver: FWD: The port can receive any packets. DISCARD: The port receives only OAMPDUs and discards all other packets. LB: OAM remote loopback is enabled on the port. All packets received, except OAMPDUs, are returned to their sources along the paths on which they arrived.
Loopback Supported	Whether remote loopback is supported: YES or NO.
Unidirectional Support	Whether unidirectional transmission is supported: YES or NO.
Link Events	Whether general link events are supported: YES or NO.
Remote Failure	Whether critical link events are supported: YES or NO.
Max_OAMPDU_Size	The maximum supported OAMPDU length.
Link Fault	Whether a Link Fault event has occurred: 0 for no, 1 for yes.
Dying Gasp	Whether a Dying Gasp event has occurred: 0 for no, 1 for yes.
Critical Event	Whether a Critical Event has occurred: 0 for no, 1 for yes.

3.11.27 show ethernet-oam events

Command: `show ethernet-oam events {local | remote} [interface {ethernet |} <IFNAME>]`

Function: Displays link event statistics, including general and critical link events, on the specified port or all ports with OAM enabled.

Parameters: local: Displays detailed information about local events.

remote: Displays detailed information about remote events.

<IFNAME>: The port whose OAM link event statistics are displayed. If this parameter is not specified, statistics for all ports are displayed.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: None.

Example: Display link event statistics of Ethernet port 1/0/1.

```
Switch#show ethernet-oam events local interface eth 1/0/1
ethernet1/0/1 link-events :
OAM_local_errored-symbol-period-events:
------------------------------------------------------------------------------
-------------------------
event time stamp : 3539                    errored symbol window(200ms) : 5
errored symbol low threshold : 1             errored symbol high threshold :
none
errored symbol : 1200120                  errored running total : 2302512542
event running total : 232
OAM_local_errored-frame-period-events:
------------------------------------------------------------------------------
-------------------------
event time stamp : 3539                     errored frame window(200ms) : 50
errored frame low threshold : 1               errored frame high threshold : none
```

```
errored frame : 1200120                    errored running total : 2302512542
event running total : 52
OAM_local_errored-frame-events:
------------------------------------------------------------------------------
------------------------
event time stamp : 3539                    errored frame window(200ms) : 5
errored frame low threshold : 1               errored frame high threshold :
none
errored frame : 1200120                     errored running total : 2302512542
event running total : 75
OAM_local_errored-frame-seconds-summary-events:
------------------------------------------------------------------------------
------------------------
event time stamp : 3520          errored frame seconds summary window(200ms) :
300
errored frame low threshold : 1               errored frame high threshold :
none
errored frame : 1200120                    errored running total : 2302512542
event running total : 232
OAM_local_link-fault : 0
OAM_local_dying gasp : 0
OAM_local_critical event : 0
```

Field	Description
OAM_local_errored-symbol-period-events	Statistics of local errored symbol period events
OAM_local_errored-frame-period-events	Statistics of local errored frame period events
OAM_local_errored-frame-events	Statistics of local errored frame events
OAM_local_errored-frame-seconds-summary-events	Statistics of local errored frame seconds events
event time stamp	Event timestamp
window	Detection period of the event
low threshold	Low detection threshold of the event
high threshold	High detection threshold of the event
errored frame	Number of errored frames
errored symbol	Number of errored symbols
errored running total	Total number of errors since OAM was reset
event running total	Total number of error events since OAM was reset
OAM_local_link-fault	Number of local link faults
OAM_local_dying gasp	Number of local dying gasp events
OAM_local_critical event	Number of local critical events

3.11.28 show ethernet-oam link-events-configuration

Command: `show ethernet-oam link-events-configuration [interface {ethernet | } <IFNAME>]`

Function: Displays the link event configuration, including detection periods and thresholds, of the specified port or all ports with OAM enabled.

Parameters: <IFNAME>: The port whose OAM link event configuration is displayed. If this parameter is not specified, the configuration of all ports is displayed.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: None.

Example: Display the link event configuration of ethernet 1/0/1.

```
Switch#show ethernet-oam link-events-configuration interface ethernet 1/0/1
Ethernet1/0/1 link-monitor configuration：
event                        high-threshold    low-threshold   window(200ms)
------------------------------------------------------------------------------
----------------------
Err-symbol-Period                  none           1            2
Err-frame-Period                   none           1           10
Err-frame                          none           2            5
Err-frame-second-summary          none           2          600
------------------------------------------------------------------------------
----------------------
```

Field	Description
Event	Event type
Err-symbol-Period	Errored symbol period event
Err-frame-Period	Errored frame period event
Err-frame	Errored frame event
Err-frame-second-summary	Errored frame seconds event
high-threshold	High threshold
low-threshold	Low threshold
window(200ms)	Detection period, in units of 200 ms

3.11.29 show ethernet-oam loopback-status

Command: `show ethernet-oam loopback status [interface {ethernet |} <IFNAME>]`

Function: Displays the OAM loopback status of the specified port or all ports.

Parameters: <IFNAME>: The port whose OAM loopback status is displayed. If this parameter is not specified, the status of all ports is displayed.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: None.

Example: Display the OAM loopback status of all ports.

```
Switch(config)#show ethernet-oam loopback status
OAM Loopback Status：
ethernet 1/0/1：disable
ethernet1/0/2：loopback_enable_waiting
ethernet1/0/3：loopback_disable_waiting
ethernet1/0/4：loopback_control
ethernet1/0/5：loopback_underControl
```

Field	Description
Disable	OAM loopback support is not enabled.
loopback_enable_waiting	The local side is the loopback controlling end; it has sent a remote loopback request and is waiting for confirmation.
loopback_disable_waiting	The local side is the loopback controlling end; it has sent a request to cancel remote loopback and is waiting for confirmation.
loopback_control	The local side is the loopback controlling end and loopback is in progress.
loopback_undercontrol	The local side is the loopback controlled end and loopback is in progress.
no_loopback	OAM loopback support is enabled, but no loopback request has been received.

3.12 Port Security

3.12.1 clear port-security

Command: clear port-security {all | configured | dynamic | sticky} [[address <mac-addr> | interface <interface-id>] [vlan <vlan-id>]]

Function: Clears secure MAC address entries on interfaces.

Parameters: all: All secure MAC address entries on the interfaces.

configured: Configured secure MAC addresses.

dynamic: Dynamic secure MAC addresses learned by the interface.

sticky: Sticky secure MAC addresses.

<mac-addr>: The specified secure MAC address.

<interface-id>: The secure MAC address entries of the specified interface.

<vlan-id>: The specified VLAN.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example: Clear all secure MAC addresses on the interfaces.

```
Switch#clear port-security all
```

3.12.2 show port-security

Command: show port-security [interface <interface-id>] [address]

Function: Displays the port security configuration.

Parameters: <interface-id>: Displays the port security configuration of the interface.

address: Displays the secure addresses of the interface.

Default: None.

Command Mode: All Modes.

Usage Guidelines: None.

Example: Display the secure MAC addresses of an interface.

```
Switch# show port-security address interface ethernet 1/0/1
```

3.12.3 switchport port-security

Command: switchport port-security
no switchport port-security

Function: Enables port security on the interface. The **no** form of this command disables port security.

Parameters: None.

Default: Disabled.

Command Mode: Port Mode.

Usage Guidelines: After port security is enabled on the interface, all dynamic MAC addresses are cleared, and all MAC addresses learned on the interface are marked FDB_TYPE_PORT_SECURITY_DYNAMIC. After port security is disabled on the interface, all secure MAC addresses are cleared or changed to dynamic MAC addresses.

Example: Enable port security on the interface.

```
Switch(config-if- ethernet1/0/1)#switchport port-security
```

3.12.4 switchport port-security aging

Command: switchport port-security aging {static | time <value> | type {absolute | inactivity}}
no switchport port-security violation aging {static | time | type}

Function: Enables aging of port security entries and specifies the aging time and type on the interface.

Parameters: static: Enables aging of static MAC addresses configured on the interface.

time <value>: The MAC address aging time of the interface, from 1 to 1440 minutes. The default is 0, which disables aging.

type: Specifies the aging type.

absolute: When the aging timer of the interface expires, all secure MAC addresses of the interface age out and are removed from the MAC address table.

inactivity: When the aging timer of the interface expires, entries without traffic age out; entries with traffic during the aging period are kept.

Default: Port security aging is disabled, and the aging time is 0.

The default aging type is absolute.

Static entries do not age by default.

Command Mode: Port Mode.

Usage Guidelines: None.

Example: Set the secure MAC address aging time on the interface to 1 minute.

```
Switch (config-if- ethernet1/0/1)# switchport port-security aging time 1
```

3.12.5 switchport port-security mac-address

Command: switchport port-security mac-address <mac-address> [vlan <vlan-id>]
no switchport port-security mac-address <mac-address> [vlan <vlan-id>]

Function: Configures a static secure MAC address on the interface. The **no** form of this command removes the configuration.

Parameters: <mac-address>: The MAC address to configure as a static secure MAC address.

<vlan-id>: The VLAN of the MAC address. This parameter takes effect only on trunk and hybrid interfaces.

Default: No secure MAC address is bound to the interface.

Command Mode: Port Mode.

Usage Guidelines: When configuring a static secure MAC address, check whether the number of secure MAC addresses would exceed the maximum allowed on the interface; exceeding the limit triggers the violation action.

Example: Configure a secure MAC address on the interface.

```
Switch (config-if- ethernet1/0/1)# switchport port-security mac-address 00-00-00-00-00-01
```

3.12.6 switchport port-security mac-address sticky

Command: switchport port-security mac-address sticky [mac-address] [vlan <vlan-id>]
no switchport port-security mac-address sticky [mac-address] [vlan <vlan-id>]

Function: Configures a sticky static secure MAC address on the interface. The **no** form of this command removes the configured secure MAC address.

Parameters: <mac-address>: The MAC address to configure as a sticky static secure MAC address.

<vlan-id>: The VLAN of the MAC address. This parameter takes effect only on trunk and hybrid interfaces.

Default: No sticky secure MAC address is bound to the interface.

Command Mode: Port Mode.

Usage Guidelines: When configuring a sticky static secure MAC address, check whether the number of secure MAC addresses would exceed the maximum allowed on the interface; exceeding the limit triggers the violation action.

Example: Configure a sticky secure MAC address on the interface.

```
Switch(config-if-ethernet1/0/1)#switchport port-security mac-address sticky
00-00-00-00-00-01
```

3.12.7 switchport port-security maximum

Command: switchport port-security maximum <value> [vlan <vlan-list>]
no switchport port-security maximum <value> [vlan <vlan-list>]

Function: Configures the maximum number of secure MAC addresses allowed on the interface. If VLANs are specified, the maximum applies to the specified VLANs. The **no** form of this command removes the configured maximum.

Parameters: <value>: The maximum number of secure MAC addresses allowed on the interface, from 1 to 128. The limit also depends on the maximum number of MAC addresses supported by the device.

<vlan-list>: The VLANs to which the maximum applies. This parameter takes effect only on trunk and hybrid interfaces.

Default: After port security is enabled, the maximum number of secure MAC addresses on the interface is 1 unless otherwise configured. There is no per-VLAN limit by default.

Command Mode: Port Mode.

Usage Guidelines: Note the relationship between the interface limit and the per-VLAN limits; the maximum configured for the interface takes precedence.

Example: Configure the maximum number of secure MAC addresses on the interface.

```
Switch(config-if- ethernet1/0/1)# switchport port-security maximum 100
```

3.12.8 switchport port-security violation

Command: switchport port-security violation {protect | recovery | restrict | shutdown}
no switchport port-security violation

Function: Configures the action taken when a port security violation occurs. A violation occurs when the number of MAC addresses exceeds the configured maximum, when a MAC address that belongs to another interface in the MAC address table accesses this interface, or when the same MAC

address is configured on several interfaces in the same VLAN. The **no** form of this command restores the default.

Parameters: protect: Protect mode. New MAC addresses are not learned and packets are dropped, but no warning is sent.

recovery: MAC address learning can be restored after the violation action is triggered on the port.

restrict: Restrict mode. New MAC addresses are not learned, packets are dropped, an SNMP trap is sent, and the event is logged in syslog.

shutdown: Shutdown mode, the default. The interface is disabled immediately, an SNMP trap is sent, and the event is logged in syslog.

Default: Shutdown.

Command Mode: Port Mode.

Usage Guidelines: None.

Example: Set the violation mode of the interface to protect.

```
Switch(config-if-ethernet1/0/1)#switchport port-security violation protect
```

3.13 VLAN

3.13.1 vlan

Command: `vlan WORD`
`no vlan WORD`

Function: Creates VLANs and enters VLAN Mode. If multiple VLANs are specified with ";" and "-", the VLANs are created only. If the VLAN already exists, the switch enters VLAN Mode; if it does not exist, the switch creates it and enters VLAN Mode. In VLAN Mode, you can set the VLAN name and assign switch ports to the VLAN. The **no** form of this command deletes the specified VLANs.

Parameters: WORD is the ID of the VLAN to create or delete, from 1 to 4094. Multiple IDs can be specified with ";" and "-".

Command Mode: Global Mode.

Default: Only VLAN 1 exists.

Usage Guidelines: VLAN 1 is the default VLAN and cannot be configured or deleted. The maximum VLAN ID is 4094. Dynamic VLANs learned through GVRP cannot be deleted with this command.

Example: Create VLAN 100 and enter VLAN Mode for VLAN 100.

```
Switch(config)#vlan 100
Switch(Config-Vlan100)#
```

3.13.2 vlan internal

Command: `vlan <2-4094> internal`

Function: Specifies the internal VLAN ID. A VLAN ID specified as the internal VLAN cannot be used by other VLANs. The internal VLAN is used only for loopback interfaces, and physical ports cannot be added to it. A new internal VLAN ID takes effect after the configuration is saved and the switch is restarted.

Parameters: <2-4094>: The VLAN ID used as the internal VLAN ID, from 2 to 4094.

Command Mode: Global Mode.

Default: 1006.

Usage Guidelines: The default internal VLAN ID is 1006. If the network uses VLAN 1006, change the internal VLAN ID. The internal VLAN ID must be an unused ID; otherwise, other VLANs are affected. This command takes effect after the configuration is saved and the switch is restarted.

Example: Set the internal VLAN ID to 100.

```
Switch(config)#vlan 100 internal
```

3.13.3 vlan ingress enable

Command: `vlan ingress enable`
`no vlan ingress enable`

Function: Enables VLAN ingress filtering on the port. The **no vlan ingress enable** command disables ingress filtering.

Command Mode: Port Mode.

Default: Enabled.

Usage Guidelines: When VLAN ingress filtering is enabled on the port, the system checks whether the receiving port is a member of the VLAN of the received data. If it is, the data is forwarded to the destination port; otherwise, the data is dropped.

Example: Disable VLAN ingress filtering on the port.

```
Switch(Config-If-Ethernet1/0/1)# no vlan ingress enable
```

3.13.4 switchport trunk native vlan

Command: `switchport trunk native vlan <vlan-id>`
`no switchport trunk native vlan`

Function: Sets the PVID of a trunk port. The **no switchport trunk native vlan** command restores the default.

Parameters: <vlan-id> is the PVID of the trunk port.

Command Mode: Port Mode.

Default: 1.

Usage Guidelines: The PVID is defined in 802.1Q. On a trunk port, the PVID is used to tag untagged frames: when an untagged frame enters a trunk port, the port tags it with the native VLAN PVID set with this command before VLAN forwarding.

Example: Set the native VLAN of a trunk port to 100.

```
Switch(config)#interface ethernet 1/0/5
Switch(Config-If-Ethernet1/0/5)#switchport mode trunk
Switch(Config-If-Ethernet1/0/5)#switchport trunk native vlan 100
Switch(Config-If-Ethernet1/0/5)#exit
```

3.13.5 switchport trunk allowed vlan

Command: `switchport trunk allowed vlan {WORD | all | add WORD | except WORD | remove WORD | none}`
`no switchport trunk allowed vlan`

Function: Sets the VLANs whose traffic is allowed on the trunk port. The **no switchport trunk allowed vlan** command restores the default.

Parameters: WORD: The specified VLAN IDs.

all: All VLAN IDs, from 1 to 4094.

add: Adds the specified VLAN IDs to the allowed VLAN list.

except: Adds all VLAN IDs except the specified ones to the allowed VLAN list.

remove: Removes the specified VLAN IDs from the allowed VLAN list.

none: Discards traffic of all VLANs.

Command Mode: Port Mode.

Default: Traffic of all VLANs is allowed.

Usage Guidelines: Use this command to set the VLANs whose traffic is allowed through the trunk port; traffic of other VLANs is blocked.

Example: Allow traffic of VLANs 1, 3, and 5-20 on the trunk port.

```
Switch(config)#interface ethernet 1/0/5
Switch(Config-If-Ethernet1/0/5)#switchport mode trunk
Switch(Config-If-Ethernet1/0/5)#switchport trunk allowed vlan 1;3;5-20
Switch(Config-If-Ethernet1/0/5)#exit
```

3.13.6 switchport mode trunk allow-null

Command: `switchport mode trunk allow-null`

Function: Sets a port to trunk mode without joining any VLAN. When GVRP is enabled, adding trunk ports to all VLANs is not appropriate, so we recommend configuring the port as a trunk port with this command before enabling GVRP on it. If the port is already a trunk port, this command clears its allowed VLAN list and removes it from all VLANs.

Parameters: None.

Command Mode: Port Mode.

Default: Access mode.

Usage Guidelines: Configures the port as a trunk port, removes it from all VLANs, and clears its allowed VLAN list.

Example: Set the port to trunk mode without joining any VLAN.

```
Switch(config-if-ethernet1/0/1)#switchport mode trunk allow-null
```

3.13.7 switchport mode

Command: `switchport mode {trunk | access | hybrid}`

Function: Sets the port to access, trunk, or hybrid mode.

Parameters: trunk: The port carries traffic of multiple VLANs. **access**: The port belongs to only one VLAN. **hybrid**: The port carries traffic of multiple VLANs in tagged or untagged mode.

Command Mode: Port Mode.

Default: Access mode.

Usage Guidelines: Ports in trunk mode are called trunk ports. Trunk ports carry traffic of multiple VLANs and interconnect VLANs on different switches. Ports in access mode are called access ports; an access port can belong to only one VLAN at a time. Hybrid ports carry traffic of multiple VLANs, receive and send packets of multiple VLANs, and can connect to switches or user computers. Hybrid and trunk ports process received data in the same way but send data differently: hybrid ports can send packets of multiple VLANs untagged, whereas trunk ports can send only packets of the default VLAN untagged. A port cannot be changed directly between hybrid and trunk; first set it to access, and then set it to hybrid or trunk. When the trunk or hybrid attribute is removed, the port returns to the default (access) attribute and belongs to VLAN 1.

Example: Set port 1/0/5 to trunk mode, port 1/0/8 to access mode, and port 1/0/10 to hybrid mode.

```
Switch(config)#interface ethernet 1/0/5
Switch(Config-If-Ethernet1/0/5)#switchport mode trunk
Switch(Config-If-Ethernet1/0/5)#exit
Switch(config)#interface ethernet 1/0/8
Switch(Config-If-Ethernet1/0/8)#switchport mode access
Switch(Config-If-Ethernet1/0/8)#exit
Switch(config)#interface ethernet 1/0/10
Switch(Config-If-Ethernet1/0/10)#switchport mode hybrid
Switch(Config-If-Ethernet1/0/10)#exit
```

3.13.8 switchport interface

Command: switchport interface [ethernet | portchannel] [<interface-name | interface-list>]
no switchport interface [ethernet | portchannel] [<interface-name | interface-list>]

Function: Adds Ethernet ports to the VLAN. The **no** form of this command removes one or more ports from the specified VLAN.

Parameters: ethernet specifies that the ports to add are Ethernet ports. **portchannel** specifies that the ports to add are port channels. **interface-name** is the port name, such as e1/0/1; if a port name is used, **ethernet** or **portchannel** is not required. **interface-list** is the list of ports to add or remove; ";" and "-" are supported, for example, ethernet1/0/1;3;4-7;8.

Command Mode: VLAN Mode.

Default: A newly created VLAN contains no ports.

Usage Guidelines: Access ports are normal ports that can join a VLAN, but a port can join only one VLAN at a time.

Example: Add Ethernet ports 1/0/1, 1/0/3, 1/0/4-7, and 1/0/8 to VLAN 100.

```
Switch(Config-Vlan100)#switchport interface ethernet 1/0/1;3;4-7;8
```

3.13.9 switchport hybrid native vlan

Command: switchport hybrid native vlan <vlan-id>
no switchport hybrid native vlan

Function: Sets the PVID of a hybrid port. The **no switchport hybrid native vlan** command restores the default.

Parameters: <vlan-id> is the PVID of the hybrid port.

Command Mode: Port Mode.

Default: 1.

Usage Guidelines: When an untagged frame enters a hybrid port, it is tagged with the native PVID set with this command and forwarded in the native VLAN.

Example: Set the native VLAN of a hybrid port to 100.

```
Switch(config)#interface ethernet 1/0/5
Switch(Config-If-Ethernet1/0/5)#switchport mode hybrid
Switch(Config-If-Ethernet1/0/5)#switchport hybrid native vlan 100
Switch(Config-If-Ethernet1/0/5)#exit
```

3.13.10 switchport hybrid allowed vlan

Command: switchport hybrid allowed vlan {WORD | all | add WORD | except WORD | remove WORD | none} {tag | untag}
no switchport hybrid allowed vlan

Function: Sets the VLANs allowed on a hybrid port and whether their traffic is tagged or untagged. The **no switchport hybrid allowed vlan** command restores the default.

Parameters: WORD: Sets the allowed VLAN list; a later configuration overwrites the previous one.

all: Allows all VLANs.

add WORD: Adds the VLAN list to the existing allowed VLAN list.

except WORD: Allows all VLANs except the specified VLAN list.

remove WORD: Removes the specified VLANs from the existing allowed VLAN list.

none: Discards traffic of all VLANs.

tag: Joins the specified VLANs in tagged mode.

untag: Joins the specified VLANs in untagged mode.

Command Mode: Port Mode.

Default: Traffic of all VLANs is denied.

Usage Guidelines: Use this command to set the VLANs whose traffic is allowed through the hybrid port; traffic of other VLANs is blocked. In untagged mode, frames of the VLAN are sent from the hybrid port without a VLAN tag; in tagged mode, they are sent with the corresponding VLAN tag. A hybrid port cannot allow the same VLAN in both tagged and untagged mode. If a VLAN allowed in tagged (or untagged) mode is reconfigured as untagged (or tagged), the latest configuration takes effect.

Example: Allow VLANs 1, 3, and 5-20 in untagged mode and VLANs 100, 300, and 500-2000 in tagged mode on a hybrid port.

```
Switch(config)#interface ethernet 1/0/5
Switch(Config-If-Ethernet1/0/5)#switchport mode hybrid
Switch(Config-If-Ethernet1/0/5)#switchport hybrid allowed vlan 1;3;5-20 untag
Switch(Config-If-Ethernet1/0/5)#switchport hybrid allowed vlan 100;300;500-
2000 tag
Switch(Config-If-Ethernet1/0/5)#exit
```

3.13.11 switchport forbidden vlan

Command: `switchport forbidden vlan {WORD | all | add WORD | except WORD | remove WORD}`
`no switchport forbidden vlan`

Function: Configures forbidden VLANs for a port. This command can be used only on trunk or hybrid ports on which GVRP is not enabled. The **no** form of this command clears the forbidden VLAN list of the port.

Parameters: WORD: Sets the VLAN list as forbidden VLANs, overwriting the previous configuration.

all: Sets all VLANs as forbidden VLANs.

add WORD: Adds the VLAN list to the current forbidden VLAN list.

except WORD: Sets all VLANs except the VLAN list as forbidden VLANs.

remove WORD: Removes the specified VLANs from the current forbidden VLAN list.

Command Mode: Port Mode.

Default: The forbidden VLAN list is empty.

Usage Guidelines: Marks the corresponding VLANs as forbidden and clears them from the port's allowed VLAN list. If the port has joined these VLANs statically, it leaves them, and the switch notifies the GVRP module so that the port's corresponding registrar state machines enter forbidden mode.

Example: Make the port leave all VLANs and put the corresponding GVRP registrar state machines into forbidden mode.

```
Switch(config-if-ethernet1/0/1)#switchport forbidden vlan all
```

3.13.12 switchport access vlan

Command: `switchport access vlan <vlan-id>`
`no switchport access vlan`

Function: Adds the current access port to the specified VLAN. The **no switchport access vlan** command removes the port from the specified VLAN and returns it to VLAN 1.

Parameters: <vlan-id> is the ID of the VLAN to which the port is added, from 1 to 4094.

Command Mode: Port Mode.

Default: All ports belong to VLAN 1.

Usage Guidelines: Only ports in access mode can join a specified VLAN, and an access port can join only one VLAN at a time.

Example: Add an access port to VLAN 100.

```
Switch(config)#interface ethernet 1/0/8
Switch(Config-If-Ethernet1/0/8)#switchport mode access
Switch(Config-If-Ethernet1/0/8)#switchport access vlan 100
Switch(Config-If-Ethernet1/0/8)#exit
```

3.13.13 show vlan

Command: show vlan [brief | summary] [id <vlan-id>] [name <vlan-name>] [internal usage [id <vlan-id> | name <vlan-name>]] [private-vlan [id <vlan-id> | name <vlan-name>]]

Function: Displays detailed information about all VLANs or the specified VLAN.

Parameters: brief displays brief information; **summary** displays VLAN statistics; **<vlan-id>** is the ID of the VLAN whose status is displayed, from 1 to 4094; **<vlan-name>** is the name of the VLAN whose status is displayed, from 1 to 11 characters; **private-vlan** displays private VLAN information, including the ID, name, associated VLANs, and ports.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: If neither **<vlan-id>** nor **<vlan-name>** is specified, information about all VLANs on the switch is displayed.

Example: Display the status of the current VLANs and VLAN statistics.

```
Switch#show vlan
VLAN Name         Type      Media      Ports
---- ------------ ---------- ---------
----------------------------------------
1    default        Static     ENET     Ethernet1/0/1   Ethernet1/0/2
                                       Ethernet1/0/3   Ethernet1/0/4
                                       Ethernet1/0/9   Ethernet1/0/10
                                       Ethernet1/0/11   Ethernet1/0/12
2    VLAN0002     Static     ENET     Ethernet1/0/5     Ethernet1/0/6
                                       Ethernet1/0/7      Ethernet1/0/8
Switch#show vlan summary
The max. vlan entrys: 4094
Existing Vlans:
Universal Vlan:
1 12 13 15 16 22
Total Existing Vlans is:6
```

Field	Description
VLAN	VLAN ID
Name	VLAN name
Type	VLAN type: statically configured or dynamically learned
Media	VLAN interface type: Ethernet
Ports	Access ports in the VLAN

```
Switch(config)#show vlan private-vlan
VLAN Name     Type  Asso  VLAN  Ports
---- ------------ ---------- ---------
----------------------------------------
100  VLAN0100  Primary  101   102    Ethernet1/0/9     Ethernet1/0/10
                                      Ethernet1/0/11
    Ethernet1/0/12
                                      Ethernet1/0/13
101  VLAN0101  Community 100        Ethernet1/0/9     Ethernet1/0/10
```

```
                                    Ethernet1/0/11     Ethernet1/0/12
                                    Ethernet1/0/13
102  VLAN0102  Isolate  100         Ethernet1/0/9
```

3.13.14 private-vlan association

Command: `private-vlan association <secondary-vlan-list>`
`no private-vlan association`

Function: Configures a private VLAN association. The **no** form of this command removes the private VLAN association.

Parameters: <secondary-vlan-list>: The list of secondary VLANs associated with the primary VLAN. Secondary VLANs are of two types: isolated VLANs and community VLANs. Multiple secondary VLANs can be specified, separated by ";".

Command Mode: VLAN Mode.

Default: No private VLAN association is configured.

Usage Guidelines: This command can be used only for private VLANs. Ports in secondary VLANs associated with a primary VLAN can communicate with ports in the primary VLAN.

Before you configure a private VLAN association, the three types of private VLANs must have no member ports. A private VLAN that has an association cannot be deleted. When a private VLAN association is removed, all member ports of the private VLANs in the association are removed from those VLANs.

Example: Associate isolated VLAN 200 and community VLAN 300 with primary VLAN 100.

```
Switch(Config-Vlan100)#private-vlan association 200;300
```

3.13.15 private-vlan

Command: `private-vlan {primary | isolated | community}`
`no private-vlan`

Function: Configures the current VLAN as a private VLAN. The **no** form of this command removes the private VLAN configuration.

Parameters: primary sets the current VLAN as a primary VLAN; **isolated** sets it as an isolated VLAN; **community** sets it as a community VLAN.

Command Mode: VLAN Mode.

Default: No private VLAN is configured.

Usage Guidelines: There are three types of private VLANs: **primary**, **isolated**, and **community**. Ports in a primary VLAN can communicate with ports in the isolated and community VLANs associated with it. Ports in an isolated VLAN are isolated from one another and can communicate only with ports in the associated primary VLAN. Ports in a community VLAN can communicate with one another and with ports in the associated primary VLAN. Ports in a community VLAN cannot communicate with ports in an isolated VLAN.

Only VLANs without Ethernet ports can be set as private VLANs, and only private VLANs with a configured association can have access Ethernet ports as members. When a normal VLAN is set as a private VLAN, its Ethernet ports are removed.

Note that private VLAN information is not propagated by GVRP.

Example: Set VLANs 100, 200, and 300 as primary, isolated, and community private VLANs, respectively.

```
Switch(config)#vlan 100
Switch(Config-Vlan100)#private-vlan primary
Note:This will remove all the ports from vlan 100
Switch(Config-Vlan100)#exit
```

```
Switch(config)#vlan 200
Switch(Config-Vlan200)#private-vlan isolated
Note:This will remove all the ports from vlan 200
Switch(Config-Vlan200)#exit
Switch(config)#vlan 300
Switch(Config-Vlan300)#private-vlan community
Note:This will remove all the ports from vlan 300
Switch(Config-Vlan300)#exit
```

3.13.16 name

Command: `name <vlan-name>`
`no name`

Function: Specifies a descriptive name for the VLAN. The **no** form of this command deletes the VLAN name.

Parameters: <vlan-name> is the name string.

Command Mode: VLAN Mode.

Default: The default VLAN name is VLANxxx, where xxx is the VLAN ID.

Usage Guidelines: Naming VLANs makes them easier to identify and manage.

Example: Set the name of VLAN 100 to TestVlan.

```
Switch(Config-Vlan100)#name TestVlan
```

3.13.17 vlan-flow-statistics

Command: `vlan-flow-statistics`
`no vlan-flow-statistics`

Function: Enables statistics of packets sent and received in the VLAN. The **no** form of this command disables this function.

Parameters: None.

Command Mode: VLAN Interface Mode.

Default: Disabled.

Usage Guidelines: None.

Example: Enable VLAN-based traffic statistics on VLAN 1.

Output of **show interface vlan** before **vlan-flow-statistics** is configured:

```
Switch#show int vlan 1
Vlan1 is up(0), line protocol is down, dev index is 11001
  Device flag 0x1002(BROADCAST MULTICAST)
  Time since last status change:0w-0d-0h-54m-59s  (3299 seconds)
  IPv4 address is:
    (NULL)
  VRF Bind: Not Bind
  Hardware is EtherSVI, address is 00-07-0a-0a-0a-1a
  MTU is 1500 bytes , BW is 0 Kbit
  Encapsulation ARPA, loopback not set
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  The last 5 second input rate 0 bits/sec, 0 packets/sec
  The last 5 second output rate 0 bits/sec, 0 packets/sec
```

Output of **show interface vlan** after **vlan-flow-statistics** is configured:

```
Switch(config)#int vlan 1
Switch(config-if-vlan1)#vlan-flow-statistics
Switch(config-if-vlan1)#end
Switch#show interface vlan 1
```

```
Vlan1 is up(0), line protocol is down, dev index is 11001
  Device flag 0x1002(BROADCAST MULTICAST)
  Time since last status change:0w-0d-0h-55m-54s  (3354 seconds)
  IPv4 address is:
    (NULL)
  VRF Bind: Not Bind
  Hardware is EtherSVI, address is 00-07-0a-0a-0a-1a
  MTU is 1500 bytes , BW is 0 Kbit
  Encapsulation ARPA, loopback not set
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  The last 5 second input rate 0 bits/sec, 0 packets/sec
  The last 5 second output rate 0 bits/sec, 0 packets/sec
  Input packets statistics:
    Input queue 0/1200, 0 drops
    0 packets input, 0 bytes, 0 no buffer
    0 unicast packets, 0 multicast packets, 0 broadcast packets
    0 input errors, 0 CRC, 0 oversize, 0 undersize
     0 jabber, 0 fragments
  Output packets statistics:
    0 packets output, 0 bytes, 0 underruns
    0 unicast packets, 0 multicast packets, 0 broadcast packets
    0 output errors, 0 collisions
```

3.14 GVRP

3.14.1 garp timer join

Command: `garp timer join <200-500>`

Function: Sets the GARP join timer. The join timer must be less than half of the leave timer.

Parameters: <200-500>: The timer value in milliseconds.

Command Mode: Global Mode.

Default: 200 ms.

Usage Guidelines: The switch checks whether the value is within the range. If it is, the GARP timer is set to the specified value; otherwise, a configuration error is returned.

Example: Set the GARP join timer to 200 ms.

```
Switch(config)#garp timer join 200
```

3.14.2 garp timer leave

Command: `garp timer leave <500-1200>`

Function: Sets the GARP leave timer. The leave timer must be at least twice the join timer and less than the leaveAll timer.

Parameters: <500-1200>: The timer value in milliseconds.

Command Mode: Global Mode.

Default: 600 ms.

Usage Guidelines: The switch checks whether the value is within the range. If it is, the GARP timer is set to the specified value; otherwise, a configuration error is returned.

Example: Set the GARP leave timer to 600 ms.

```
Switch(config)#garp timer leave 600
```

3.14.3 garp timer leaveAll

Command: `garp timer leaveall <5000-60000>`

Function: Sets the GARP leaveAll timer. The leaveAll timer must be greater than the leave timer.

Parameters: <5000-60000>: The timer value in milliseconds.

Command Mode: Global Mode.

Default: 10000 ms.

Usage Guidelines: The switch checks whether the value is within the range. If it is, the GARP leaveAll timer is set to the specified value; otherwise, a configuration error is returned.

Example: Set the GARP leaveAll timer to 20000 ms.

```
Switch(config)#garp timer leaveall 20000
```

3.14.4 gvrp (Global)

Command: `gvrp`
`no gvrp`

Function: Enables or disables GVRP globally.

Parameters: None.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: GVRP must be enabled globally for the GVRP module to work.

Example: Enable GVRP globally.

```
Switch(config)#gvrp
```

3.14.5 gvrp (Port)

Command: `gvrp`
`no gvrp`

Function: Enables or disables GVRP on the port. Note: GVRP can be enabled on a port when it is not enabled globally, but it does not take effect until GVRP is enabled globally.

Parameters: None.

Command Mode: Port Mode.

Default: Disabled.

Usage Guidelines: GVRP can be enabled only on trunk and hybrid ports; enabling it on an access port returns an error. After GVRP is enabled on a port, the port is added to GVRP (that is, the corresponding state machines are added for the port).

Example: Enable GVRP on the port.

```
Switch(config-if-ethernet1/0/1)#gvrp
```

3.14.6 no garp timer

Command: `no garp timer (join | leave | leaveall)`

Function: Restores the GARP join, leave, or leaveAll timer to its default value.

Parameters: join: The join timer.

leave: The leave timer.

leaveall: The leaveAll timer.

Command Mode: Global Mode.

Default: 200, 600, and 10000 milliseconds for the join, leave, and leaveAll timers, respectively.

Usage Guidelines: The switch checks whether the default value is within the valid range. If it is, the GARP join, leave, or leaveAll timer is restored to its default; otherwise, a configuration error is returned.

Example: Restore a GARP timer to its default value.

```
Switch(config)#no garp timer leaveall
```

3.14.7 show garp timer

Command: show garp timer (join | leave | leaveall |)

Function: Displays the value of each timer. The value shown is the initial value of the timer, not the remaining time.

Parameters: join: The join timer.

leave: The leave timer.

leaveall: The leaveAll timer.

Command Mode: Admin Mode.

Default: 200, 600, and 10000 milliseconds for the join, leave, and leaveAll timers, respectively.

Usage Guidelines: Displays the value of the specified timer.

Example: Display the value of the GARP join timer.

```
Switch#show garp timer join
Garp join timer’s value is 200(ms)
```

3.14.8 show gvrp fsm information

Command: show gvrp fsm information interface (ethernet | port-channel) IFNAME

Function: Displays the current state of all registrar and applicant state machines on the specified port.

Parameters: ethernet: A physical port.

port-channel: A port channel.

IFNAME: The port name.

Command Mode: Admin Mode.

Default: MT for registrar state machines and VO for applicant state machines.

Usage Guidelines: Displays the state of all registrar and applicant state machines.

Example: Display the state of all state machines.

```
Switch#show gvrp fsm information interface ethernet 1/0/1
```

VA: Very anxious Active member; AA: Anxious Active member; QA: Quiet Active member

VP: Very anxious Passive member; AP: Anxious Passive member; QP: Quiet Passive member

VO: Very anxious Observer; AO: Anxious Observer; QO: Quiet Observer

LA: Leaving Active member; LO: Leaving Observer

```
Interface ethernet 1/0/1 gvrp fsm information:
Index  VLANID       Applicant         Registrar
----   ------------        ----------          ---------
1      100             VO               LV
2      300             VP               IN
```

3.14.9 show gvrp leaveAll fsm information

Command: show gvrp leaveall fsm information interface (ethernet | port-channel) IFNAME

Function: Displays the state of the leaveAll state machine on the specified port.

Parameters: ethernet: A physical port.

port-channel: A port channel.

IFNAME: The port name.

Command Mode: Admin Mode.

Default: Passive.

Usage Guidelines: Displays the state of the leaveAll state machine.

Example: Display the state of the leaveAll state machine on a port.

```
Switch#show gvrp leaveall fsm information interface ethernet 1/0/1
Interface     leaveAll fsm
----------    ------------
Ethernet1/0/1    passive
```

3.14.10 show gvrp leavetimer running information

Command: show gvrp leavetimer running information (vlan <1-4094> |) interface (Ethernet | port-channel |) IFNAME

Function: Displays the running status of all leave timers on the specified port.

Parameters: <1-4094>: The VLAN ID.

Ethernet: A physical port.

port-channel: A port channel.

IFNAME: The port name.

Command Mode: Admin Mode.

Default: Leave timers are not running.

Usage Guidelines: Displays the running state and expiration time of each leave timer.

Example: Display the running state and expiration time of each leave timer on the port.

```
Switch#show gvrp leavetimer running information interface ethernet 1/0/1
VLANID     running state     expired time
------------     ----------        ---------
100            UP            0.2 s
300          DOWN          non
```

3.14.11 show gvrp port-member

Command: show gvrp (active|) port-member

Function: Displays all ports on which GVRP is enabled. **active** displays only ports in the active state.

Parameters: active: Displays ports in the active state.

Command Mode: Admin Mode.

Default: GVRP is disabled on ports.

Usage Guidelines: Displays all GVRP-enabled ports recorded in GVRP.

Example: Display all ports on which GVRP is enabled.

```
Switch#show gvrp port-member
Ports which were enabled gvrp included:
Ethernet1/0/3 (T)     Ethernet1/0/4 (T)
Ethernet1/0/5 (T)     Ethernet1/0/6 (T)
```

```
Ethernet1/0/7 (T)     Ethernet1/0/8 (T)
Ethernet1/0/9 (T)     Ethernet1/0/10 (T)
```

3.14.12 show gvrp port registerd vlan

Command: show gvrp port (dynamic | static |) registerd vlan interface (Ethernet | port-channel |) IFNAME

Function: Displays the VLANs registered dynamically or statically on the specified port.

Parameters: dynamic: Dynamic registration.

static: Static registration.

Ethernet: A physical port.

port-channel: A port channel.

IFNAME: The port name.

Command Mode: Admin Mode.

Default: No VLANs are registered dynamically or statically on the port.

Usage Guidelines: Displays the VLANs of the registrar state machines registered dynamically or statically.

Example: Display all VLANs registered dynamically or statically on the port.

```
Switch#show gvrp port registerd vlan interface ethernet 1/0/1
Current port dynamic registerd vlan included：
Vlan10    vlan20
Vlan40    vlan60
Current port static registerd vlan included：
Vlan10    vlan30
Vlan40    vlan200
```

3.14.13 show gvrp timer running information

Command: show gvrp timer (join | leaveall) running information interface (ethernet | port-channel |) IFNAME

Function: Displays the running status of the join or leaveAll timers on the specified port.

Parameters: join: The join timer.

leaveall: The leaveAll timer.

ethernet: A physical port.

port-channel: A port channel.

IFNAME: The port name.

Command Mode: Admin Mode.

Default: The join timer is not running and the leaveAll timer is running.

Usage Guidelines: Displays the running state of the join or leaveAll timer on the port.

Example: Display the running state and expiration time of the join timer.

```
Switch(config)#show gvrp timer join running information interface ethernet
1/0/1
Current port’s jointimer running state is: UP
Current port’s jointimer expired time is: 0.2 s
```

3.14.14 show gvrp vlan registerd port

Command: show gvrp vlan <1-4094> registerd port

Function: Displays the ports on which the specified VLAN is registered.

Parameters: <1-4094>: The VLAN ID.

Command Mode: Admin Mode.

Default: The specified VLAN is not registered on any port.

Usage Guidelines: None.

Example: Display all ports on which VLAN 100 is registered.

```
Switch#show gvrp vlan 100 registerd port
Ethernet1/0/3 (T)     Ethernet1/0/4 (T)
Ethernet1/0/5 (T)     Ethernet1/0/6 (T)
Ethernet1/0/7 (T)     Ethernet1/0/8 (T)
Ethernet1/0/9 (T)     Ethernet1/0/10 (T)
```

3.14.15 debug gvrp event

Command: debug gvrp event interface (ethernet | port-channel |) IFNAME
no debug gvrp event interface (ethernet | port-channel |) IFNAME

Function: Enables or disables GVRP event debugging, including state machine transitions and timer expirations.

Parameters: ethernet: A physical port.

port-channel: A port channel.

IFNAME: The port name.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: Use this command to enable GVRP event debugging.

Example: Display GVRP event debugging information.

```
Switch#debug gvrp event interface ethernet 1/0/1
%Jan 16 02:25:14 2006 GVRP EVENT:  LO -> VO , interface ethernet 1/0/1, vlan
100
%Jan 16 02:35:15 2006 GVRP EVENT:  join timer expire, interface ethernet
1/0/1
```

3.14.16 debug gvrp packet

Command: debug gvrp packet (receive | send) interface (ethernet | port-channel |) IFNAME
no debug gvrp packet (receive | send) interface (ethernet | port-channel |) IFNAME

Function: Enables or disables GVRP packet debugging.

Parameters: receive: Enables debugging of received GVRP packets.

send: Enables debugging of sent GVRP packets.

ethernet: A physical port.

port-channel: A port channel.

IFNAME: The port name.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: Use this command to enable GVRP packet debugging.

Example: Display information about GVRP packets received.

```
Switch#debug gvrp packet receive interface ethernet 1/0/1
Receive packet, smac 00-21-27-aa-0f-46, dmac 01-80-C2-00-00-21,
      length 90, protocol ID:1,attribute type:0x01,
```

```
      Attribute Index   Length     Event      Value
--------------------     ---------     -------      -------
    1              10        joinIn       100
    2              10        joinEmpty   140
    3              10        leaveIn      150
          4              10        leaveEmpty   180
```

3.15 Dot1q-tunnel

3.15.1 dot1q-tunnel enable

Command: `dot1q-tunnel enable`
`no dot1q-tunnel enable`

Function: Sets an access port of the switch to dot1q-tunnel (QinQ) mode. The **no** form of this command restores the default.

Parameters: None.

Command Mode: Port Mode.

Default: Disabled.

Usage Guidelines: After dot1q-tunnel is enabled on the port, untagged packets entering the port are tagged, and tagged packets are given an outer tag. The TPID of the added tag is 0x8100, and its VLAN ID is the VLAN to which the port belongs. Double-tagged packets are forwarded based on the MAC address and the outer tag until the outer tag is removed when they leave through an access port. Because adding an outer tag can make packets oversized, we recommend using this command together with the jumbo frame function. This command is normally used on access ports. It is mutually exclusive with the **dot1q-tunnel tpid** and **vlan-translation enable** commands.

Example: Add port 1/0/1 to VLAN 3 and enable dot1q-tunnel on it.

```
Switch(config)#vlan 3
Switch(Config-Vlan3)#switchport interface ethernet 1/0/1
Switch(Config-Vlan3)#exit
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)# dot1q-tunnel enable
Switch(Config-If-Ethernet1/0/1)# exit
Switch(config)#
```

3.15.2 dot1q-tunnel tpid

Command: `dot1q-tunnel tpid {0x8100|0x9100|0x9200| <1-65535> }`

Function: Configures the protocol type (TPID) of a trunk port of the switch.

Parameters: 0x8100 | 0x9100 | 0x9200 | <1-65535>: The TPID value.

Command Mode: Port Mode.

Default: 0x8100.

Usage Guidelines: This function facilitates interworking with equipment from other vendors. If the device connected to the switch trunk port sends packets with a TPID of 0x9100, set the port TPID to 0x9100 so that the switch receives and processes the packets normally. This command and the **dot1q-tunnel enable** command are mutually exclusive.

Example: Set port 1/0/10 as a trunk port and set its TPID to 0x9100.

```
Switch(config)#interface ethernet 1/0/10
Switch(Config-If-Ethernet1/0/10)#switchport mode trunk
Switch(Config-If-Ethernet1/0/10)#dot1q-tunnel tpid 0x9100
Switch(Config-If-Ethernet1/0/10)#exit
Switch(config)#
```

3.15.3 show dot1q-tunnel

Command: `show dot1q-tunnel`

Function: Displays information about all ports in dot1q-tunnel state.

Parameters: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Use this command to display information about ports in dot1q-tunnel state.

Example: Display the current dot1q-tunnel state.

```
Switch#show dot1q-tunnel
Interface Ethernet1/0/1:
dot1q-tunnel is enable
Interface Ethernet1/0/3:
dot1q-tunnel is enable
```

3.16 VLAN translation

3.16.1 vlan-translation

Command: `vlan-translation <old-vlan-id> to <new-vlan-id>{in | out}`
`no vlan-translation <old-vlan-id>{in | out}`

Function: Adds a VLAN translation entry that maps an original VLAN ID to a new VLAN ID. The **no** form of this command deletes the mapping.

Parameters: <old-vlan-id> is the original VLAN ID; **<new-vlan-id>** is the translated VLAN ID; **in** specifies ingress translation; **out** specifies egress translation.

Command Mode: Port Mode.

Default: No VLAN translation entry is configured.

Usage Guidelines: Configures the ingress and egress translation entries of the VLAN translation function. Packets are matched against the configured entries; when an entry matches, the VLAN ID is changed to the VLAN ID in the entry. If no entry matches, forwarding is determined by the **vlan-translation miss drop** command.

Access ports do not support this function.

Example: Translate VLAN 100 traffic entering port 1/0/1 to VLAN 2 at ingress.

```
Switch#config
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#vlan-translation enable
Switch(Config-If-Ethernet1/0/1)#vlan-translation 100 to 2 in
Switch(Config-If-Ethernet1/0/1)#exit
Switch(config)#
```

3.16.2 vlan-translation enable

Command: `vlan-translation enable`
`no vlan-translation enable`

Function: Enables VLAN translation on the port. The **no** form of this command restores the default.

Parameters: None.

Command Mode: Port Mode.

Default: Disabled.

Usage Guidelines: This command and dot1q-tunnel are mutually exclusive.

Access ports do not support this function.

Example: Enable VLAN translation on port 1/0/1.

```
Switch#config
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#vlan-translation enable
```

3.16.3 vlan-translation cvid

Command: `vlan-translation cvid < 1-4094> svid <1-4094> {pri < 0-7>}`
`no vlan-translation cvid < 1-4094> svid <1-4094>`

Function: Adds a VLAN translation entry that maps a customer VLAN ID (CVID) to a service VLAN ID (SVID). The **no** form of this command deletes the mapping.

Parameters:

<1-4094>: The VLAN ID.

<0-7>: The packet priority after VLAN translation.

Command Mode: Port Mode.

Default: Disabled.

Usage Guidelines: Configures the ingress and egress translation entries of the VLAN translation function. For ingress traffic that matches the CVID of an entry, the VLAN ID is changed to the SVID; for egress traffic that matches the SVID, the VLAN ID is changed to the CVID. If no entry matches, forwarding is determined by the **vlan-translation miss drop** command.

Access ports do not support this function.

Example: Translate VLAN 100 traffic entering the port to VLAN 200 at ingress, and translate VLAN 200 traffic to VLAN 100 at egress.

```
Switch#config
Switch(config)#interface ethernet 1/1/1
Switch(Config-If-Ethernet1/1/1)#vlan-translation enable
Switch(Config-If-Ethernet1/1/1)# vlan-translation cvid 100 svid 200
Switch(Config-If-Ethernet1/1/1)#exit
Switch(config)#
```

3.16.4 vlan-translation miss drop

Command: `vlan-translation miss drop in`
`no vlan-translation miss drop in`

Function: Drops packets that do not match any VLAN translation entry. The **no** form of this command restores the default.

Parameters: in specifies the ingress direction.

Command Mode: Port Mode.

Default: Packets that do not match any VLAN translation entry are not dropped.

Usage Guidelines: By default, packets that do not match any configured VLAN translation entry are not dropped. After this command is configured, tagged packets that do not match are dropped. This command has no effect on untagged packets.

Access ports do not support this function.

Example: Drop ingress packets on port 1/0/1 that fail VLAN translation.

```
Switch(Config-If-Ethernet1/0/1)#vlan-translation miss drop in
```

3.16.5 show vlan-translation

Command: `show vlan-translation`

Function: Displays the VLAN translation configuration.

Parameters: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays the VLAN translation configuration.

Access ports do not support this function.

Example: Display the VLAN translation configuration.

```
Switch#show vlan-translation
Interface Ethernet1/0/1:
    vlan-translation is enable, miss drop is not set
    vlan-translation 5 to 10 in
```

3.17 Dynamic VLAN

3.17.1 dynamic-vlan mac-vlan prefer

Command: `dynamic-vlan mac-vlan prefer`

Function: Gives MAC-based VLANs the highest priority.

Parameters: None.

Command Mode: Global Mode.

Default: MAC-based VLANs have the highest priority.

Usage Guidelines: Configures the dynamic VLAN priority on the switch. By default, when several dynamic VLAN types apply, the priority order is MAC-based VLAN, IP subnet-based VLAN, and then protocol-based VLAN. If IP subnet-based VLANs have been given priority, use this command to give MAC-based VLANs priority again.

Example: Give MAC-based VLANs priority.

```
Switch#config
Switch(config)#dynamic-vlan mac-vlan prefer
```

3.17.2 dynamic-vlan subnet-vlan prefer

Command: `dynamic-vlan subnet-vlan prefer`

Function: Gives IP subnet-based VLANs the highest priority.

Parameters: None.

Command Mode: Global Mode.

Default: MAC-based VLANs have the highest priority.

Usage Guidelines: Configures the dynamic VLAN priority on the switch. By default, when several dynamic VLAN types apply, the priority order is MAC-based VLAN, IP subnet-based VLAN, and then protocol-based VLAN. Use this command to give IP subnet-based VLANs priority.

Example: Give IP subnet-based VLANs priority.

```
Switch#config
Switch(config)#dynamic-vlan subnet-vlan prefer
```

3.17.3 mac-vlan

Command: `mac-vlan mac <mac-addrss> <mac-mask> vlan <vlan-id> priority <priority-id>`

`no mac-vlan {mac <mac-addrss> <mac-mask>|all}`

Function: Maps a MAC address to a VLAN so that the specified MAC address joins the specified VLAN. The **no** form of this command deletes the specified mapping or all mappings.

Parameters: <mac-addrss> is the MAC address in the format XX-XX-XX-XX-XX-XX. **<mac-mask>** is the MAC address mask in the format XX-XX-XX-XX-XX-XX. **<vlan-id>** is the VLAN ID, from 1 to 4094. **<priority-id>** is the priority used in the VLAN tag, from 0 to 7. **all** specifies all MAC addresses.

Command Mode: Global Mode.

Default: No MAC address is mapped to a VLAN.

Usage Guidelines: Use this command to add the specified MAC address to the specified VLAN. When an untagged packet from the specified MAC address enters a switch port, it is assigned the specified VLAN ID and placed in that VLAN, regardless of the port through which it enters. The command does not affect tagged packets.

Example: Add the network device with MAC address 00-03-0f-11-22-33 to VLAN 100.

```
Switch#config
Switch(config)#mac-vlan mac 00-03-0f-11-22-33 ff-ff-ff-ff-ff-ff vlan 100
priority 0
```

3.17.4 mac-vlan vlan

Command: mac-vlan vlan <vlan-id>
no mac-vlan vlan <vlan-id>

Function: Configures the specified VLAN as a MAC VLAN. The **no mac-vlan vlan <vlan-id>** command removes the MAC VLAN configuration of the VLAN.

Parameters: <vlan-id> is the VLAN ID.

Command Mode: Global Mode.

Default: No MAC VLAN is configured.

Usage Guidelines: Configures the specified VLAN as a MAC VLAN.

Example: Configure VLAN 100 as a MAC VLAN.

```
Switch#config
Switch(config)#mac-vlan vlan 100
```

3.17.5 protocol-vlan

Command: protocol-vlan mode {ethernetii etype <etype-id> | llc {dsap <dsap-id> ssap <ssap-id>} | snap etype <etype-id>} vlan <vlan-id> priority <priority-id>
no protocol-vlan {mode {ethernetii etype <etype-id> | llc {dsap <dsap-id> ssap <ssap-id>} | snap etype <etype-id>} | all}

Function: Maps a protocol to a VLAN so that packets of the specified protocol join the specified VLAN. The **no** form of this command deletes the specified mapping or all mappings.

Parameters: mode is the encapsulation type: **ethernetii** (Ethernet II), **llc** (LLC), or **snap** (SNAP). **<etype-id>** is the protocol type of the packet, from 1536 to 65535. **<dsap-id>** is the destination service access point, from 0 to 255. **<ssap-id>** is the source service access point, from 0 to 255. **<vlan-id>** is the VLAN ID, from 1 to 4094. **<priority-id>** is the priority, from 0 to 7. **all** specifies all encapsulation protocols.

Command Mode: Global Mode.

Default: No protocol is mapped to a VLAN.

Usage Guidelines: This command adds the specified protocol to the specified VLAN. When an untagged packet of the specified protocol enters a switch port, it is assigned the specified VLAN ID and placed in that VLAN, regardless of the port through which it enters. The command does not affect tagged packets. We recommend configuring the ARP protocol together with the IP protocol; otherwise, some applications may be affected.

Example: Assign IP packets with Ethernet II encapsulation to VLAN 200.

```
Switch#config
Switch(config)#protocol-vlan mode ethernetii etype 2048 vlan 200
```

3.17.6 show dynamic-vlan prefer

Command: `show dynamic-vlan prefer`

Function: Displays the dynamic VLAN priority.

Parameters: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the dynamic VLAN priority.

Example: Display the dynamic VLAN priority.

Example: Display current dynamic VLAN preference.

```
Switch#show dynamic-vlan prefer
Mac Vlan/Voice Vlan
IP Subnet Vlan
Protocol Vlan
```

3.17.7 show mac-vlan

Command: `show mac-vlan`

Function: Displays the MAC-based VLAN configuration of the switch.

Parameters: None.

Command Mode: Admin Mode and Other Configuration Modes.

Usage Guidelines: Displays the MAC-based VLAN configuration of the switch.

Example: Display the current MAC-based VLAN configuration.

```
Switch#show mac-vlan
MAC-Address                    VLAN_ID   Priority
------------------                      -----------     --------
00-e0-4c-77-ab-9d                   2          2
00-0a-eb-26-8d-f3                   2          2
00-03-0f-11-22-33                      5          5
```

3.17.8 show mac-vlan interface

Command: `show mac-vlan interface`

Function: Displays the ports on which MAC-based VLAN is enabled.

Parameters: None.

Command Mode: Admin Mode and Other Configuration Modes.

Usage Guidelines: Displays the ports on which MAC-based VLAN is enabled. The letter in parentheses indicates the port mode: A for access port, T for trunk port, and H for hybrid port.

Example: Display the ports on which MAC-based VLAN is currently enabled.

```
Switch#show mac-vlan interface
Ethernet1/0/1(A)         Ethernet1/0/2(A)
Ethernet1/0/3(A)         Ethernet1/0/4(A)
Ethernet1/0/5(H)         Ethernet1/0/6(T)
```

3.17.9 show protocol-vlan

Command: `show portocol-vlan`

Function: Displays the protocol-based VLAN configuration of the switch.

Parameters: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the protocol-based VLAN configuration of the switch.

Example: Display the current protocol-based VLAN configuration.

```
Switch#show protocol-vlan
Protocol_Type                 VLAN_ID          Priority
------------------                          -------------          ---------
mode ethernetii etype 0x800             200             4
mode ethernetii etype 0x860             200             4
mode snap etype 0xabc                   100             5
mode llc dsap 0xac ssap 0xbd                100             5
```

3.17.10 show subnet-vlan

Command: show subnet-vlan

Function: Displays the IP subnet-based VLAN configuration of the switch.

Parameters: None.

Command Mode: Admin Mode and Other Configuration Modes.

Usage Guidelines: Displays the IP subnet-based VLAN configuration of the switch.

Example: Display the current IP subnet-based VLAN configuration.

```
Switch#show subnet-vlan
IP-Address              Mask              VLAN_ID
------------------            -------                 -------
192.168.1.165           255.255.255.0           2
202.200.121.21          255.255.0.0             2
10.0.0.1                 255.248.0.0             5
```

3.17.11 show subnet-vlan interface

Command: show subnet-vlan interface

Function: Displays the ports on which IP subnet-based VLAN is enabled.

Parameters: None.

Command Mode: Admin Mode and Other Configuration Modes.

Usage Guidelines: Displays the ports on which IP subnet-based VLAN is enabled. The letter in parentheses indicates the port mode: A for access port, T for trunk port, and H for hybrid port.

Example: Display the ports on which IP subnet-based VLAN is currently enabled.

```
Switch#show subnet-vlan interface
Ethernet1/0/1(A)          Ethernet1/0/2(A)
Ethernet1/0/3(A)          Ethernet1/0/4(A)
Ethernet1/0/5(H)          Ethernet1/0/6(T)
```

3.17.12 subnet-vlan

Command: subnet-vlan ip-address <ipv4-addrss> mask <subnet-mask> vlan <vlan-id> priority <priority-id>
no subnet-vlan {ip-address <ipv4-addrss> mask <subnet-mask> | all}

Function: Maps an IP subnet to a VLAN so that the specified IP subnet joins the specified VLAN. The **no** form of this command deletes the specified mapping or all mappings.

Parameters: <ipv4-addrss> is the IPv4 address in dotted decimal notation; each octet ranges from 0 to 255. **<subnet-mask>** is the subnet mask in dotted decimal notation; each octet ranges from 0 to 255. **<priority-id>** is the priority used in the VLAN tag, from 0 to 7. **<vlan-id>** is the VLAN ID, from 1 to 4094. **all** specifies all subnets.

Command Mode: Global Mode.

Default: No IP subnet is mapped to a VLAN.

Usage Guidelines: Use this command to add the specified IP subnet to the specified VLAN. When an untagged packet from the specified IP subnet enters a switch port, it is assigned the specified VLAN ID and placed in that VLAN, regardless of the port through which it enters. This command does not affect tagged packets.

Example: Add network devices in IP subnet 192.168.1.0/24 to VLAN 300.

```
Switch#config
Switch(config)#subnet-vlan ip-address 192.168.1.1 mask 255.255.255.0 vlan 300
priority 0
```

3.17.13 switchport mac-vlan enable

Command: `switchport mac-vlan enable`
`no switchport mac-vlan enable`

Function: Enables MAC-based VLAN on the port. The **no** form of this command disables MAC-based VLAN on the port.

Parameters: None.

Command Mode: Port Mode.

Default: Enabled.

Usage Guidelines: After a MAC address is added to a VLAN, MAC-based VLAN is enabled globally. Use this command to disable MAC-based VLAN on specific ports for special applications.

Example: Disable MAC-based VLAN on port 1/0/1.

```
Switch#config
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#no switchport mac-vlan enable
```

3.17.14 switchport subnet-vlan enable

Command: `switchport subnet-vlan enable`
`no switchport subnet-vlan enable`

Function: Enables IP subnet-based VLAN on the port. The **no** form of this command disables IP subnet-based VLAN on the port.

Parameters: None.

Command Mode: Port Mode.

Default: Enabled.

Usage Guidelines: After an IP subnet is added to a VLAN, IP subnet-based VLAN is enabled globally. Use this command to disable IP subnet-based VLAN on specific ports for special applications.

Example: Disable IP subnet-based VLAN on port 1/0/1.

```
Switch#config
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#no switchport subnet-vlan enable
```

3.18 Voice VLAN

3.18.1 show voice-vlan

Command: show voice-vlan

Function: Displays the voice VLAN configuration of the switch.

Parameters: None.

Command Mode: Admin Mode and Other Configuration Modes.

Usage Guidelines: Displays the voice VLAN configuration.

Example: Display the current voice VLAN configuration.

```
Switch#show voice-vlan
Voice VLAN ID:2
Ports:ethernet1/0/1;ethernet1/0/3
Voice name       MAC-Address              Mask     Priority
------------ -----    ----------------------          -----       --------
financePhone   00-e0-4c-77-ab-9d            0xff          5
manager       00-0a-eb-26-8d-f3            0xfe         6
Mr_Lee        00-03-0f-11-22-33            0x80         5
NULL          00-03-0f-11-22-33            0x0          5
```

3.18.2 switchport voice-vlan enable

Command: switchport voice-vlan enable
no switchport voice-vlan enable

Function: Enables voice VLAN on the port. The **no** form of this command disables voice VLAN on the port.

Parameters: None.

Command Mode: Port Mode.

Default: Enabled.

Usage Guidelines: When voice equipment is added to the voice VLAN, voice VLAN is enabled globally by default. Use this command to disable voice VLAN on specific ports for special applications.

Example: Disable voice VLAN on port 1/0/3.

```
Switch#config
Switch(config)#interface ethernet1/0/3
switch(Config-If-Ethernet1/0/3)#no switchport voice-vlan enable
```

3.18.3 voice-vlan

Command: voice-vlan mac <mac-address> mask <mac-mask> priority <priority-id> [name <voice-name>]
no voice-vlan {mac <mac-address> mask <mac-mask> | name <voice-name> | all}

Function: Adds specified voice equipment to the voice VLAN. The **no** form of this command removes the equipment from the voice VLAN.

Parameters: <mac-address> is the MAC address of the voice equipment, in the format xx-xx-xx-xx-xx-xx. **<mac-mask>** is the last eight bits of the MAC address mask; valid values are 0xff, 0xfe, 0xfc, 0xf8, 0xf0, 0xe0, 0xc0, 0x80, and 0x0. **<priority-id>** is the priority of the voice traffic, from 0 to 7. **<voice-name>** is the name of the voice equipment, used to simplify equipment management. **all** specifies the MAC addresses of all voice equipment.

Command Mode: Global Mode.

Usage Guidelines: This command adds the specified voice equipment to the voice VLAN. When an untagged packet from the specified voice equipment enters a switch port, it belongs to the voice VLAN regardless of the port through which it enters. The command does not affect tagged packets.

Example: Add the 256 voice devices of the R&D department, with MAC addresses from 00-03-0f-11-22-00 to 00-03-0f-11-22-ff, to the voice VLAN.

```
Switch#config
Switch(config)#voice-vlan vlan 100
Switch(config)#voice-vlan mac 00-03-0f-11-22-00 mask 0 priority 5 name test
```

3.18.4 voice-vlan vlan

Command: `voice-vlan vlan <vlan-id>`
`no voice-vlan`

Function: Configures the specified VLAN as the voice VLAN. The **no voice-vlan** command removes the voice VLAN configuration.

Parameters: <vlan-id> is the VLAN ID.

Command Mode: Global Mode.

Default: No voice VLAN is configured.

Usage Guidelines: Configures the specified VLAN as the voice VLAN. Only one voice VLAN can exist at a time. The voice VLAN cannot be used together with MAC-based VLAN.

Example: Configure VLAN 100 as the voice VLAN.

```
Switch#config
Switch(config)#voice-vlan vlan 100
```

3.19 Multi-to-One VLAN Translation

3.19.1 vlan-translation n-to-1

Command: `vlan-translation n-to-1 <WORD> to <new-vlan-id>`
`no vlan-translation n-to-1 <WORD>`

Function: Enables or disables Multi-to-One VLAN translation on the port.

Parameters: <WORD> is the original VLAN IDs, from 1 to 4094, separated with ";" and "-". If two VLAN ranges on the same port are translated to different VLAN IDs, the ranges must not overlap.

<new-vlan-id> is the translated VLAN ID, from 1 to 4094.

Command Mode: Port Mode.

Default: Disabled.

Usage Guidelines: Multi-to-One VLAN translation is used at the network edge to map multiple VLANs to one VLAN of the backbone network. When traffic returns from the backbone network to the edge, the original edge VLAN is restored. This saves VLAN resources in the backbone network. Note: Before using this function, create both the original and the translated VLANs, and add both the downlink port on which this function is enabled and the uplink port connected to the backbone network to the original and translated VLANs in tagged mode. This function cannot be used together with dot1q-tunnel or VLAN translation.

Note: Multi-to-One VLAN translation takes effect only after MAC addresses are learned.

Access ports do not support this function.

Example: On Ethernet port 1/0/1, translate traffic from VLANs 1 to 5 to VLAN 100, and translate traffic of VLANs 1 to 5 leaving VLAN 100 back to the corresponding VLAN IDs. The uplink port to the backbone network is Ethernet 1/0/5.

```
Switch(config)#vlan 1-5;100
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)# switchport mode trunk
Switch(Config-If-Ethernet1/0/1)# vlan-translation n-to-1 1-5 to 100
Switch(config)#interface ethernet 1/0/5
Switch(Config-If-Ethernet1/0/5)# switchport mode trunk
```

3.19.2 show vlan-translation n-to-1

Command: `show vlan-translation n-to-1 [<interface-name>]`

Function: Displays the Multi-to-One VLAN translation configuration of ports.

Parameters: <interface-name>: The name of the port to display. If no port is specified, all ports with this function configured are displayed.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Access ports do not support this function.

Example: Display all ports configured with Multi-to-One VLAN translation.

```
Switch# show vlan-translation n-to-1
Interface Ethernet1/0/1:
vlan-translation n-to-1 enable, vlan 1-4 to 100
vlan-translation n-to-1 enable,vlan 5-8;13 to 101
Interface Ethernet1/0/2:
vlan-translation n-to-1 enable,vlan 1-4 to 100
```

3.20 Super VLAN

3.20.1 supervlan

Command: `supervlan`
`no supervlan`

Function: Configures the VLAN as a super VLAN. The **no** form of this command restores the default.

Parameters: None.

Command Mode: VLAN Mode.

Default: Not configured.

Usage Guidelines: Configures a VLAN (other than a sub VLAN) as a super VLAN. A super VLAN is automatically filtered when trunk ports are configured, and no port can belong to it.

Example: Configure VLAN 2 as a super VLAN.

```
Swithc#config
Switch(config)#vlan 2
Switch (config-vlan2)#supervlan
```

3.20.2 subvlan

Command: `subvlan WORD`
`no subvlan {WORD | all}`

Function: Configures VLANs as sub VLANs. The **no** form of this command restores the default.

Parameters: WORD: The VLAN IDs, separated with "-" and ";".

all: All sub VLANs.

Command Mode: VLAN Mode.

Default: Not configured.

Usage Guidelines: Configures VLANs as sub VLANs. Each VLAN must exist and must be a common VLAN that is neither a super VLAN nor a sub VLAN of another super VLAN. Each super VLAN can be mapped to up to 127 sub VLANs, and the switch supports up to 1024 super VLANs.

Example: Configure VLAN 3 as a sub VLAN.

```
Swithc#config
Switch(config)#vlan 2-3
Switch(config)#vlan 2
Switch (config-vlan2)#supervlan
Switch (config-vlan2)#subvlan 3
```

3.20.3 arp-proxy subvlan

Command: `arp-proxy subvlan {WORD | all}`
`no arp-proxy subvlan {WORD | all}`

Function: Enables ARP proxy for sub VLANs so that traffic received in a sub VLAN can be forwarded to other sub VLANs. The **no** form of this command restores the default.

Parameters: WORD: The VLAN IDs, separated with "-" and ";".

all: All sub VLANs.

Command Mode: Interface Mode.

Default: Not configured.

Usage Guidelines: The VLAN interface must be the interface of a super VLAN. Traffic received in a sub VLAN can then be forwarded to other sub VLANs: when the switch receives an ARP request from the VLAN, it replies with its own MAC address so that the switch forwards the traffic.

Example: Enable ARP proxy for all sub VLANs on VLAN 2.

```
Swithc#config
Switch(config)#interface vlan 2
Switch (config-if-vlan2)#arp-proxy subvlan all
```

3.20.4 ip-addr-range subvlan

Command: `ip-addr-range subvlan <vlan-id> <ipv4-address> to <ipv4-address>`
`no ip-addr-range subvlan <vlan-id>`

Function: Configures an IP address range for a sub VLAN. When the switch receives traffic and needs to send an ARP request, it checks whether the destination IP address of the packet is within the range; if not, it does not send the ARP request. The **no** form of this command restores the default.

Parameters: <vlan-id>: The VLAN ID, from 1 to 4094.

<ipv4-address>: An IPv4 address in dotted decimal notation; each octet ranges from 0 to 255.

Command Mode: Interface Mode.

Default: No address range is configured.

Usage Guidelines: When the switch receives traffic from a sub VLAN with an address range and needs to send an ARP request, it checks whether the destination IP address of the packet is within the range; if not, it does not send the ARP request.

Example: Configure the address range of sub VLAN 3.

```
Swithc#config
```

```
Switch(config)#interface vlan 2
Switch (config-if-vlan2)#ip-addr-range subvlan 3 1.1.1.1 to 1.1.1.10
```

3.20.5 ip-addr-range

Command: `ip-addr-range <ipv4-address> to <ipv4-address>`
`no ip-addr-range`

Function: Configures an IP address range for an interface. When the switch receives traffic and needs to send an ARP request, it checks whether the destination IP address of the packet is within the range; if not, it does not send the ARP request. The **no** form of this command restores the default.

Parameters: <ipv4-address>: An IPv4 address in dotted decimal notation; each octet ranges from 0 to 255.

Command Mode: Interface Mode.

Default: No address range is configured.

Usage Guidelines: When the switch receives traffic on an interface with an address range and needs to send an ARP request, it checks whether the destination IP address of the packet is within the range; if not, it does not send the ARP request. If the interface is a super VLAN interface and receives an ARP request for an IP address outside the range, it does not forward the ARP request.

Example: Configure the address range of interface VLAN 2.

```
Swithc#config
Switch(config)#interface vlan 2
Switch (config-if-vlan2)#ip-addr-range 1.1.1.1 to 1.1.1.10
```

3.20.6 show supervlan

Command: `show supervlan [<vlan-id>]`

Function: Displays the super VLAN configuration.

Parameters: <vlan-id>: The VLAN ID, from 1 to 4094.

Command Mode: Admin Mode.

Usage Guidelines: If no VLAN ID is specified, all super VLAN configurations are displayed.

Example: Display the current super VLAN configuration.

```
Swithc#show supervlan
VLAN Name        Type       sub VLAN  Ports
---- ------------ ---------- ---------
---------------------------------------
2    VLAN0002     Universal   3     Ethernet1/0/2
                              4     Ethernet1/0/3
```

3.21 MAC Address Table

3.21.1 clear collision-mac-address-table

Command: `clear collision-mac-address-table`

Function: Clears the hash collision MAC address table.

Parameters: None.

Command Mode: Admin Mode.

Usage Guidelines: If the hash collision MAC address function that installs entries in the FFP (**mac-address-table avoid-collision**) is enabled, the MAC addresses cannot be cleared.

Example: Clear the hash collision MAC address table.

```
Switch#clear collision-mac-address-table
```

3.21.2 clear mac-address-table dynamic

Command: clear mac-address-table dynamic [address <mac-addr>] [vlan <vlan-id>] [interface [ethernet | portchannel] <interface-name>]

Function: Clears dynamic entries from the MAC address table.

Parameters: <mac-addr>: The MAC address to delete. **<interface-name>**: The port that forwards packets for the MAC address. **<vlan-id>**: The VLAN ID.

Command Mode: Admin Mode.

Usage Guidelines: Deletes all dynamic entries in the MAC address table, except application and system entries. MAC address entries are classified by source into the following types: DYNAMIC, STATIC, APPLICATION, and SYSTEM. DYNAMIC entries are learned by the switch and can be aged out automatically.

Example: Delete all dynamic MAC addresses.

```
Switch#clear mac-address-table dynamic
```

3.21.3 mac-address-learning cpu-control

Command: mac-address-learning cpu-control
no mac-address-learning cpu-control

Function: Enables CPU-controlled MAC address learning. The **no** form of this command restores automatic MAC address learning by the chip.

Parameters: None.

Command Mode: Global Mode.

Default: The chip learns MAC addresses automatically.

Usage Guidelines: Before enabling port security, private VLAN, MAC notification, MAC address limiting, or similar functions, enable CPU-controlled MAC address learning.

Example: Enable CPU-controlled MAC address learning.

```
Switch(Config)#mac-address-learning cpu-control
```

3.21.4 mac-address-table aging-time

Command: mac-address-table aging-time <0 | aging-time>
no mac-address-table aging-time

Function: Sets the aging time of dynamic entries in the MAC address table.

Parameters: <aging-time> is the aging time in seconds, from 10 to 1000000. **0** disables aging.

Command Mode: Global Mode.

Default: 300 seconds.

Usage Guidelines: If no packet with a destination address matching an address entry is received within the aging time, the entry ages out. Set the aging time according to network conditions; the default value is usually appropriate.

Example: Set the aging time to 600 seconds.

```
Switch(config)#mac-address-table aging-time 600
```

3.21.5 mac-address-table static | static-multicast | blackhole

Command: mac-address-table {static | static-multicast | blackhole} address <mac-addr> vlan <vlan-id> [interface [ethernet | portchannel] <interface-name>] | [source | destination | both]
no mac-address-table {static | static-multicast | blackhole | dynamic} [address <mac-addr>] [vlan <vlan-id>] [interface [ethernet | portchannel] <interface-name>]

Function: Adds or modifies static address entries, static multicast entries, and filter (blackhole) address entries. The **no** form of this command deletes these entries.

Parameters: static: Static entries. **static-multicast**: Static multicast entries. **blackhole**: Filter entries, which discard frames from or to a specific MAC address; filtering can be based on the source address, destination address, or both. Filter entries are not port-based and cannot be configured on an interface. **dynamic**: Dynamic address entries. **<mac-addr>**: The MAC address to add or delete. **<interface-name>**: The name of the port that forwards packets for the MAC address. **<vlan-id>**: The VLAN ID. **source**: Filters based on the source address. **destination**: Filters based on the destination address. **both**: Filters based on both the source and destination addresses (default).

Command Mode: Global Mode.

Default: When a VLAN interface is configured and up, the system generates a static address entry that maps the interface's own MAC address to the VLAN ID.

Usage Guidelines: In certain special applications, or when the switch cannot learn a MAC address dynamically, use this command to manually map a MAC address to a port and VLAN.

The **no mac-address-table** command deletes all dynamic, static, and filter MAC address entries in the switch MAC address table, except application and system entries. MAC address entries are classified by source into the following types: DYNAMIC, STATIC, APPLICATION, and SYSTEM. DYNAMIC entries are learned by the switch and can be aged out automatically. STATIC entries (including blackhole entries) are added by users. APPLICATION entries are static entries added by application protocols (such as 802.1X and port security). SYSTEM entries are static entries added for VLAN interfaces. A STATIC entry can overwrite a conflicting DYNAMIC entry, but not APPLICATION or SYSTEM entries.

After a static multicast MAC address is configured with this command, traffic to that multicast MAC address is forwarded to the specified port of the specified VLAN.

Example: Port 1/0/1 belongs to VLAN 200; map MAC address 00-03-0f-f0-00-18 to it.

```
Switch(config)#mac-address-table static address 00-03-0f-f0-00-18 vlan 200
interface ethernet 1/0/1
```

Configure static multicast MAC address 01-00-5e-00-00-01 with egress port ethernet 1/0/1.

```
Switch(config)#mac-address-table static-multicast address 01-00-5e-00-00-01
vlan 1 interface ethernet1/0/1
```

3.21.6 show collision-mac-address-table

Command: show collision-mac-address-table

Function: Displays the hash collision MAC address table.

Parameters: None.

Command Mode: Global Mode.

Usage Guidelines: If the hash collision MAC address function that installs entries in the FFP (**mac-address-table avoid-collision**) is enabled, collision MAC addresses installed in the FFP are marked with an asterisk (*).

Example: Display the hash collision MAC address table.

```
Switch(Config)#show collision-mac-address-table
```

```
The max number can be recorded is 200
The max number of collision is 0
The current number recorded is 0
 MAC Address        VLAN  Collision-count
```

3.21.7 show mac-address-table

Command: show mac-address-table [static | blackhole | multicast | aging-time <aging-time> | count] [address <mac-addr>] [vlan <vlan-id>] [count] [interface <interface-name>]

Function: Displays the current MAC address table.

Parameters: static: Static entries. **blackhole**: Filter entries. **aging-time <aging-time>**: The address aging time. **count**: The number of entries. **multicast**: Multicast entries. **<mac-addr>**: The MAC address of the entry. **<vlan-id>**: The VLAN ID of the entry. **<interface-name>**: The interface name of the entry.

Command Mode: Admin Mode and Configuration Mode.

Default: None.

Usage Guidelines: This command displays various types of MAC address entries. You can also use **show mac-address-table** to display all MAC address entries.

Example: Display all filter MAC address entries.

```
Switch#show mac-address-table blackhole
```

3.22 MAC Notification

3.22.1 clear mac-notification statistics

Command: clear mac-notification statistics

Function: Clears MAC notification trap statistics.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: After executing this command, you can check the result with the corresponding show command.

Example:

```
Switch# clear mac-notification statistics
```

3.22.2 mac-address-table notification

Command: mac-address-table notification
no mac-address-table notification

Function: Enables MAC address notification globally. The **no** form of this command disables global MAC address notification.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: This command works together with the SNMP trap setting. When MAC address notification is disabled, other settings can still be displayed but have no effect.

Example: Enable MAC address notification.

```
Switch(Config)#mac-address-table notification
```

3.22.3 mac-address-table notification history-size

Command: `mac-address-table notification history-size <0-500>`
`no mac-address-table notification history-size`

Function: Configures the maximum history size for storing MAC address change messages. The **no** form of this command restores the default.

Parameters: history-size: The amount of notification data stored, from 1 to 500.

Default: 10.

Command Mode: Global Mode.

Usage Guidelines: This command can be configured even when the global MAC notification function is disabled.

Example: Set the maximum history size to 256.

```
Switch(Config)#mac-address-table notification history-size 256
```

3.22.4 mac-address-table notification interval

Command: `mac-address-table notification interval <0-86400>`
`no mac-address-table notification interval`

Function: Configures the interval for sending MAC address notifications. The **no** form of this command restores the default interval.

Parameters: interval: The notification interval in seconds, from 0 to 86400.

Default: 30 seconds.

Command Mode: Global Mode.

Usage Guidelines: This command can be configured even when the global MAC notification function is disabled.

Example: Set the MAC address notification interval to 30 seconds.

```
Switch(Config)#mac-address-table notification interval 30
```

3.22.5 mac-notification

Command: `mac-notification {added | both | removed}`
`no mac-notification`

Function: Configures MAC address notification on the specified port. The **no** form of this command disables the function.

Parameters: added: Notifies when MAC addresses are added.

removed: Notifies when MAC addresses are removed.

both: Notifies when MAC addresses are added or removed.

Default: MAC address notification is not configured.

Command Mode: Port Mode.

Usage Guidelines: This command can be configured even when the global MAC notification function is disabled.

Example: Send a trap notification when a MAC address is added on Ethernet port 1/0/5.

```
Switch(Config)#in ethernet 1/0/5
Switch(Config-if-ethernet 1/0/5)#mac-notification added
```

3.22.6 show mac-notification summary

Command: `show mac-notification summary`

Function: Displays the MAC notification configuration and notification packet statistics.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Use this command to check the MAC notification configuration and the status of MAC notification traps sent.

Example:

```
Switch#show mac-notification summary
MAC address notification:enabled
MAC address snmp traps:enabled
MAC address notification interval = 10
MAC address notification history log size = 120
MAC address added = 0
MAC address removed = 0
MAC address snmp traps generated = 0
```

3.22.7 snmp-server enable traps mac-notification

Command: `snmp-server enable traps mac-notification`
`no snmp-server enable traps mac-notification`

Function: Enables MAC address notification traps globally. The **no** form of this command disables the traps.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: This command works together with the MAC notification setting. When MAC notification is disabled, other settings can still be displayed but have no effect.

Example: Enable MAC address notification traps.

```
Switch(Config)#snmp-server enable traps mac-notification
```

3.23 CFM OAM

3.23.1 clear ethernet cfm

Command: `clear ethernet cfm { statistic | traceroute-reply }`

Function: Clears MEP message receive statistics and link trace results.

Parameters: statistic: MEP message receive statistics.

traceroute-reply: Automatic link trace results.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Clears the current MEP message receive statistics and link trace results on the switch.

Example: Clear the local MEP message receive statistics.

```
Switch#clear ethernet cfm statistic
```

3.23.2 continuity-check

Command: `continuity-check enable`
`no continuity-check enable`

Function: Enables sending and receiving of CCMs on the local MEP.

Parameters: None.

Default: Disabled.

Command Mode: MA Mode.

Usage Guidelines: Use this command to enable CCM sending and receiving on the maintenance point.

Example: Enable CCM sending and receiving in MA test_ma.

```
Switch(config)#ethernet cfm domain test_1
Switch (config-ecfm)#service test_ma
Switch (config-ecfm-srv)#continuity-check enable
```

3.23.3 continuity-check interval

Command: `continuity-check interval < interval-value >`
`no continuity-check interval`

Function: Configures the interval at which MEPs send CCMs.

Parameters: <interval-value>: The interval value, from 1 to 7.

Default: 4 (1 second).

Command Mode: MA Mode.

Usage Guidelines: Use this command to change the CCM transmission interval of all MEPs in the MA. The range is 1 to 7.

Example: Set the CCM transmission interval to 7 in MA test_ma.

```
Switch(config)#ethernet cfm domain test_1
Switch (config-ecfm)#service test_ma
Switch(config-ecfm-srv)#continuity-check interval 7
```

3.23.4 continuity-check receive

Command: `continuity-check receive rmep <mep-id> [active time < time >]`
`no continuity-check receive rmep <mep-id>`

Function: Enables CCM reception and creates a remote MEP (RMEP) in the MA.

Parameters: <mep-id>: The RMEP ID, from 1 to 4094.

<time>: The activation time of the RMEP, from 0 to 600 seconds.

Default: CCM reception in the MA is disabled. The default activation time is 0 seconds; once an RMEP is configured, CCM reception from that RMEP is enabled.

Command Mode: MA Mode.

Usage Guidelines: Use this command to enable CCM detection for the specified RMEP in the MEP list of the MA. A local MEP can then receive CCMs sent by other MEPs in the same MA.

Example: Detect CCMs sent by RMEP 2 in MA test_ma.

```
Switch(config)#ethernet cfm domain test_1
Switch (config-ecfm)#service test_ma
Switch(config-ecfm-srv)#continuity-check receive rmep 2
```

3.23.5 cos

Command: cos < cos-value >
no cos

Function: Configures the priority (CoS) of messages sent by MEPs.

Parameters: <cos-value>: The message priority, from 0 to 7.

Default: 0.

Command Mode: MA Mode.

Usage Guidelines: Use this command to set the CoS value carried in all messages sent by MEPs in the MA, including fault notifications.

Example: Set the message CoS priority to 5 in MA test_ma.

```
Switch(config)#ethernet cfm domain test_1
Switch (config-ecfm)#service test_ma
Switch(config-ecfm-srv)# cos 5
```

3.23.6 debug ethernet cfm

Command: debug ethernet cfm packet [detail] [lb|lt]
debug ethernet cfm packet [detail] cc [domain <md_name> [service { ma-name | number < ma-num > | pvlan < vlan-id > }]]
debug ethernet cfm fsm [lb|lt]
debug ethernet cfm fsm cc [send|received] [domain <md_name> [service { ma-name | number < ma-num > | pvlan < vlan-id > }]]
debug ethernet cfm timer [domain < md_name > [service { ma-name | number < ma-num > | pvlan < vlan-id > }]
no debug ethernet cfm packet [detail] [lb|lt]
no debug ethernet cfm packet [detail] cc [domain <md_name> [service { ma-name | number < ma-num > | pvlan < vlan-id > }]]
no debug ethernet cfm fsm [lb|lt]
no debug ethernet cfm fsm cc [send|received] [domain < md_name > [service { ma-name | number < ma-num > | pvlan < vlan-id > }]]
no debug ethernet cfm timer [domain <md_name > [service { ma-name | number < ma-num > | pvlan < vlan-id > }]

Function: Enables CFM debugging.

Parameters: packet: Enables message debugging.

detail: Enables detailed message debugging.

cc: Enables continuity check (CC) message debugging.

send: Enables debugging of status related to CC messages sent.

received: Enables debugging of status related to CC messages received.

lb: Enables loopback (LB) debugging.

lt: Enables linktrace (LT) debugging.

fsm: Enables state machine debugging.

timer: Enables timer debugging.

<md_name>: Enables debugging for the specified maintenance domain.

<ma-name>: The maintenance association (MA) name, from 1 to 43 characters. It can contain letters, digits, and underscores, but cannot begin or end with an underscore. The MA name and domain name together cannot exceed 44 characters.

number <ma-num>: The unique MA number within the maintenance domain, from 0 to 65535.

<vlan-id>: The primary VLAN of the service, from 1 to 4094.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Use this command to enable debugging of CFM messages, state machines, and timers. Debugging can be enabled for all maintenance domains or for a specific MA.

Example: Enable local CFM debugging.

```
Switch#debug ethernet cfm all
```

3.23.7 debug ethernet cfm error

Command: **debug ethernet cfm error**
no debug ethernet cfm error

Function: Displays CFM fault information.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Use this command to display CFM fault information.

Example: Display CFM fault information.

```
Switch#debug ethernet cfm error
```

3.23.8 debug ethernet cfm operation

Command: **debug ethernet cfm operation**
no debug ethernet operation

Function: Displays information about CFM platform calls to the driver for sending.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Displays information about CFM platform calls to the driver for sending.

Example: Display local CFM platform-to-driver sending information.

```
Switch#debug ethernet cfm operation
```

3.23.9 ethernet cfm alarm

Command: **ethernet cfm alarm {delay < mseconds > | notification { all | error-xcon | mac-remote-error-xcon | none | remote-error-xcon | xcon} | reset < mseconds >}**
no ethernet cfm alarm { delay | notification { all | error-xcon | mac-remote-error-xcon | none | remote-error-xcon | xcon} | reset }

Function: Configures CFM fault alarms.

Parameters: delay <mseconds>: The notification delay; a fault must be detected continuously for this time before it is reported. The unit is milliseconds, the range is 2500 to 10000, and the default is 2500.

notification: Configures which faults are reported.

all: Reports all faults: DefRDI, DefMACStatus, DefRemote, DefError, and DefXcon.

error-xcon: Reports DefError and DefXcon faults.

mac-remote-error-xcon: Reports only DefMACStatus, DefRemote, DefError, and DefXcon faults. This is the default.

none: No faults are reported.

remote-error-xcon: Reports only DefRemote, DefError, and DefXcon faults.

xcon: Reports only DefXcon faults.

reset <mseconds>: The reset time after a fault is detected and reported; no further fault notification is sent within this time. The unit is milliseconds, the range is 2500 to 10000, and the default is 10000.

Default: The notification delay is 2.5 seconds; only DefMACStatus, DefRemote, DefError, and DefXcon faults are reported; and no further notification is sent within 10 seconds.

Command Mode: Global Mode.

Usage Guidelines: Use this command to select the fault types to report and to set the notification delay and reset time.

Example: Report only xcon faults.

```
Switch(config)#ethernet cfm alarm notification xcon
```

3.23.10 ethernet cfm auto-traceroute cache

Command: ethernet cfm auto-traceroute cache { size < size-value > | hold-time <minutes>}
no ethernet cfm auto-traceroute cache { size | hold-time }

Function: Configures the cache size and hold time for automatic linktrace (LT) results.

Parameters: <size-value>: The automatic LT result cache size, from 1 to 100, in number of linktrace operations. The default is 5, meaning the 5 most recent results are cached.

<minutes>: The hold time of automatic LT results in the cache, from 1 to 65535 minutes. The default is 100 minutes; cached records older than this are deleted.

Default: The cache stores the 5 most recent automatic LT results, and the hold time is 100 minutes.

Command Mode: Global Mode.

Usage Guidelines: Use this command to configure the size and hold time of the local cache for automatic LT results.

Example: Set the hold time of automatic LT results to 500 minutes.

```
Switch(config)#ethernet cfm auto-traceroute cache hold-time 500
```

3.23.11 ethernet cfm domain

Command: ethernet cfm domain < domain-name > level < level-id >
no ethernet cfm domain < domain-name >

Function: Creates a maintenance domain (MD) and enters MD Configuration Mode.

Parameters: <domain-name>: The MD name, from 1 to 43 characters. It can contain letters, digits, and underscores, but cannot begin or end with an underscore.

<level-id>: The MD level, from 0 to 7.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: Creates an MD. No MD exists by default. If the MD name is invalid, the MD is not created. Multiple MDs with different names and levels can be configured on the same switch, but each MD can have only one level, which cannot be changed after the MD is created.

Example: Create a level 3 MD named operatorA.

```
Switch(config)#ethernet cfm domain operatorA level 3
Switch(config-ecfm)#
```

3.23.12 ethernet cfm global

Command: **`ethernet cfm global`**
`no ethernet cfm global`

Function: Enables CFM on the local device.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Use this command to enable CFM OAM on the local device.

Example: Enable CFM OAM.

```
Switch(config)#ethernet cfm global
```

3.23.13 ethernet cfm logging

Command: **`ethernet cfm logging`**
`no ethernet cfm logging`

Function: Enables CFM logging.

Parameters: None.

Default: Alarms are recorded in the log.

Command Mode: Global Mode.

Usage Guidelines: Enables logging. When an alarm occurs, it is recorded in the log and the fault is reported.

Example: Enable CFM logging.

```
Switch(config)#ethernet cfm logging
```

3.23.14 ethernet cfm mep

Command: **`ethernet cfm mep < mepid > domain < domain-name > service { < ma-name > | number < ma-num > | pvlan < vlan-id > }`**
`no ethernet cfm mep < mepid > domain < domain-name > service { < ma-name > | number < ma-num > | pvlan < vlan-id > }`

Function: Creates a MEP.

Parameters: **<domain-name>**: The MD name.

<mepid>: The MEP ID.

<ma-name>: The MA name.

<ma-num>: The unique MA number within the MD, from 0 to 65535.

<vlan-id>: The primary VLAN of the service, from 1 to 4094.

Default: No MEP exists on the port.

Command Mode: Port Mode.

Usage Guidelines: The specified MD must exist; otherwise, an error occurs. To configure the port as a MEP for several MDs, run this command for each MD. The VLAN specified in the command must already be the primary VLAN of the MA, which is used to find the corresponding MA; otherwise, an error occurs.

Example: Create MEP 5 in MA ma1 of MD CustomerB on port e1/1.

```
Switch(config)#interface ethernet 1/1
Switch(config-if-ethernet1/1)#ethernet cfm mep 5 domain CustomerB service ma1
```

3.23.15 ethernet cfm mip

Command: ethernet cfm mip auto-create level < level-id > vlan < WORD > [lower-mep-only] [sender-id chassis]
no ethernet cfm mip auto-create level

Function: Configures automatic MIP creation at levels not associated with an MA.

Parameters: <level-id>: The default MD level, from 0 to 7.

<WORD>: The list of VLANs, not associated with an MA, on which MIPs are created, from 1 to 4094, separated with ";" and "-".

lower-mep-only: Uses the explicit rule. If the port has no MEP at a higher level, a MIP is created at this level only if a MEP exists at a lower MA level. If this parameter is not specified, the default rule is used: if the port has no MEP at a higher level and no MIP at a lower level, a MIP is created at this level.

sender-id chassis: Messages sent by MIPs created in the default MD carry the Sender ID TLV. If this parameter is not specified, the TLV is not carried.

Default: No MIP creation rule is configured, no MIP exists, and the Sender ID TLV is not carried.

Command Mode: Global Mode.

Usage Guidelines: MIPs created by this command have lower priority than those created manually with the **ethernet cfm mip level** command; that is, if a MIP is created manually in Port Mode, the automatic creation rules are not used. The 802.1ag-2007 standard specifies that each device can have one default MD. To change the default MD, delete the existing one and create a new one. The default MD level must be higher than the levels of all MDs with MEPs. MIPs created at a level equal to a higher MD level pass CCMs of the higher level and respond with LTRs.

Example: Configure the rule for creating MIPs at level 6 on ports in VLAN 500.

```
Switch(config)#ethernet cfm mip auto-create level 6 vlan 500 lower-mep-only
```

3.23.16 ethernet cfm mode

Command: ethernet cfm mode {hw|sw|auto}
no ethernet cfm mode

Function: Configures how the device implements CFM.

Parameters: hw: CFM is implemented in hardware.

sw: CFM is implemented in software.

auto: The implementation method is selected automatically. If all cards support the same method, that method is used; otherwise, software is used.

Default: auto.

Command Mode: Global Mode.

Usage Guidelines: Use this command to switch the implementation mode. If the cards do not all support the same method, you can configure the method explicitly.

Example: Configure hardware-based CFM in Global Mode.

```
Switch(config)# ethernet cfm mode hw
```

3.23.17 ethernet cfm pvlan

Command: ethernet cfm pvlan <1-4094> vlan WORD
no ethernet cfm pvlan <1-4094>

Function: Configures the mapping between a primary VLAN (PVLAN) and VLANs.

Parameters: <1-4094>: The primary VLAN ID, from 1 to 4094.

WORD: The VLANs associated with the primary VLAN.

Default: No PVLAN-to-VLAN mapping is configured.

Command Mode: Global Mode.

Usage Guidelines: This command maps a primary VLAN to VLANs. An MA is associated with one primary VLAN, so one MA can be associated with several VLANs. Note that VLAN mappings cannot be configured for a primary VLAN that is already associated with an MA.

Example: Map primary VLAN 1 to VLAN 10.

```
Switch(config)#ethernet  cfm pvlan 1 vlan 10
```

3.23.18 ethernet cfm snmp-server enable traps

Command: ethernet cfm snmp-server enable traps
no ethernet cfm snmp-server enable traps

Function: Enables SNMP notifications for CFM alarms.

Parameters: None.

Default: Enabled.

Command Mode: Global Mode.

Usage Guidelines: When configured, an SNMP notification is sent when an alarm occurs.

Example: Enable trap notifications for alarms.

```
Switch(config)# ethernet cfm snmp-server enable traps
```

3.23.19 ethernet cfm y1731 global

Command: ethernet cfm y1731 global
no ethernet cfm y1731 global

Function: Enables Y.1731.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Enables Y.1731. When this function is enabled, the switch operates in Y.1731 mode and sends and parses messages in Y.1731 format.

Note: Run the **ethernet cfm global** command before using this command; otherwise, this command does not take effect.

Example: Enable Y.1731 globally.

```
Switch(config)# ethernet cfm y1731 global
```

3.23.20 id

Command: id {mac-address XX-XX-XX-XX-XX-XX domain-number < domain-number > | dns < dns-name > | null }
no id

Function: Configures the MD ID (MDID).

Parameters: mac-address XX-XX-XX-XX-XX-XX domain-number <domain-number>: MD name format 3; **<domain-number>** is a 2-byte integer.

dns <dns-name>: MD name format 2, a DNS name of 1 to 43 characters.

null: MD name format 1, with no MD name configured; the MA name must be globally unique.

Default: None.

Command Mode: MD Mode.

Usage Guidelines: When this command is configured, the domain name configured with the **ethernet cfm domain** command is not carried in messages. The MDID and MA name form the MAID, whose total length is 44 bytes; this length cannot be exceeded, or an error occurs.

Example: Configure the MDID.

```
Switch(config)#ethernet cfm domain customerA level 5
Switch(config-ecfm)#id mac-address 00-03-0f-07-08-09 domain-number 1017
```

3.23.21 mep mepid

Command: mep mepid < WORD >
no mep mepid [< WORD >]

Function: Creates the list of MEPs allowed in the MA.

Parameters: <WORD>: The MEP ID list, separated with ";" and "-". The range is 1 to 4094.

Default: None.

Command Mode: MA Mode.

Usage Guidelines: Use this command to create the list of MEPs allowed in the MA.

Example: In MD operatorA, create MEP IDs 1 to 25 for service ma1 in VLAN 5.

```
Switch(config)#ethernet cfm domain operatorA level 5
Switch(config-ecfm)#service ma1 vlan 5
Switch(config-ecfm-srv)#mep mepid 1-25
```

3.23.22 mip auto-create

Command: mip auto-create [lower-mep-only | none]
no mip auto-create

Function: Configures automatic MIP creation in the MA.

Parameters: lower-mep-only: Uses the explicit rule. If the port has no higher-level MEP and no MIP at a lower MA level, a MIP is created at this level only if a MEP exists at a lower MA level.

none: Uses the none rule; MIPs are not created automatically.

Default: No MIP is created.

Command Mode: MA Mode.

Usage Guidelines: Configures the rule for automatically creating MIPs for the MA. MIPs are created automatically on ports in the VLAN according to the rule. If no parameter is specified, the default rule is used: if the port has no higher-level MEP and no MIP at a lower MA level, a MIP is created at this level.

Note: MIPs created by this command have lower priority than MIPs created manually with the **ethernet cfm mip level** command; that is, if you create MIPs manually in Port Mode, the automatic rules are not used.

To create MIPs on all ports of the MD, select the default rule. To create MIPs only where MEPs exist at a lower maintenance level, select the explicit rule.

If the MIP creation rule of an MA differs from that of its MD, the MA rule is used.

The number of MIPs cannot exceed 384. MIPs are created according to the rules; if the number would exceed this limit, creation fails and an error is reported.

The default rule for an MD is none; the default for MIPs under an MA is defer, meaning the MA inherits the MIP creation rule of the MD.

Example: Use the default MIP creation rule in level 5 MD customerA.

```
Switch(config)#ethernet cfm domain customerA level 5
Switch(config-ecfm)#mip auto-create
```

3.23.23 ping ethernet

Command: ping ethernet [target-mep < mepid > | target-mac < mac-address >] {domain < domain-name > service { < ma-name > | number < ma-num > | pvlan < vlan-id > }} [number < number >] [packetsize < size >] [timeout < timeout >]

Function: Starts the loopback function.

Parameters: <mepid>: The ID of the destination MEP of the LBM.

<mac-address>: The destination MAC address, in H-H-H format.

<domain-name>: The MD name of the destination MP.

<ma-name>: The MA name, from 1 to 43 characters. It can contain letters, digits, and underscores, but cannot begin or end with an underscore.

number <ma-num>: The unique MA number within the MD, from 0 to 65535.

<vlan-id>: The primary VLAN of the service, from 1 to 4094.

<number>: The number of LBMs to send, from 1 to 10. The default is 5.

<size>: The LBM data packet size, from 46 to 1500 bytes. The default is 46.

<timeout>: The LBM timeout. If no LBR is received within this time, the loopback process ends. The range is 3 to 10 seconds; the default is 5 seconds.

Default: Loopback is disabled. When enabled, 5 LBMs of 46 bytes are sent with a timeout of 5 seconds.

Command Mode: Admin Mode.

Usage Guidelines: Sends LBMs from a specified maintenance point to another point and receives LBRs. This function is disabled by default. If a target MEP ID is specified, the switch looks up the corresponding MAC address and reports an error if it is not found. If a MAC address is specified, loopback is performed to that address. If only a domain name is specified, Y.1731 must be enabled, and multicast LBMs are sent.

Example: Start loopback to check the link status of MEP 2 in test_ma.

```
Swtich#ping ethernet target-mep 2 domain test_ma service 4
Reply from 00-03-0f-00-00-03: bytes = 46 sequence number=0
Reply from 00-03-0f-00-00-03: bytes = 46 sequence number=1
Reply from 00-03-0f-00-00-03: bytes = 46 sequence number=2
Reply from 00-03-0f-00-00-03: bytes = 46 sequence number=3
Reply from 00-03-0f-00-00-03: bytes = 46 sequence number=4
Packets statistics for 00-03-0f-00-00-03:
Sent = 5, Received = 5, Lost = 0 (0% loss).
Approximate round trip times in milli-seconds:
Minimum < 16 ms, Maximum = 16 ms, Average < 16 ms.
```

Field	Description
Reply from 00-03-0f-00-00-03	An LBR was received from the device with MAC address 00-03-0f-00-00-03
bytes = 46	Size of the received LBR message
sequence number	Sequence number of the received LBR
Packets statistics for 00-03-0f-00-00-03	Statistics of LBRs received from the device with MAC address 00-03-0f-00-00-03
Send	Number of LBMs sent
Received	Number of LBRs received
Lost	Number of LBMs or LBRs lost
Minimum	Shortest round-trip time between sending an LBM and receiving an LBR
Maximum	Longest round-trip time between sending an LBM and receiving an LBR
Average	Average round-trip time between sending an

	LBM and receiving an LBR

3.23.24 sender-id

Command: sender-id { chassis | none}

Function: Configures whether sent messages carry Sender ID information.

Parameters: chassis: Sent messages carry Chassis ID information.

none: Sent messages do not carry the Sender ID TLV.

Default: Sent messages do not carry the Sender ID TLV.

Command Mode: MA Mode.

Usage Guidelines: Use this command to determine whether messages carry Sender ID information.

Example: Configure messages in the MA to carry Chassis ID information.

```
Switch(config-ecfm-srv)#sender-id chassis
```

3.23.25 service

Command: service { < ma-name > | number < ma-num > | pvlan < vlan-id > }{ port | pvlan < vlan-id > } [direction down]
no service { < ma-name > | number < ma-num > | pvlan < vlan-id > }

Function: Creates an MA.

Parameters: <ma-name>: The MA name, from 1 to 43 characters. It can contain letters, digits, and underscores, but cannot begin or end with an underscore. The MA name and domain name together cannot exceed 44 characters.

number <ma-num>: The unique MA number within the MD, from 0 to 65535.

<vlan-id>: The primary VLAN of the service, from 1 to 4094.

port: The MA is not associated with any VLAN.

direction down: The direction of the MA. The default is up; specify this keyword for down.

Default: No MA is created.

Command Mode: MD Mode.

Usage Guidelines: An MA must be unique within its MD. If the MD name is null, the MA must be globally unique.

If the MAID does not include the MD name, the MA name cannot exceed 45 characters. If it includes the MD name, the MD name cannot exceed 43 characters, and the MA name and MD name together cannot exceed 44 characters.

An MD must be created before an MA. A switch supports up to 512 MAs.

A service (MA) can be associated with one or more VLANs. If the service direction is down, services of several levels can be associated with the same VLANs; if the direction is up, they cannot.

A primary VLAN cannot be associated with MDs of different levels; the primary VLAN and level identify the MA.

If a service is configured as **port**, it is not associated with any VLAN and links only two points. The MEPs in the service must be down MEPs; messages are sent only between these two points and are not forwarded.

Example: In MD customerA, create MA 10 associated with VLAN 17 in the down direction.

```
Switch(config)#ethernet cfm domain customerA level 5
Switch(config-ecfm)#service 10 pvlan 17 direction down
Switch(config-ecfm-srv)#
```

3.23.26 show ethernet cfm domain

Command: **`show ethernet cfm domain { < domain_name > | brief }`**

Function: Displays the MD configuration.

Parameters: <domain_name>: The MD name, from 1 to 43 characters. It can contain letters, digits, and underscores, but cannot begin or end with an underscore. If no MD is specified, all MDs on the device are displayed.

brief: Displays brief MD information.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays the MD configuration.

Example: Display brief information for all local MDs.

```
Switch#show ethernet cfm domain brief
Domain Name                                Level             Services Number
-----------------------------------------------------------------------------
--------------------------------------
test_ma                                      Lv4                2
```

Field	Description
Domain Name	MD name, which uniquely identifies the MD
Level	MD level
Services Number	Number of MAs in the MD

Display the configuration of local MD test_ma.

```
Switch#show ethernet cfm domain test_ma
Domain Name: test_ma
Level: 4
Total Services: 2
Service Name   Primary Vlan   Dir      CC Send   CC Received   CC Interval
-----------------------------------------------------------------------------
-------------------------------------
4              Vlan1          Down    Enable    Enable         1(s)
1              Vlan2          Up      Disable    Disable         1(s)
```

Field	Description
Domain Name	MD name, which uniquely identifies the MD
Level	MD level
Total Services	Number of MAs in the MD
Service Name	MA name
Primary Vlan	Primary VLAN associated with the MA
Dir	Direction of the MA
CC Send	Whether CC sending is enabled in the MA
CC Received	Whether CC reception is enabled in the MA
CC Interval	CC transmission interval in the MA

3.23.27 show ethernet cfm errors

Command: **`show ethernet cfm errors`**

Function: Displays the errors detected on the device.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays the errors detected on the device.

Example: Display the errors detected on the device.

```
Switch(config))#show ethernet cfm errors
Code：X – xconCCDomainefect, E – errorCCDomainefect, O -
someRMEPCCDomainefect, M – someMACstatusDefect, R - someRDIdefect
Mepid        Error type             Domain name          Service name   Level
-------------------------------------------------------------------------------
-------------------------------------
1             X E                  kk                     ma           lv7
1             X E                  kk                     ma           lv7
1             X E                  kk                     ma           lv7
1             X E                  kk                     ma           lv7
```

Field	Description
MEPID	Local MEP ID that detected the errors
Domain ID	Name of the MD where the MEP that detected the errors is located
MAName	MA name of the MEP that detected the errors
error-type	Error types: xconCCMdefect, errorCCMdefect, someRMEPCCMdefect, someMACstatusDefect, and someRDIdefect
Level	Level of the MEP

3.23.28 show ethernet cfm maintenance-points local

Command: show ethernet cfm maintenance-points local [detail] [mep | mip] [domain < domain-name > | interface { ethernet | } <IFNAME>]

Function: Displays the attributes and operating information of local maintenance points.

Parameters: detail: Displays detailed information.

mep: Displays MEP information.

mip: Displays MIP information.

<domain-name>: The MD name.

interface { ethernet | } <IFNAME>: The port where the maintenance point is located.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays local maintenance point information. If no optional parameter is specified, basic information about all MPs on the switch is displayed. The display can be filtered by MD or port.

Example: Display all local MEP information on the switch.

```
Switch#show ethernet cfm maintenance-points local mep
-------------------------------------------------------------------------------
--------------------------------
Mepid    Domain Name     Level             Vlan-id        CC Send
         Service Name      Direction          Port
-------------------------------------------------------------------------------
--------------------------------
1        test_ma           Lv4               Vlan1         Enable
4                 Down             Ethernet1/4
```

Field	Description
Mepid	MP ID; None for a MIP
Domain Id	Domain ID
MA Name	MA name
Lvl	Level of the MP
Dir	MP direction
Port	Port where the MP is located
Type	MEP type (VLAN or port)
Vlan-id	List of VLAN IDs associated with the MEP

CC	Whether the CC function is enabled

```
Switch#show ethernet cfm maintenance-points local detail mep
Mepid:11
Port:Ethernet1/1                      Active:0
Domain Name:kk
Service Name:mb
Level:2                         Vlan:None                       Direction:Down
------------------------------------------------------------------------------
------------------------------
CCM:
CC Send:Enable   CC Received:Enable   Interval:1(s)
------------------------------------------------------------------------------
------------------------------
No CCM from some remote MEPs is received.
------------------------------------------------------------------------------
---------------------------------
One or more error CCM is received. The last-received CCM:
Domain Name: kk
Service Name: ma
Mepid:2
Received Time:Jan 01 00:17:25 2006
------------------------------------------------------------------------------
---------------------------------
One or more cross-connect CCM is received. The last-received CCM:
Domain Name: kk
Service Name: ma
Mepid:2
Received Time:Jan 01 00:17:25 2006
------------------------------------------------------------------------------
---------------------------------
Some other MEPs are transmitting the RDI bit.
```

Field	Description
Interface	Port where the maintenance point is located
DOMAIN	MD where the maintenance point is located
SERVICE	MA where the maintenance point is located
Level	MD level
VLAN	VLAN of the MA
Direction	Direction of the maintenance point
CCM	CCM information
CCM send	Whether the maintenance point sends CCMs
CCM received	Whether the maintenance point receives CCMs
Interval	CCM transmission interval
Crosscheck	Whether the maintenance point checks for cross-connect errors
Start-delay	Delay before the cross-connect check starts
No CCM from some remote MEPs is received	Indicates that CCMs from some remote MEPs have not been received (timeout error)
One or more streams of error CCMs is received. The last-received CCM	Indicates that error CCMs were received and displays information about the last error CCM
DOMAIN	MD of the last error CCM
SERVICE	Service of the last error CCM
MEP	MEP of the last error CCM
Received Time	Time the last error CCM was received
One or more cross-connect CCMs is received. The last-	Indicates a possible cross-connect in the network: cross-connect CCMs were received, and information about the

received CCM	last one is displayed
Some other MEPs are transmitting the RDI bit	Indicates that RDI (remote defect indication), set in CCMs, was received from other maintenance points (displayed only when such CCMs are received)

3.23.29 show ethernet cfm maintenance-points remote

Command: show ethernet cfm maintenance-points remote (domain WORD (service (WORD|number <0-65535>|pvlan <1-4094>) (mepid <1-4094>|)|)|)

Function: Displays the attributes and operating information of remote maintenance points.

Parameters: <domain-name>: The MD name.

<mepid>: The MEP ID.

<ma-name>: The MA name, from 1 to 43 characters. It can contain letters, digits, and underscores, but cannot begin or end with an underscore.

number <ma-num>: The unique MA number within the MD, from 0 to 65535.

<vlan-id>: The primary VLAN of the service, from 1 to 4094.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays remote maintenance point information. If no optional parameter is specified, basic information about all remote MEPs on the switch is displayed.

Example: Display all remote MEP information on the switch.

```
Switch#show ethernet cfm maintenance-points remote
-------------------------------------------------------------------------------
---------------------------------
Mepid       Domain Name   Level         Mac Address           RDI
Service Name    Vlanid        Ingress               Status
-------------------------------------------------------------------------------
---------------------------------
2           test_ma         Lv4           00-03-0f-00-00-03       Y
            4               Vlan1         Ethernet1/4           Linkup
```

Field	Description
Mepid	MEP ID
Domain Name	MD name
Level	MD level
Mac Address	MEP MAC address
RDI	Whether the RDI bit is set in CCMs sent by the remote MEP
Service Name	MA name
Vlanid	VLAN associated with the MA
Ingress	Port on which messages from the remote MEP are received
Status	Remote MEP status

3.23.30 show ethernet cfm maintenance-points remote detail

Command: show ethernet cfm maintenance-points remote detail (mac XX-XX-XX-XX-XX-XX | domain WORD (service ((WORD)|(number <0-65535>)|(pvlan <1-4094>))) mepid <1-4094>)

Function: Displays the attributes and operating information of remote maintenance points.

Parameters: mac <mac-address>: The MEP MAC address.

<mepid>: The MEP ID.

<domain-name>: The MD name.

<ma-name>: The MA name, from 1 to 43 characters. It can contain letters, digits, and underscores, but cannot begin or end with an underscore.

number <ma-num>: The unique MA number within the MD, from 0 to 65535.

<vlan-id>: The primary VLAN of the service, from 1 to 4094.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: If a MAC address is specified, detailed information about all remote MEPs using that MAC address is displayed. If a MEP ID is specified, the MD and MA must also be specified.

Example: Display the specified remote MEP on the switch; the MEP belongs to Domain_L5, and the primary VLAN of the MA is 5.

```
Switch#show ethernet cfm maintenance-points remote detail mepid 401 domain
Domain_L5 vlan 5
Mac Address:00-03-0f-07-04-01
Domain Name:kk
Service Name:ma
Level:2
Vlan:1
Mepid:1
Incoming Port:Ethernet1/2
CC Send Interval:1(s)
Mep Port Status:Up
Receive Rdi:N
```

Field	Description
MAC Address	MAC address of the remote MEP
Domain Name	MD name
MA Name	MA name
Level	MA level
VLAN	Primary VLAN of the MA
MPID	Remote MEP ID
Sender Chassis ID	Content of the Sender ID TLV
Incoming Port(s)	Local port that receives messages from the remote MEP
Cc send interval(ms)	CC transmission interval of the remote MEP
MEP interface status	Status of the remote MEP
Receive RDI	Whether RDI is being received

3.23.31 show ethernet cfm mpdb

Command: `show ethernet cfm mpdb`

Function: Displays the contents of the MIP database.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays the contents of the MIP database.

Example: Display the contents of the MIP database.

```
Switch#show ethernet cfm mpdb
Mac Address          Ingress               Vlan                  Age
--------------------------------------------------------------------------------
---------------------------------
```

```
00-03-0f-00-00-03     Ethernet1/4          Vlan1                    0 (s)
```

Field	Description
MacAddress	Source MAC address in the CCM
Ingress	Ingress port of the CCM
Type Id	FID and its value
Age	Time since the MIP database entry was last updated

3.23.32 show ethernet cfm service

Command: show ethernet cfm service [domain < domain-name > [service { ma-name | number < ma-num > | pvlan < vlan-id > }]]

Function: Displays MA configuration.

Parameters: <domain-name>: The MD name.

<ma-name>: The MA name, from 1 to 43 characters. It can contain letters, digits, and underscores, but cannot begin or end with an underscore.

number <ma-num>: The unique MA number within the MD, from 0 to 65535.

<vlan-id>: The primary VLAN of the service, from 1 to 4094.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays the MA configuration.

Note: If no MD is specified, the configuration of all MAs in all MDs is displayed.

If only an MD is specified, all MAs in that MD are displayed.

Example: Display the configuration of all MAs in all MDs.

```
Switch#show ethernet cfm service
Domain Name: test_ma
Level: 4
Service Name: 4
Active: 1
Primary Vlan: 1
Vlanlist: 1
Direction: Down
CC Send: Enable
CC Received: Enable
CC Interval: 1(s)
Meplist: 1-4094
Remote Mep: 2
------------------------------------------------------------
Domain Name: test_ma
Level: 4
Service Name: 1
Active: 1
Primary Vlan: 2
Vlanlist: 2
Direction: Up
CC Send: Disable
CC Received: Disable
CC Interval: 1(s)
------------------------------------------------------------
```

Field	Description
Domain Name	MD name
Level	MD level
Service Name	MA name
Active	Whether the MA is active

Primary Vlan	Primary VLAN associated with the MA
Vlanlist	VLANs associated with the MA
Direction	Direction of the MA
CC Send	Whether CC sending is enabled in the MA
CC Received	Whether CC reception is enabled in the MA
CC Interval	CC transmission interval in the MA
Meplist: 1-4094	MEP list
Remote Mep	Remote MEP

3.23.33 show ethernet cfm statistic

Command: `show ethernet cfm statistic [ domain < domain-name > [service { ma-name | number < ma-num > | pvlan < vlan-id > }]]`

Function: Displays CFM message statistics of the device.

Parameters: <domain-name>: The MD name.

<ma-name>: The MA name, from 1 to 43 characters. It can contain letters, digits, and underscores, but cannot begin or end with an underscore.

number <ma-num>: The unique MA number within the MD, from 0 to 65535.

<vlan-id>: The primary VLAN of the service, from 1 to 4094.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays CFM message statistics of the device.

Example: Display CFM message statistics of the device.

```
Switch#show ethernet cfm statistic
LB:
   SendLBM: 5                    ReceiveLBM: 0
   SendLBR: 0                    ReceiveLBR: 5
   ReceiveInOrderLBR: 5          ReceiveOutOrderLBR: 0          ErrorLBR: 0
LT:
   SendLTM: 0                    ReceiveLTM: 0
   SendLTR: 0                    ReceiveLTR: 0                  ErrorLTR: 0
Domain Name: test_ma
Service Name: 4
Mepid: 1
CCM:
   SendCCM: 0               ReceivedCCM: 18162
   OutOfOrder: 0              Xcon: 24
   ErrorCCM: 0                MacStatusCCM: 0               RdiCCM: 18138
```

Field	Description
SendLBM	Number of LBMs sent
ReceiveLBM	Number of LBMs received
SendLBR	Number of LBRs sent
ReceiveLBR	Number of LBRs received
ReceiveInOrderLBR	Number of LBRs received in order
ReceiveOutOrderLBR	Number of LBRs received out of order
ErrorLBR	Number of invalid LBRs received
SendLTM	Number of LTMs sent
ReceiveLTM	Number of LTMs received
SendLTR	Number of LTRs sent
ReceiveLTR	Number of LTRs received
ErrorLTR	Number of invalid LTRs received
Domain Name	MD name

Service Name	MA name
Mepid	MEP ID
SendCCM	Number of CCMs sent
ReceivedCCM	Number of CCMs received
OutOfOrder	Number of CCMs received out of order
Xcon	Number of cross-connect CCMs received
ErrorCCM	Number of invalid CCMs received
MacStatusCCM	Number of CCMs received with a MAC status error
RdiCCM	Number of CCMs received with the RDI bit set to 1

3.23.34 show ethernet cfm status

Command: `show ethernet cfm status`

Function: Displays the CFM status of the device.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays the CFM status of the device.

Example: Display the CFM status of the device.

```
Switch#show ethernet cfm status
Ethernet cfm is enabled.
Y1731 global is enabled.
```

Field	Description
CFM is enabled.	CFM is enabled
CFM is disabled.	CFM is disabled
Y1731 global is enabled	Y.1731 is enabled

3.23.35 show ethernet cfm traceroute-reply auto

Command: `show ethernet cfm traceroute-reply auto [ domain < domain_name > [service { ma-name | number < ma-num > | pvlan < vlan-id > }] ]`

Function: Displays automatic linktrace (LT) results.

Parameters: <domain_name>: The MD name.

<ma-name>: The MA name, from 1 to 43 characters. It can contain letters, digits, and underscores, but cannot begin or end with an underscore.

number <ma-num>: The unique MA number within the MD, from 0 to 65535.

<vlan-id>: The primary VLAN of the service, from 1 to 4094.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays the LTRs received in response to automatically sent LTMs.

Note: If no MD is specified, all automatic LT results on the device are displayed.

If no MA is specified, the automatic LT results of the specified MD are displayed.

Example: Display all automatic LT results.

```
Switch#show ethernet cfm traceroute-reply auto
Traceroute to MEP 606 with the sequence number 0,TTL 255.
Timeout is 5 seconds.Tracing the route to 00-03-0f-aa-22-23 on DOMAIN
test_4 ,Level 4, Service:4
```

```
Traceroute sent via Ethernet1/1, path found via MPDB
I-----Intermedian Bridge
D----Target Destination
*-----Per hop Timeout
MAC Address     TTL     Last MAC      Ingress/Egress Action    Relay Action
------------------------------------------------------------------------------
----------------------------------------
I   00-03-0f-00-00-03  254     00-03-0f-00-00-03   IngOK/EgrOK       FDB
D  00-03-0f-aa-22-23  253     00-03-0f-00-00-03         /EgrDown     Hit
```

Field	Description
MAC Address	Source MAC address in the LTR
TTL	Number of hops the LTM can still traverse (TTL)
Last MAC	MAC address of the previous-hop device traversed by the LTM
Ingress/Egress Action	Port status derived from the Reply Ingress TLV and Reply Egress TLV
Relay Action	Indicates whether the forwarding device found the target MAC address: Hit: This device is the target MAC address. FDB: The target MAC address was found in the forwarding table.

3.23.36 show ethernet cfm vlan table

Command: `show ethernet cfm vlan table`

Function: Displays the mapping between primary VLANs (PVLANs) and VLANs configured on the device.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: After associating primary VLANs with VLANs using the **ethernet cfm pvlan <1-4094> vlan WORD** command, use this command to display the mapping configured on the device.

Example: Display the PVLAN-to-VLAN mapping configured on the device.

```
Switch(config))# show ethernet cfm vlan table
ethernet cfm vlan table:
pvlan 2 vlan 3-6
pvlan 7 vlan 8-10
```

3.23.37 switchport ulpp group <group-id> track cfm cc level <level-value>

Command: `switchport ulpp group <group-id> track cfm cc level <level-value>`

Function: Associates a ULPP group member port with CFM continuity check (CC) detection.

Parameters: <group-id>: The ULPP group ID.

<level-value>: The level of the down MEP on the port whose CC error detection is associated with the ULPP group.

Default: Not associated.

Command Mode: Port Mode.

Usage Guidelines: Configures the level used to associate a ULPP group member port with CFM CC detection. When the ULPP group member port receives matching CFM information (timeout or recovery), the association action is performed.

Example: Associate the port in ULPP group 1 with CC detection of the down MEP at level 1.

```
Switch(config-if-ethernet1/1)#switchport ulpp group 1 track cfm level 1
```

3.23.38 traceroute ethernet

Command: traceroute ethernet { target-mep < target-mep-id > | target-mac < mac-address > } {domain < domain-name > service { < ma-name > | number < ma-num > | pvlan < vlan-id > }} [fdb-only | source < mepid >]] [ttl < ttl-value >]

Function: Checks the path from the specified maintenance point to the target point.

Parameters: <target-mep-id>: The ID of the target MEP of the LTM.

<mac-address>: The target MAC address, in H-H-H format.

<domain-name>: The MD of the target MP.

<ma-name>: The MA name, from 1 to 43 characters. It can contain letters, digits, and underscores, but cannot begin or end with an underscore.

number <ma-num>: The unique MA number, from 0 to 65535.

<vlan-id>: The primary VLAN of the service, from 1 to 4094.

fdb-only: Uses only the FDB to find the egress port. If not specified, both the FDB and the MIP database are queried.

source <mepid>: The ID of the MEP that sends the LTM.

<ttl-value>: The maximum number of hops the LTM can traverse, from 1 to 255. The default is 64.

Default: TTL is 64, and both the FDB and the MIP database are queried.

Command Mode: Admin Mode.

Usage Guidelines: The CFM traceroute command checks the path from the specified maintenance point to the target point. It sends an LTM to the target maintenance point and examines the LTRs returned to determine the path between devices.

Example: Trace the path to MAC address 00-03-0f-aa-22-23 in test_4.

```
Switch#traceroute ethernet target-mac 00-03-0f-aa-22-23 domain test_4 service
4
Traceroute with the sequence number 4,TTL 64.
Timeout is 5 seconds.Tracing the route to 00-03-0f-aa-22-23 on MD test_4,
Level 4, Service:4
Traceroute sent via Ethernet1/4, path found via MPDB
I-----Intermedian Bridge
D----Target Destination
*-----Per hop Timeout
MAC Address   TTL     Last MAC         Ingress/Egress Action  Relay Action
------------------------------------------------------------------------------
---------------------------------------
D  00-03-0f-aa-22-23  63     00-03-0f-00-00-03     IngOK/                 Hit
```

Field	Description
MAC Address	Source MAC address in the LTR
TTL	Number of hops the LTM can still traverse (TTL)
Last MAC	MAC address of the previous-hop device traversed by the LTM
Ingress/Egress Action	Port status derived from the Reply Ingress TLV and Reply Egress TLV
Relay Action	Indicates whether the forwarding device found the target MAC address: Hit: This device is the target MAC address. FDB: The target MAC address was found in the forwarding table.

3.23.39 traceroute ethernet auto

Command: **`traceroute ethernet auto`**
`no traceroute ethernet auto`

Function: Enables automatic sending of linktrace messages.

Parameters: None.

Default: Disabled.

Command Mode: MA Mode.

Usage Guidelines: Enables automatic sending of linktrace messages. This function is disabled by default.

Note: When this function is enabled and a maintenance point does not receive CCMs from a remote point within 3.5 CCM intervals, the connection to the remote point is considered faulty. The maintenance point then sends an LTM (targeting the remote maintenance point, with the TTL set to the maximum of 255) and examines the returned LTRs to locate the fault.

Example: Enable automatic sending of linktrace messages.

```
Switch(config-ecfm-srv)#traceroute ethernet auto
```

Chapter 4 Commands for IP Services

4.1 Layer 3 Interface

4.1.1 Bandwidth

Command: `bandwidth <bandwidth>`
`no bandwidth`

Function: Configures the bandwidth of a VLAN interface. The **no bandwidth** command restores the default. The VLAN interface bandwidth is used in protocol calculations and does not limit port bandwidth. For example, OSPF uses the interface bandwidth to calculate the link cost (cost = 10^8/bandwidth), so changing the bandwidth changes the OSPF link cost.

Parameters: <bandwidth> is the bandwidth of the VLAN interface, from 1 to 10000000000 bits. The units k, m, and g can be used; the converted value cannot contain decimals.

Command Mode: VLAN Interface Mode.

Default: 100,000,000 bits.

Usage Guidelines: This command can be used only in VLAN Interface Mode. Unit conversion: 1g = 1,000m = 1,000,000k = 1,000,000,000 bits.

Example: Set the bandwidth of VLAN 1 to 50,000,000 bits.

```
Switch(Config-if-Vlan1)#bandwidth 50m
```

4.1.2 description

Command: `description <text>`
`no description`

Function: Configures the description of a VLAN interface. The **no** form of this command removes the description.

Parameters: <text> is the VLAN interface description, up to 256 characters.

Default: Not configured.

Command Mode: VLAN Interface Mode.

Usage Guidelines: The description entered after the **description** keyword is displayed under the configured VLAN interface.

Example: Set the description of the VLAN interface to "test vlan".

```
Switch(config)#interface vlan 2
Switch(config-if-vlan2)#description test vlan
```

4.1.3 description (VRF mode)

Command: `description <text>`
`no description`

Function: Configures a description for the VRF, for example, to record the relationship between VPN instances. The **no** form of this command removes the description.

Parameters: <text>: The description text, from 1 to 256 characters.

Default: Not configured.

Command Mode: VRF Mode.

Usage Guidelines: The description entered after the **description** keyword is displayed under the configured VRF to provide related information.

Example: Set the VRF description to "associate with VRF-B VRF-C".

```
Switch(config)#ip vrf VRF-A
Switch(config-vrf)#description associate with VRF-B VRF-C
```

4.1.4 interface loopback

Command: `interface loopback <loopback-id>`
`no interface loopback <loopback-id>`

Function: Creates a loopback interface. The **no** form of this command deletes the specified loopback interface.

Parameters: <loopback-id> is the ID of the new loopback interface.

Default: No loopback interface exists.

Command Mode: Global Mode.

Usage Guidelines: Loopback interfaces use VLAN IDs starting from 1006. Users cannot configure a VLAN whose ID is used by a loopback interface (1006 or higher). If a VLAN at or after 1006 is already configured, such as VLAN 1006, the loopback interface uses the next available VLAN, such as VLAN 1007.

Example: Enter configuration mode for loopback interface 1.

```
Switch(config)#interface loopback 1
Switch(Config-if-Loopback1)#
```

4.1.5 interface vlan

Command: `interface vlan <vlan-id>`
`no interface vlan <vlan-id>`

Function: Creates a VLAN interface (Layer 3 interface). The **no interface vlan <vlan-id>** command deletes the specified Layer 3 interface.

Parameters: <vlan-id> is the ID of an existing VLAN, from 1 to 4094.

Default: No Layer 3 interface is configured at the factory.

Command Mode: Global Mode.

Usage Guidelines: Before creating a VLAN interface (Layer 3 interface), configure the VLAN; for details, see the VLAN section. When a VLAN interface is created with this command, the switch enters VLAN Interface Mode. After the VLAN interface is created, you can use the **interface vlan** command again to enter its configuration mode.

Example: Create a VLAN interface (Layer 3 interface).

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#
```

4.1.6 ip vrf

Command: `ip vrf <vrf-name>`
`no ip vrf <vrf-name>`

Function: Creates a VPN instance (VRF). The **no** form of this command deletes the VPN instance.

Parameters: <vrf-name>: The name of the VPN instance, from 1 to 64 characters.

Default: Not configured.

Command Mode: Global Mode.

Usage Guidelines: Creates a VPN instance. There is no default VPN instance on a PE; a PE can have multiple VPN instances, and instance names are case-sensitive. Note that a VPN instance takes effect only after an RD is configured.

Example:

```
Switch(config)#ip vrf VRF-A
Switch(config-vrf)#
```

4.1.7 ip vrf forwarding vrfName

Command: `ip vrf forwarding <vrfName>`
`no ip vrf forwarding <vrfName>`

Function: Binds the interface to the specified VRF.

Parameters: <vrfName>: The name of the VPN instance, fewer than 32 characters.

Default: The interface is bound to the master (global) VRF.

Command Mode: Interface Mode.

Usage Guidelines: Configure this command when the interface needs to access the VPN. An interface can be bound to only one VRF, but a VRF can be bound to multiple interfaces.

Example:

```
Switch(config)#int vlan 9
Switch(Config-if-Vlan9)#ip vrf forwarding vpn1
```

4.1.8 no interface IFNAME

Command: `no interface IFNAME`

Function: Deletes an interface. This command applies only to VLAN interfaces and loopback interfaces.

Parameters: IFNAME: The interface name.

Command Mode: Global Mode.

Usage Guidelines: Use this command to delete a Layer 3 interface. It accepts different spellings of the interface name; for example, vlan1, Vlan1, v1, and V1 all match.

Example: Delete interface vlan1.

```
(config)# no interface vlan1
```

4.1.9 rd

Command: `rd <ASN:nn_or_IP-address:nn>`

Function: Configures the route distinguisher (RD) of the VRF.

Parameters: <ASN:nn_or_IP-address:nn> is the route distinguisher, in ASN:nn or IP-address:nn format.

Default: Not configured.

Command Mode: VRF Mode.

Usage Guidelines: The RD identifies a VPN; each VPN must have a unique RD. Through RDs, VPN instances have independent address spaces and can use overlapping addresses. Note that the RD consists of an AS number (or IP address) and an arbitrary number, and an RD cannot be deleted directly.

Example:

```
Switch (config)#ip vrf VRF-A
Switch (config-vrf)# rd 300:3
Switch (config-vrf)#
```

4.1.10 route-target

Command: `route-target {import | export | both} <rt-value>`
`no route-target {import | export | both} <rt-value>`

Function: Configures the route target (RT) of the specified VRF. The **no** form of this command deletes the configuration.

Parameters: import: Applies ingress filtering to routes, that is, determines whether a VPN route can be added to this VRF.

export: The route target attached to routes of this VRF when they are advertised as VPNv4 routes; the receiving end uses it for ingress filtering.

both: Uses the same route target value for import and export.

<rt-value>: The route target value.

Default: Not configured.

Command Mode: VRF Mode.

Usage Guidelines: A route target is a BGP extended community used to filter VPN routes and control VPN membership and routing policies of directly connected sites. For import rules, the switch examines all routes received by all BGP processes and adds routes that meet the conditions (the export route target of the route intersects the import route target of this VRF) to the BGP process of this VRF, and then sends route updates to the private-network BGP neighbors of this VRF. For export rules, the switch adds the export route target to all BGP routes stored in the BGP process associated with this VRF and then sends route updates to all public-network neighbors. In addition, if the import route target of another VRF matches this export route target, a copy of the route is added to the matching VRF and route updates are sent to the private-network BGP neighbors of that VRF.

Example:

```
Switch (config)#ip vrf VRF-A
Switch (config-vrf)# route-target both 100:1
Switch (config-vrf)#
```

4.1.11 show ip route

Command: `show ip route [ database ]`

Function: Displays the routing table.

Parameters: database: Displays routing database information.

Command Mode: Admin Mode.

Usage Guidelines: Displays the contents of the core routing table, including the route type, destination network, mask, next-hop address, and interface.

Example:

```
Switch#show ip route
Codes: C - connected, S - static, R - RIP derived, O - OSPF derived
A - OSPF ASE, B - BGP derived
Destination Mask Nexthop Interface Pref
C 2.2.2.0 255.255.255.0 0.0.0.0 vlan2 0
C 4.4.4.0 255.255.255.0 0.0.0.0 vlan4 0
S 6.6.6.0 255.255.255.0 9.9.9.9 vlan9 1
```

Field	Description
C - connected	Directly connected route: a network segment directly connected to the Layer 3 switch
S – static	Static route: a route to a network segment manually configured by the user
R - RIP derived	RIP route, learned by the Layer 3 switch through RIP

O - OSPF derived	OSPF route, learned by the Layer 3 switch through OSPF
A - OSPF ASE	OSPF external route (imported into OSPF)
B - BGP derived	BGP route, learned through BGP
Destination	Destination network
Mask	Mask of the destination network
Nexthop	Next-hop IP address
Interface	Interface of the Layer 3 switch through which the next hop is reached
Preference	Route preference. If routes of several types lead to the same destination network, only the route with the highest preference is displayed in the core routing table.

4.1.12 show ip route vrf

Command: `show ip route vrf <vrf-name> [bgp | datebase]`

Function: Displays the routes of the specified VRF.

Parameters: <vrf-name>: The VRF name, created with the **ip vrf <vrf-name>** command.

bgp: Displays routes imported through BGP.

database: Displays the IP routing table database.

Default: None.

Command Mode: All Modes.

Usage Guidelines: Displays routes of the specified routing protocol.

Example:

```
Switch#show ip route vrf vrf-a bgp
Network Next Hop Metric LocPrf Weight Path
Route Distinguisher: 100:10 (Default for VRF test)
*> 11.1.1.0/24 11.1.1.64 0 0 200 ?
*> 20.1.1.0/24 11.1.1.64 0 0 200 ?
```

4.1.13 show ip vrf

Command: `show ip vrf [<vrf-name>]`

Function: Displays VRF (VPN routing/forwarding instance) information, including related RIP instance information; it can also display the fallback global option.

Parameters: <vrf-name>: The name of the VPN routing/forwarding instance.

Default: None.

Command Mode: All Modes.

Usage Guidelines: This command is also available in other routing protocols; when it is used, the related information of those protocols is displayed.

Example: Display the RIP instance information related to VRF "IPI".

```
Switch# show ip vrf IPI
VRF IPI, FIB ID 1
Router ID: 11.1.1.1 (automatic)
Interfaces:
Vlan1
!
VRF IPI; (id=1); RIP enabled Interfaces:
Ethernet1/0/8
Name             Interfaces
IPI                 Vlan1
```

```
Name                    Default RD          Interfaces
IPI                                           Vlan1
```

4.1.14 shutdown

Command: `shutdown`
`no shutdown`

Function: Shuts down the specified VLAN interface of the switch. The **no** form of this command enables the VLAN interface.

Command Mode: VLAN Interface Mode.

Default: Enabled.

Usage Guidelines: When a VLAN interface is shut down, it does not send data frames. If the interface needs to obtain an IP address through BOOTP or DHCP, it must be enabled.

Example: Enable the VLAN 1 interface of the switch.

```
Switch(Config-if-Vlan1)#no shutdown
```

4.2 Network Management Port

4.2.1 interface ethernet

Command: `interface ethernet <interface-name>`

Function: Enters Network Management Port Configuration Mode from Global Mode.

Parameters: <interface-name> is the port number; set it to 0.

Command Mode: Global Mode.

Usage Guidelines: Use the **exit** command to return from Network Management Port Configuration Mode to Global Mode.

Example: Enter the network management port.

```
Switch(config)#interface ethernet 0
Switch(Config-If-Ethernet0)#
```

4.2.2 ip address

Command: `ip address <ip-address> <mask>`
`no ip address [<ip-address> <mask>]`

Function: Sets the IP address and subnet mask of the network management port. The **no** form of this command deletes the IP address.

Parameters: <ip-address> is the IP address in dotted decimal notation. **<mask>** is the subnet mask in dotted decimal notation.

Command Mode: Network Management Port Configuration Mode.

Default: No IP address is configured.

Usage Guidelines: Use this command to configure the IP address of the network management port.

For example, set the IP address of the network management port to 192.168.1.10/24:

```
Switch(Config-If-Ethernet0)#ip address 192.168.1.10 255.255.255.0
```

4.2.3 shutdown

Command: `shutdown`
`no shutdown`

Function: Shuts down the network management port. The **no** form of this command enables the port.

Command Mode: Network Management Port Configuration Mode.

Default: Enabled.

Usage Guidelines: When the network management port is shut down, it does not send data frames, and the port status is displayed as down by the **show interface** command.

Example: Enable the network management port.

```
Switch(config)#interface ethernet 0
Switch(Config-If-Ethernet0)#no shutdown
```

4.3 IP Configuration

4.3.1 clear ip traffic

Command: `clear ip traffic`

Function: Clears IP protocol statistics.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Clears the statistics of packets received and sent by the IP kernel, including received, sent, and dropped packets and the send/receive error information for IP, ICMP, TCP, and UDP.

Example: Clear IP protocol statistics.

```
Switch#clear ip traffic
```

4.3.2 clear ipv6 neighbor

Command: `clear ipv6 neighbors`

Function: Clears the IPv6 neighbor cache.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: This command cannot clear static neighbors.

Example: Clear the neighbor list.

```
Switch#clear ipv6 neighbors
```

4.3.3 debug ip icmp

Command: `debug ip icmp`
`no debug ip icmp`

Function: Enables debugging of ICMP packets sent and received.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example:

```
Switch#debug ip icmp
IP ICMP: sent, type 8, src 0.0.0.0, dst 20.1.1.1
```

Field	Description
IP ICMP: sent	ICMP packet sent
type 8	Type 8 (ping request)
src 0.0.0.0	Source IPv4 address
dst 20.1.1.1	Destination IPv4 address

4.3.4 debug ip packet

Command: `debug ip packet`
`no debug ip packet`

Function: Enables IP packet debugging. The **no debug ip packet** command disables this debugging.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Displays information about IP packets received and sent, including the source and destination addresses and size.

Example: Enable IP packet debugging.

```
Switch #debug ip packet
IP PACKET: sent, src 200.1.1.35, dst 224.0.0.9, size 312, proto 17, vrf 0
IP PACKET: rcvd, src 101.1.1.1, dst 224.0.0.9, size 312, proto 17, from
Vlan200, vrf 0
```

4.3.5 debug ipv6 packet

Command: `debug ipv6 packet`
`no debug ipv6 packet`

Function: Enables debugging of IPv6 packets received and sent.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example:

```
Switch#debug ipv6 packet
IPv6 PACKET: rcvd, src <fe80::203:fff:fe01:2786>, dst <fe80::1>, size <64>,
proto <58>, from Vlan1
```

Field	Description
IPv6 PACKET: rcvd	IPv6 packet received
Src <fe80::203:fff:fe01:2786>	Source IPv6 address
Dst <fe80::1>	Destination IPv6 address
size <64>	Size of the packet
proto <58>	Protocol field in the IPv6 header
from Vlan1	The IPv6 packet was received on Layer 3 interface Vlan1

4.3.6 debug ipv6 icmp

Command: debug ipv6 icmp
no debug ipv6 icmp

Function: Enables debugging of ICMPv6 packets received and sent.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example:

```
Switch#debug ipv6 icmp
IPv6 ICMP: sent, type <129>, src <2003::1>, dst <2003::20a:ebff:fe26:8a49>
from Vlan1
```

Field	Description
IPv6 ICMP: sent	IPv6 ICMP packet sent
type <129>	ICMPv6 type (129: echo reply)
Src <2003::1>	Source IPv6 address
Dst <2003::20a:ebff:fe26:8a49>	Destination IPv6 address
from Vlan1	Layer 3 interface on which the packet is sent

4.3.7 debug ipv6 nd

Command: debug ipv6 nd [ns | na | rs | ra | redirect]
no debug ipv6 nd [ns | na | rs | ra | redirect]

Function: Enables debugging of the specified types of IPv6 ND messages received and sent. The **ns**, **na**, **rs**, **ra**, and **redirect** parameters represent neighbor solicitation, neighbor advertisement, router solicitation, router advertisement, and redirect messages. If no type is specified, debugging is enabled for all five types. The **no** form of this command disables debugging for the specified types, or for all five types if no type is specified.

Parameters: ns | na | rs | ra | redirect: The ND message type.

Default: Disabled for all five types of IPv6 ND messages.

Command Mode: Admin Mode.

Usage Guidelines: ND is an essential part of IPv6. This command displays ND messages of the specified type for troubleshooting.

Example:

```
Switch#debug ipv6 nd
IPv6 ND: rcvd, type <136>, src <fe80::203:fff:fe01:2786>, dst
<fe80::203:fff:fe01:59ba>
```

Field	Description
IPv6 ND: rcvd	ND packet received
type <136>	ND message type
src <fe80::203:fff:fe01:2786>	Source IPv6 address
dst <fe80::203:fff:fe01:59ba>	Destination IPv6 address

4.3.8 debug ipv6 tunnel packet

Command: `debug ipv6 tunnel packet`
`no debug ipv6 tunnel packet`

Function: Enables debugging of tunnel packets received and sent.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example:

```
Switch#debug ipv6 tunnel packet
IPv6 tunnel: rcvd, type <136>, src <fe80::203:fff:fe01:2786>, dst
<fe80::203:fff:fe01:59ba>
IPv6 tunnel packet : rcvd  src 178.1.1.1 dst 179.2.2.2 size 128 from tunnel1
```

Field	Description
IPv6 tunnel packet : rcvd	Tunnel packet received
type <136>	ND message type
src 178.1.1.1	Tunnel source IPv4 address
dst 179.2.2.2	Tunnel destination IPv4 address

4.3.9 description

Command: `description <desc>`
`no description`

Function: Configures the tunnel description. The **no** form of this command deletes the tunnel description.

Parameters: <desc> is the tunnel description, up to 256 characters.

Command Mode: Tunnel Mode.

Default: No tunnel description is configured.

Usage Guidelines: When the system has multiple tunnels, descriptions help users identify the purpose of each tunnel.

Example: Set the tunnel description to "toCernet2".

```
Switch(Config-if-Tunnel1)#description toCernet2
```

4.3.10 ip address

Command: `ip address <ip-address> <mask> [secondary]`
`no ip address [<ip-address> <mask>] [secondary]`

Function: Sets the IP address and subnet mask of the switch interface. The **no ip address [<ip-address> <mask>] [secondary]** command deletes the IP address configuration.

Parameters: <ip-address> is the IP address in dotted decimal notation. **<mask>** is the subnet mask in dotted decimal notation. **secondary** specifies that the IP address is a secondary IP address.

Command Mode: VLAN Interface Mode.

Default: No IP address is configured.

Usage Guidelines: This command manually configures an IP address on a VLAN interface. If **secondary** is not specified, the address is the primary IP address of the VLAN interface; if **secondary** is specified, it is a secondary IP address. A VLAN interface can have only one primary IP address and multiple secondary IP addresses. Both primary and secondary IP addresses can be

used for SNMP, Web, and Telnet management. The switch can also obtain an IP address through BOOTP or DHCP.

Example: Set the IP address of the VLAN 1 interface to 192.168.1.10/24.

```
Switch(Config-if-Vlan1)#ip address 192.168.1.10 255.255.255.0
```

4.3.11 ipv6 address

Command: ipv6 address <ipv6-address|prefix-length> [eui-64]
no ipv6 address <ipv6-address|prefix-length> [eui-64]

Function: Configures an aggregatable global unicast address, site-local address, or link-local address for the interface.

Parameters: <ipv6-address> is the IPv6 address prefix. **<prefix-length>** is the prefix length, from 3 to 128. **eui-64** specifies that the IPv6 address is generated automatically from the EUI-64 interface ID of the interface.

Command Mode: Interface Mode.

Default: None.

Usage Guidelines: The IPv6 address prefix cannot be a multicast address or any other special-purpose IPv6 address, and different Layer 3 interfaces cannot have the same address prefix. For a global unicast address, the prefix length must be at least 3. For site-local and link-local addresses, the prefix length must be at least 10. For a loopback interface, the prefix length must be 128.

Example: Configure an IPv6 address with prefix 2001:3f:ed8::99 and prefix length 64 on the Layer 3 interface of VLAN 1.

```
Switch(Config-if-Vlan1)#ipv6 address 2001:3f:ed8::99/64
```

4.3.12 ipv6 route

Command: ipv6 route <ipv6-prefix | prefix-length> {<ipv6address> | <interface-type interface-number> | {<ipv6address> <interface-type interface-number>} | tunnel <tunnel no> } [<precedence>]
no ipv6 route <ipv6-prefix | prefix-length> {<ipv6address> | <interface-type interface-number> | {<ipv6address> <interface-type interface-number>} | tunnel <tunnel no> } [<precedence>]

Function: Configures an IPv6 static route.

Parameters: <ipv6-prefix> is the destination prefix of the static route. **<prefix-length>** is the prefix length. **<ipv6address>** is the next-hop IPv6 address. **<interface-type interface-number>** is the name of the egress interface. **<tunnel no>** is the egress tunnel number of a tunnel route. **<precedence>** is the route weight, from 1 to 255; the default is 1.

Default: No IPv6 static route is configured.

Command Mode: Global Mode.

Usage Guidelines: If the next-hop IPv6 address is a link-local address, the interface name must be specified. If the next-hop IPv6 address is a global aggregatable unicast address or a site-local address and no egress interface is specified, the next-hop IP address must be in the same network segment as an interface address of the switch. For a tunnel route, the interface name can be specified directly.

Example: Configure static route 1 with destination 3ffe:589:dfc::88, prefix length 64, and next hop 2001:8fd:c32::99 (the router has IPv6 address 2001:8fd:c32::34/64 configured).

```
Switch(config)#ipv6 route 3ffe:589:dfc::88/64 2001:8fd:c32::99
```

Configure static route 2 with destination 3ffe:ff7:123::55, prefix length 64, next hop fe80::203:ff:89fd:46ac, and egress interface Vlan1.

```
Switch(config)#ipv6 route 3ffe:ff7:123::55/64 fe80::203:ff:89fd:46ac Vlan1
```

4.3.13 ipv6 redirect

Command: ipv6 redirect
no ipv6 redirect

Function: Enables IPv6 redirection. The **no** form of this command disables the function.

Parameters: None.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: If router A, router B, and node C are on the same link, and router A forwards IPv6 packets from node C to router B for further forwarding, router A sends an ICMPv6 redirect message to node C (the source of the packets), notifying it that router B is the best next hop for this destination. This reduces the forwarding load on router A and the transmission delay of node C.

Example: Enable IPv6 redirection.

```
Switch(config)# ipv6 redirect
```

4.3.14 ipv6 nd dad attempts

Command: ipv6 nd dad attempts <value>
no ipv6 nd dad attempts

Function: Sets the number of consecutive neighbor solicitation messages sent by the interface for duplicate address detection (DAD).

Parameters: <value> is the number of consecutive neighbor solicitation messages sent for DAD, from 0 to 10. The **no** form of this command restores the default of 1.

Command Mode: Interface Mode.

Default: 1.

Usage Guidelines: When an IPv6 address is configured, duplicate address detection is performed. Use this command to configure the number of ND messages sent for DAD; a value of 0 disables DAD.

Example: Set the number of consecutive neighbor solicitation messages sent for DAD to 3.

```
Switch(Config-if-Vlan1)# ipv6 nd dad attempts 3
```

4.3.15 ipv6 nd ns-interval

Command: ipv6 nd ns-interval <seconds>
no ipv6 nd ns-interval

Function: Sets the interval at which the interface sends neighbor solicitation messages.

Parameters: <seconds> is the interval for sending neighbor solicitation messages, from 1 to 3600 seconds. The **no** form of this command restores the default of 1 second.

Command Mode: Interface Mode.

Default: 1 second.

Usage Guidelines: The configured value is included in all router advertisements sent on the interface. A very short interval is generally not recommended.

Example: Set the neighbor solicitation interval of interface Vlan1 to 8 seconds.

```
Switch(Config-if-Vlan1)#ipv6 nd ns-interval 8
```

4.3.16 ipv6 nd suppress-ra

Command: **`ipv6 nd suppress-ra`**
`no ipv6 nd suppress-ra`

Function: Suppresses router advertisements.

Parameters: None.

Command Mode: Interface Mode.

Default: Router advertisement is disabled.

Usage Guidelines: The **no ipv6 nd suppress-ra** command enables router advertisement.

Example: Enable router advertisement.

```
Switch(Config-if-Vlan1)#no ipv6 nd suppress-ra
```

4.3.17 ipv6 nd ra-lifetime

Command: **`ipv6 nd ra-lifetime <seconds>`**
`no ipv6 nd ra-lifetime`

Function: Configures the router lifetime carried in router advertisements.

Parameters: **<seconds>** is the router lifetime in seconds, from 0 to 9000.

Command Mode: Interface Mode.

Default: 1800 seconds.

Usage Guidelines: Configures the router lifetime on the Layer 3 interface. A value of 0 means the interface cannot be used as a default router; otherwise, the value must not be less than the maximum router advertisement interval. If not configured, the value is three times the maximum router advertisement interval.

Example: Set the router advertisement lifetime to 100 seconds.

```
Switch(Config-if-Vlan1)#ipv6 nd ra-lifetime 100
```

4.3.18 ipv6 nd min-ra-interval

Command: **`ipv6 nd min-ra-interval <seconds>`**
`no ipv6 nd min-ra-interval`

Function: Sets the minimum interval for sending router advertisements.

Parameters: **<seconds>** is the minimum router advertisement interval, from 3 to 1350 seconds.

Command Mode: Interface Mode.

Default: 200 seconds.

Usage Guidelines: The minimum router advertisement interval must not exceed three quarters of the maximum interval.

Example: Set the minimum router advertisement interval to 10 seconds.

```
Switch(Config-if-Vlan1)#ipv6 nd min-ra-interval 10
```

4.3.19 ipv6 nd max-ra-interval

Command: **`ipv6 nd max-ra-interval <seconds>`**
`no ipv6 nd max-ra-interval`

Function: Sets the maximum interval for sending router advertisements.

Parameters: **<seconds>** is the maximum router advertisement interval, from 4 to 1800 seconds.

Command Mode: Interface Mode.

Default: 600 seconds.

Usage Guidelines: The maximum router advertisement interval must be less than the router advertisement lifetime.

Example: Set the maximum router advertisement interval to 20 seconds.

```
Switch(Config-if-Vlan1)#ipv6 nd max-ra-interval 20
```

4.3.20 ipv6 nd prefix

Command: ipv6 nd prefix <ipv6-prefix | prefix-length>{ [<valid-lifetime> <preferred-lifetime>] [no-autoconfig | off-link[no-autoconfig]]}
no ipv6 nd prefix <ipv6-prefix | prefix-length>

Function: Configures the address prefix and related parameters advertised in router advertisements.

Parameters: <ipv6-prefix> is the advertised address prefix. **<prefix-length>** is the prefix length. **<valid-lifetime>** is the valid lifetime of the prefix. **<preferred-lifetime>** is the preferred lifetime of the prefix; the valid lifetime must be greater than or equal to the preferred lifetime. **no-autoconfig** specifies that hosts on the local link cannot use this prefix for IPv6 address autoconfiguration. **off-link** specifies that the advertised prefix is not assigned to the local link, so nodes sending data to addresses with this prefix treat them as not reachable on the local link.

Command Mode: Interface Mode.

Default: The valid lifetime is 2592000 seconds (30 days) and the preferred lifetime is 604800 seconds (7 days). off-link and no-autoconfig are disabled.

Usage Guidelines: This command controls the router advertisement parameters of each IPv6 prefix. The valid lifetime and preferred lifetime must be configured together.

Example: Advertise prefix 2001:410:0:1::/64 on Vlan1 with a valid lifetime of 8640 seconds and a preferred lifetime of 4320 seconds.

```
Switch(Config-if-Vlan1)#ipv6 nd prefix 2001:410:0:1::/64 8640 4320
```

4.3.21 ipv6 nd ra-hoplimit

Command: ipv6 nd ra-hoplimit <value>

Function: Sets the hop limit advertised in router advertisements.

Parameters: <value> is the hop limit, from 0 to 255.

Command Mode: Interface Configuration Mode.

Default: 64.

Example: Set the router advertisement hop limit of interface vlan 1 to 128.

```
Switch#(Config-if-Vlan1)#ipv6 nd ra-hoplimit 128
```

4.3.22 ipv6 nd ra-mtu

Command: ipv6 nd ra-mtu <value>

Function: Sets the MTU advertised in router advertisements.

Parameters: <value> is the MTU, from 0 to 1500.

Command Mode: Interface Configuration Mode.

Default: 1500.

Example: Set the router advertisement MTU of interface vlan 1 to 500.

```
Switch#(Config-if-Vlan1)#ipv6 nd ra-mtu 500
```

4.3.23 ipv6 nd reachable-time

Command: `ipv6 nd reachable-time <seconds>`

Function: Sets the reachable time advertised in router advertisements.

Parameters: <seconds> is the reachable time, from 0 to 3600000 milliseconds.

Command Mode: Interface Mode.

Default: 30000 milliseconds.

Example: Set the router advertisement reachable time of interface vlan 1 to 100000 milliseconds.

```
Switch(Config-if-Vlan1)#ipv6 nd reachable-time 100000
```

4.3.24 ipv6 nd retrans-timer

Command: `ipv6 nd retrans-timer <seconds>`

Function: Sets the retransmission timer advertised in router advertisements.

Parameters: <seconds> is the retransmission timer, from 0 to 4294967295 milliseconds.

Command Mode: Interface Mode.

Default: 1000 milliseconds.

Example: Set the router advertisement retransmission timer of interface vlan 1 to 10000 milliseconds.

```
Switch(Config-if-Vlan1)#ipv6 nd retrans-timer 10000
```

4.3.25 ipv6 nd other-config-flag

Command: `ipv6 nd other-config-flag`

Function: Sets the flag indicating whether hosts obtain information other than addresses through DHCPv6.

Parameters: None.

Command Mode: Interface Mode.

Default: Hosts do not obtain information other than addresses through DHCPv6.

Example: Configure interface vlan 1 so that hosts obtain information other than addresses through DHCPv6.

```
Switch(Config-if-Vlan1)#ipv6 nd other-config-flag
```

4.3.26 ipv6 nd managed-config-flag

Command: `ipv6 nd managed-config-flag`

Function: Sets the flag indicating whether hosts obtain addresses through DHCPv6.

Parameters: None.

Command Mode: Interface Mode.

Default: Hosts do not obtain addresses through DHCPv6.

Example: Configure interface vlan 1 so that hosts obtain addresses through DHCPv6.

```
Switch(Config-if-Vlan1)#ipv6 nd managed-config-flag
```

4.3.27 ipv6 neighbor

Command: `ipv6 neighbor <ipv6-address> <hardware-address> interface <interface-type interface-name>`
`no ipv6 neighbor <ipv6-address>`

Function: Configures a static neighbor entry.

Parameters: <ipv6-address> is the IPv6 address of the static neighbor, which must match the interface prefix. **<hardware-address>** is the hardware address of the static neighbor. **<interface-type>** is the Ethernet type, and **<interface-name>** is the Layer 2 interface name.

Command Mode: Interface Mode.

Default: No static neighbor entry is configured.

Usage Guidelines: Special-purpose IPv6 addresses, multicast addresses, and local addresses cannot be configured as neighbors.

Example: Configure static neighbor 2001:1:2::4 on port E1/0/1 with hardware MAC address 00-03-0f-89-44-bc.

```
Switch(Config-if-Vlan1)#ipv6 neighbor 2001:1:2::4 00-03-0f-89-44-bc interface
Ethernet 1/0/1
```

4.3.28 interface tunnel

Command: `interface tunnel <tnl-id>`
`no interface tunnel <tnl-id>`

Function: Creates or deletes a tunnel.

Parameters: <tnl-id> is the tunnel number.

Command Mode: Global Mode.

Default: None.

Usage Guidelines: This command creates a virtual tunnel interface. Because no tunnel mode or tunnel source has been specified yet, the **show ipv6 tunnel** command does not display the tunnel. After creating the tunnel, the switch enters Tunnel Mode, where you can specify the tunnel source and destination. The **no** form of this command deletes the tunnel.

Example: Create tunnel 1.

```
Switch(Config)#interface tunnel 1
```

4.3.29 show ip interface

Command: `show ip interface [<ifname> | vlan <vlan-id>] brief`

Function: Displays brief information about configured Layer 3 interfaces.

Parameters: <ifname>: The interface name. **<vlan-id>**: The VLAN ID.

Default: If no parameter is specified, brief information about all configured Layer 3 interfaces is displayed.

Command Mode: All Modes.

Usage Guidelines: None.

Example:

```
Restarter#show ip interface vlan1 brief
Index     Interface            IP-Address      Protocol
3001      Vlan1              192.168.2.11     up
```

4.3.30 show ip traffic

Command: `show ip traffic`

Function: Displays IP packet statistics.

Command Mode: Admin Mode.

Usage Guidelines: Displays statistics of IP, ICMP, TCP, and UDP packets received and sent.

Example:

```
Switch#show ip traffic
IP statistics:
Rcvd:  3249810 total, 3180 local destination
0 header errors, 0 address errors
0 unknownnnnn protocol, 0 discards
Frags:  0 reassembled, 0 timeouts
0 fragment rcvd, 0 fragment dropped
0 fragmented, 0 couldn't fragment, 0 fragment sent
Sent:   0 generated, 3230439 forwarded
0 dropped, 0 no route
ICMP statistics:
Rcvd:  0 total 0 errors 0 time exceeded
0 redirects, 0 unreachable, 0 echo, 0 echo replies
0 mask requests, 0 mask replies, 0 quench
0 parameter, 0 timestamp, 0 timestamp replies
Sent:   0 total 0 errors 0 time exceeded
0 redirects, 0 unreachable, 0 echo, 0 echo replies
0 mask requests, 0 mask replies, 0 quench
0 parameter, 0 timestamp, 0 timestamp replies
TCP statistics:
TcpActiveOpens          0, TcpAttemptFails          0
TcpCurrEstab            0, TcpEstabResets           0
TcpInErrs               0, TcpInSegs                3180
TcpMaxConn            0, TcpOutRsts               3
TcpOutSegs             0, TcpPassiveOpens           8
TcpRetransSegs          0, TcpRtoAlgorithm           0
TcpRtoMax             0, TcpRtoMin                0
UDP statics:
UdpInDatagrams         0, UdpInErrors              0
UdpNoPorts             0, UdpOutDatagrams          0
```

Field	Description
IP statistics：	IP packet statistics
Rcvd: 3249810 total, 3180 local destination 0 header errors, 0 address errors 0 unknown protocol, 0 discards	Statistics of received packets: total packets received, packets destined for the local device, packets with header errors, packets with address errors, packets of unknown protocols, and packets discarded.
Frags： 0 reassembled, 0 timeouts 0 fragment rcvd, 0 fragment dropped 0 fragmented, 0 couldn't fragment, 0 fragment sent	Fragmentation statistics: packets reassembled, reassembly timeouts, fragments received, fragments discarded, packets fragmented, packets that could not be fragmented, and fragments sent.
Sent： 0 generated, 0 forwarded 0 dropped, 0 no route	Statistics of sent packets: packets generated locally, packets forwarded, packets dropped, and packets with no route.
ICMP statistics：	ICMP packet statistics
Rcvd： 0 total 0 errors 0 time exceeded 0 redirects, 0 unreachable, 0 echo, 0 echo replies 0 mask requests, 0 mask replies, 0 quench 0 parameter, 0 timestamp, 0 timestamp replies	Statistics of ICMP packets received, by type
Sent： 0 total 0 errors 0 time exceeded 0 redirects, 0 unreachable, 0 echo, 0 echo replies 0 mask requests, 0 mask replies, 0 quench 0 parameter, 0 timestamp, 0 timestamp replies	Statistics of ICMP packets sent, by type
TCP statistics:	TCP packet statistics

UDP statistics:	UDP packet statistics

4.3.31 show ipv6 interface

Command: `show ipv6 interface {brief|<interface-name>}`

Function: Displays the IPv6 parameters of interfaces.

Parameters: brief displays a brief summary of IPv6 status and configuration; **<interface-name>** is the Layer 3 interface name.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: If **brief** is specified, information about all Layer 3 interfaces is displayed; you can also specify a Layer 3 interface.

Example:

```
Switch#show ipv6 interface Vlan1
Vlan1 is up, line protocol is up, dev index is 2004
Device flag 0x1203(UP BROADCAST ALLMULTI MULTICAST)
IPv6 is enabled
Link-local address(es):
fe80::203:fff:fe00:10  PERMANENT
Global unicast address(es):
3001::1                                    subnet is 3001::1/64  PERMANENT
Joined group address(es):
ff02::1
ff02::16
ff02::2
ff02::5
ff02::6
ff02::9
ff02::d
ff02::1:ff00:10
ff02::1:ff00:1
MTU is 1500 bytes
ND DAD is enabled,    number of DAD attempts is 1
ND managed_config_flag is unset
ND other_config_flag is unset
ND NS interval is 1 second(s)
ND router advertisements is disabled
ND RA min-interval is 200 second(s)
ND RA max-interval is 600 second(s)
ND RA hoplimit is 64
ND RA lifetime is 1800 second(s)
ND RA MTU is 0
ND advertised reachable time is 0 millisecond(s)
ND advertised retransmit time is 0 millisecond(s)
```

Field	Description
Vlan1	Layer 3 interface name
[up/up]	Layer 3 interface status
dev index	Internal index number
fe80::203:fff:fe00:10	Automatically configured IPv6 address of the Layer 3 interface
3001::1	Configured IPv6 address of the Layer 3 interface

4.3.32 show ipv6 route

Command: show ipv6 route [<destination>|<destination >|<length>| database| fib [local]| nsm [connected | static | rip| ospf | bgp | isis| kernel| database]|statistics]

Function: Displays the IPv6 routing table.

Parameters: <destination> is the destination network address. **<destination>/<length>** is the destination network address and prefix length. **connected**: directly connected routes. **static**: static routes. **rip**: RIP routes. **ospf**: OSPF routes. **bgp**: BGP routes. **isis**: IS-IS routes. **kernel**: kernel routes. **statistics**: displays the number of routes. **database**: the route database.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: show ipv6 route displays only the IPv6 kernel routing table (the TCP/IP routing table). **database** displays all routes except local routes, **fib local** displays local routes, and **statistics** displays route statistics.

Example:

```
Switch#show ipv6 route
Codes: C - connected, L - Local, S - static, R - RIP, O - OSPF,
I - IS-IS, B - BGP
C    ::/0    via ::,   tunnel3   256
S    2001:2::/32    via fe80::789,   Vlan2   1024
S    2001:2:3:4::/64    via fe80::123,   Vlan2   1024
O    2002:ca60:c801:1::/64    via ::,   Vlan1   1024
C    2002:ca60:c802:1::/64    via ::,   tunnel49   256
C    2003:1::/64    via ::,   Vlan4   256
C    2003:1::5efe:0:0/96    via ::,   tunnel26   256
S    2004:1:2:3::/64    via fe80:1::88,   Vlan2   1024
O    2006:1::/64    via ::,   Vlan1   1024
S    2008:1:2:3::/64    via fe80::250:baff:fef2:a4f4,   Vlan1   1024
C    2008:2005:5:8::/64    via ::,   Ethernet0   256
S    2009:1::/64    via fe80::250:baff:fef2:a4f4,   Vlan1   1024
C    2022:1::/64    via ::,   Ethernet0   256
O    3333:1:2:3::/64    via fe80::20c:ceff:fe13:eac1,   Vlan12   1024
C    3ffe:501:ffff:1::/64    via ::,   Vlan4   256
O    3ffe:501:ffff:100::/64    via ::,   Vlan5   1024
O    3ffe:3240:800d:1::/64    via ::,   Vlan1   1024
O    3ffe:3240:800d:2::/64    via ::,   Vlan2   1024
O    3ffe:3240:800d:10::/64    via ::,   Vlan12   1024
O    3ffe:3240:800d:20::/64    via fe80::20c:ceff:fe13:eac1,   Vlan12   1024
C    fe80::/64    via ::,   Vlan1   256
C    fe80::5efe:0:0/96    via ::,   tunnel26   256
C    ff00::/8    via ::,   Vlan1   256
```

Field	Description
IPv6 Routing Table	IPv6 routing table status
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,I - IS-IS, B - BGP > - selected route, * - FIB route, p - stale info	Codes used to mark each entry
S 2009:1::/64 via fe80::250:baff:fef2:a4f4, Vlan1 1024	A static route in the FIB: the destination network segment is 2009:1::/64, the next hop (via) is fe80::250:baff:fef2:a4f4, the egress interface is Vlan1, and the route weight is 1024.

4.3.33 show ipv6 neighbors

Command: show ipv6 neighbors [{vlan|ethernet|tunnel } interface-number | interface-name | address <ipv6address>]

Function: Displays neighbor table entries.

Parameters: {vlan|ethernet|tunnel} interface-number | interface-name looks up entries by interface. **address <ipv6address>** looks up entries by IPv6 address. If no parameter is specified, all neighbor table entries are displayed.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: None.

Example:

```
Switch#show ipv6 neighbors
IPv6 neighbour unicast items: 14, valid: 11, matched: 11, incomplete: 0,
delayed: 0,
manage items 5
IPv6 Address                            Hardware Addr         Interface
Port            State
2002:ca60:c801:1:250:baff:fef2:a4f4     00-50-ba-f2-a4-f4     Vlan1
Ethernet1/0/2     reachable
3ffe:3240:800d:1::100                   00-03-0f-01-27-86     Vlan1
Ethernet1/0/3     reachable
3ffe:3240:800d:1::8888                  00-02-01-00-00-00     Vlan1
Ethernet1/0/1     permanent
3ffe:3240:800d:1:250:baff:fef2:a4f4     00-50-ba-f2-a4-f4     Vlan1
Ethernet1/0/4     reachable
3ffe:3240:800d:2::8888                  00-02-01-00-01-01     Vlan2
Ethernet1/0/16    permanent
3ffe:3240:800d:2:203:fff:fefe:3045      00-03-0f-fe-30-45     Vlan2
Ethernet1/0/15    reachable
fe80::203:fff:fe01:2786                 00-03-0f-01-27-86     Vlan1
Ethernet1/0/5     reachable
fe80::203:fff:fefe:3045                 00-03-0f-fe-30-45     Vlan2
Ethernet1/0/17    reachable
fe80::20c:ceff:fe13:eac1                00-0c-ce-13-ea-c1     Vlan12
Ethernet1/0/20    reachable
fe80::250:baff:fef2:a4f4                00-50-ba-f2-a4-f4     Vlan1
Ethernet1/0/6     reachable
IPv6 neighbour table: 11 entries
```

Field	Description
IPv6 Address	IPv6 address of the neighbor
Hardware Addr	MAC address of the neighbor
Interface	Egress Layer 3 interface name
Port	Egress port name
State	Neighbor state (reachable, stale, delay, probe, permanent, incomplete, or unknown)

4.3.34 show ipv6 traffic

Command: show ipv6 traffic

Function: Displays IPv6 packet statistics.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch#show ipv6 traffic
IP statistics:
Rcvd:  90 total, 17 local destination
0 header errors, 0 address errors
0 unknownnnnn protocol, 13 discards
Frags: 0 reassembled, 0 timeouts
0 fragment rcvd, 0 fragment dropped
0 fragmented, 0 couldn't fragment, 0 fragment sent
Sent:  110 generated, 0 forwarded
0 dropped, 0 no route
ICMP statistics:
Rcvd:  0 total 0 errors 0 time exceeded
0 redirects, 0 unreachable, 0 echo, 0 echo replies
```

Field	Description
IP statistics	IPv6 packet statistics
Rcvd: 90 total, 17 local destination0 header errors, 0 address errors0 unknown protocol, 13 discards	Statistics of IPv6 packets received
Frags: 0 reassembled, 0 timeouts 0 fragment rcvd, 0 fragment dropped0 fragmented, 0 couldn't fragment, 0 fragment sent	IPv6 fragmentation statistics
Sent: 110 generated, 0 forwarded 0 dropped, 0 no route	Statistics of IPv6 packets sent

4.3.35 show ipv6 redirect

Command: `show ipv6 redirect`

Function: Displays the state of the IPv6 redirection function.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Use this command to check whether IPv6 redirection is enabled.

Example:

```
Switch show ipv6 redirect
ipv6 redirect is disabled
```

4.3.36 show ipv6 tunnel

Command: `show ipv6 tunnel [<tnl-id>]`

Function: Displays tunnel information.

Parameters: <tnl-id> is the tunnel number.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: If no tunnel number is specified, information about all tunnels is displayed. If a tunnel number is specified, detailed information about that tunnel is displayed.

Example:

```
Switch#show ipv6 tunnel
name      mode      source              destination          nexthop
tunnel3      6to4      178.1.1.1
```

Field	Description

Name	Tunnel name
Mode	Tunnel type
Source	Tunnel source IPv4 address
Destination	Tunnel destination IPv4 address
Nexthop	Tunnel next hop (applies only to ISATAP tunnels)

4.3.37 tunnel source

Command: `tunnel source {<ipaddress> | <ipv6address> | <interface-name>}`
`no tunnel source`

Function: Configures the IPv4 or IPv6 address of the tunnel source.

Parameters: <ipaddress> is the IPv4 address of the tunnel source, which must be a unicast address. **<ipv6address>** is the IPv6 address of the tunnel source. **<interface-name>** specifies that the tunnel source address is the IPv4 address of this interface.

Command Mode: Tunnel Mode.

Default: No tunnel source address or interface is configured.

Usage Guidelines: Configure the tunnel by setting the source IPv4 or IPv6 address or specifying an interface whose address is used as the tunnel source address.

Example: Set the tunnel source IPv4 address to 202.89.176.6.

```
Switch(Config-if-Tunnel1)#tunnel source 202.89.176.6
```

4.3.38 tunnel destination

Command: `tunnel destination <ipaddress | ipv6address>`
`no tunnel destination`

Function: Configures the IPv4 or IPv6 address of the tunnel destination.

Parameters: <ipaddress> is the IPv4 address of the tunnel destination. **<ipv6address>** is the IPv6 address of the tunnel destination.

Command Mode: Tunnel Mode.

Default: No tunnel destination address is configured.

Usage Guidelines: Use this command to configure the IPv4 or IPv6 address of the tunnel destination.

Example: Set the tunnel destination to 203.78.120.5.

```
Switch(Config-if-Tunnel1)#tunnel destination 203.78.120.5
```

4.3.39 tunnel nexthop

Command: `tunnel nexthop <ipaddress>`
`no tunnel nexthop`

Function: Configures the tunnel next hop.

Parameters: <ipaddress> is the IPv4 address of the tunnel next hop.

Command Mode: Tunnel Mode.

Default: No tunnel next-hop IPv4 address is configured.

Usage Guidelines: This command applies to ISATAP tunnels; other tunnel types do not check the next-hop configuration. Note: The IPv4 address of the ISATAP tunnel next hop must be in the same network segment as the IPv4 address of the tunnel source.

Example: Set the tunnel next hop to 178.99.156.8.

```
Switch(Config-if-Tunnel1)#tunnel source 178.99.156.7
Switch(Config-if-Tunnel1)#tunnel nexthop 178.99.156.8
Switch(Config-if-Tunnel1)#tunnel mode ipv6ip isatap
```

4.3.40 tunnel mode

Command: `tunnel mode [[gre] | ipv6ip [6to4 | isatap]]`
`no tunnel mode`

Function: Configures the tunnel mode.

Parameters: gre: GRE tunnel. **ipv6ip**: IPv6-over-IPv4 tunnel. **6to4**: 6to4 tunnel. **isatap**: ISATAP tunnel.

Command Mode: Tunnel Mode.

Default: None.

Usage Guidelines: Specifying only **ipv6ip** configures a configured (manual) tunnel; **ipv6ip 6to4** configures a 6to4 tunnel; **ipv6ip isatap** configures an ISATAP tunnel.

Example: Configure the tunnel mode.

```
1、Switch(Config-if-Tunnel1)#tunnel mode ipv6ip
2、Switch(Config-if-Tunnel1)#tunnel mode ipv6ip 6to4
3、Switch(Config-if-Tunnel1)#tunnel mode ipv6ip isatap
```

4.4 IP Forwarding

4.4.1 ip fib optimize

Command: `ip fib optimize`
`no ip fib optimize`

Function: Enables the optimized IP route aggregation algorithm. The **no ip fib optimize** command disables it.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: This command optimizes the aggregation algorithm: if the routing table contains no default route, the most frequently used next hop is used to construct a virtual default route that simplifies the aggregation result. This simplifies the aggregation result more effectively. However, while adding a virtual default route to the chip's route table reduces CPU load, it may send unnecessary traffic to next-hop switches; in effect, part of the local CPU load is shifted to the next-hop switches.

Example: Disable the optimized IP route aggregation algorithm.

```
Switch(config)# no ip fib optimize
```

4.5 URPF

4.5.1 debug urpf

Command: `debug urlf`

Function: Enables URPF debugging, which reports an error when URPF rule installation fails. The **no** form of this command disables the debugging.

Command Mode: Admin Mode.

Parameters: None.

Usage Guidelines: None.

Example:

```
Switch#debug urpf
```

4.5.2 show urpf

Command: **`show urpf`**

Function: Displays the interfaces on which URPF is enabled.

Command Mode: Admin Mode and Configuration Mode.

Parameters: None.

Usage Guidelines: None.

Example:

```
Switch#show urpf
```

4.5.3 urpf enable

Command: **`urpf enable`**
`no urpf enable`

Function: Enables URPF globally. The **no** form of this command disables it.

Parameters: None.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: None.

Example:

```
Switch(config)#urpf enable
```

4.6 ARP

4.6.1 arp

Command: **`arp <ip_address> <mac_address> {interface [ethernet] <portName>}`**
`no arp <ip_address>`

Function: Configures a static ARP entry. The **no arp <ip_address>** command deletes the ARP entry of the specified IP address.

Parameters: **<ip_address>** is the IP address, which must be in the same subnet as the interface address. **<mac_address>** is the MAC address. **ethernet** specifies an Ethernet port. **<portName>** is the name of the Layer 2 port.

Default: No static ARP entry is configured.

Command Mode: VLAN Interface Mode.

Usage Guidelines: Static ARP entries can be configured on the switch.

Example: Configure a static ARP entry on interface VLAN 1.

```
Switch(Config-if-Vlan1)#arp 1.1.1.1 00-03-0f-f0-12-34 interface eth 1/0/2
```

4.6.2 clear arp-cache

Command: `clear arp-cache`

Function: Clears the ARP table.

Command Mode: Admin Mode.

Example:

```
Switch#clear arp-cache
```

4.6.3 clear arp traffic

Command: `clear arp traffic`

Function: Clears ARP message statistics of the switch. On box switches, this command clears only the statistics of ARP messages received and sent by the current card.

Command Mode: Admin Mode.

Example:

```
Switch#clear arp traffic
```

4.6.4 debug arp

Command: `debug arp {receive|send|state}`
`no debug arp {receive|send|state}`

Function: Enables ARP debugging. The **no debug arp {receive|send|state}** command disables this debugging.

Parameters: receive: Debugging of ARP packets received by the switch. **send**: Debugging of ARP packets sent by the switch. **state**: Debugging of ARP state changes on the switch.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Displays the contents of ARP packets received and sent, including the type and the source and destination addresses.

Example: Enable ARP debugging.

```
Switch#debug arp receive
%Jan 01 01:05:53 2006 IP ARP: rcvd, type REQUEST, src 172.16.1.251, 00-e0-4c-
88-ad-bc, dst 172.16.1.110, 00-00-00-00-00-00 flag 0x0, pkt type 1, intf
Vlan100.
%Jan 01 01:05:53 2006 IP ARP: rcvd, type REQUEST, src 172.16.1.251, 00-e0-4c-
88-ad-bc, dst 172.16.1.110, 00-00-00-00-00-00 flag 0x0, pkt type 1, intf
Vlan100.
e%Jan 01 01:05:53 2006 IP ARP: rcvd, type REQUEST, src 172.16.1.251, 00-e0-
4c-88-ad-bc, dst 172.16.1.110, 00-00-00-00-00-00 flag 0x0, pkt type 1, intf
Vlan100.
%Jan 01 01:05:53 2006 IP ARP: rcvd, type REQUEST, src 172.16.1.251, 00-e0-4c-
88-ad-bc, dst172.16.1.110, 00-00-00-00-00-00 flag 0x0, pkt type 1, intf
Vlan100.
```

4.6.5 clear ip arp dynamic

Command: `clear ip arp dynamic`

Function: Clears all dynamic ARP entries on the interface.

Parameters: None.

Command Mode: Interface Mode.

Usage Guidelines: This command clears dynamic entries before ARP binding. It takes effect once when executed and is not retained in the configuration.

Example:

```
Switch(Config-if-Vlan1)#clear ip arp dynamic
```

4.6.6 clear ipv6 nd dynamic

Command: `clear ipv6 nd dynamic`

Function: Clears all dynamic ND entries on the interface.

Parameters: None.

Command Mode: Interface Mode.

Usage Guidelines: This command clears dynamic entries before ND binding. It takes effect once when executed and is not retained in the configuration.

Example:

```
Switch(Config-if-Vlan1)#clear ipv6 nd dynamic
```

4.6.7 ip proxy-arp

Command: `ip proxy-arp`
`no ip proxy-arp`

Function: Enables proxy ARP on the VLAN interface. The **no** form of this command disables proxy ARP.

Default: Disabled.

Command Mode: VLAN Interface Mode.

Usage Guidelines: When a Layer 3 interface with proxy ARP enabled receives an ARP request for an IP address in the same IP subnet as the interface but on a different physical network, the interface replies with its own MAC address and forwards the packets it then receives. This allows hosts that are physically separated but in the same IP subnet to communicate through the proxy ARP interface as if they were on the same physical network. Before replying to an ARP request, proxy ARP checks the routing table to determine whether the destination network is reachable, and replies only if it is.

Note: Proxy ARP is not used for ARP requests that match the default route.

Example: Enable proxy ARP on VLAN 1.

```
Switch(Config-if-Vlan1)#ip proxy-arp
```

4.6.8 show arp

Command: `show arp [<ipaddress>] [<vlan-id>] [<hw-addr>] [type {static | dynamic}] [count] [vrf word]`

Function: Displays the ARP table.

Parameters: **<ipaddress>** displays the entry with the specified IP address. **<vlan-id>** displays entries of the specified VLAN. **<hw-addr>** displays the entry with the specified MAC address. **static** displays static ARP entries. **dynamic** displays dynamic ARP entries. **count** displays the number of ARP entries. **word** is the VRF name.

Command Mode: Admin Mode.

Usage Guidelines: Displays the current ARP table, including the IP address, MAC address, hardware type, and interface name.

Example:

```
Switch#show arp
ARP Unicast Items: 7, Valid: 7, Matched: 7, Verifying: 0, Incomplete: 0,
Failed: 0, None: 0
Address          Hardware Addr      Interface     Port            Flag
50.1.1.6         00-0a-eb-51-51-38  Vlan50        Ethernet1/0/11     Dynamic
```

```
50.1.1.9          00-00-00-00-00-09    Vlan50      Ethernet1/0/1      Static
150.1.1.2         00-00-58-fc-48-9f       Vlan150     Ethernet1/0/4
Dynamic
```

Field	Description
Total arp items	Total number of ARP entries
Valid	Number of ARP entries that match the filter conditions and are valid
Matched	Number of ARP entries that match the filter conditions
Verifying	Number of ARP entries whose validity is being re-verified
InCompleted	Number of ARP entries for which an ARP request was sent but no reply was received
Failed	Number of ARP entries in the failed state
None	Number of ARP entries in the initial state
Address	IP address of the ARP entry
Hardware Address	MAC address of the ARP entry
Interface	Layer 3 interface of the ARP entry
Port	Physical (Layer 2) port of the ARP entry
Flag	Whether the ARP entry is dynamic or static

4.6.9 show arp traffic

Command: `show arp traffic`

Function: Displays ARP message statistics of the switch. On box switches, this command displays only the statistics of ARP messages received and sent by the current card.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays statistics of ARP messages received and sent.

Example:

```
Switch#show arp traffic
ARP statistics:
  Rcvd:  10 request, 5 response
  Sent:   5 request, 10 response
```

4.7 Hardware Tunnel Capacity

4.7.1 hardware tunnel-capacity

Command: `hardware tunnel-capacity <size>`
`no hardware tunnel-capacity`

Function: Configures the maximum hardware tunnel capacity. The **no** form of this command restores the default.

Parameters: <size> is the hardware tunnel capacity, from 0 to 1024.

Default: 64.

Command Mode: Global Mode.

Usage Guidelines: Configures the maximum number of tunnel and MPLS entries forwarded in hardware. Increasing this capacity reduces the number of hardware routes supported by the switch, and vice versa.

Note: The switch must be restarted for the configuration to take effect.

Example: Set the maximum hardware tunnel capacity to 200.

```
Switch(config)#hardware tunnel-capacity 200
Set successfully! Write and reload to take effect.
Switch(config)#exit
Switch#write
Switch#reload
```

4.8 ARP Scanning Prevention

4.8.1 anti-arpscan enable [ip|port]

Command: anti-arpscan enable [ip|port]
no anti-arpscan enable [ip|port]

Function: Enables ARP scanning prevention globally. The **no anti-arpscan enable** command disables it globally.

Parameters: ip: IP-based prevention. **port**: Port-based prevention.

Default: Port-based and IP-based ARP scanning prevention are enabled or disabled together.

Command Mode: Global Mode.

Usage Guidelines: When managing the switch remotely (for example, through Telnet), set the uplink port as a super trusted port before enabling ARP scanning prevention so that the port is not shut down for receiving too many ARP messages. After ARP scanning prevention is disabled, the port returns to its default attribute (untrusted).

Example: Enable ARP scanning prevention on the switch.

```
Switch(config)#anti-arpscan enable ip
```

4.8.2 anti-arpscan port-based threshold

Command: anti-arpscan port-based threshold <threshold-value>
no anti-arpscan port-based threshold

Function: Sets the threshold for port-based ARP scanning prevention. If the rate of ARP messages received on a port exceeds the threshold, the port is shut down. The unit is packets per second. The **no anti-arpscan port-based threshold** command restores the default of 10 packets per second.

Parameters: <threshold-value>: The rate threshold, from 2 to 200.

Default: 10 packets per second.

Command Mode: Global Mode.

Usage Guidelines: The port-based threshold must be greater than the IP-based threshold; otherwise, IP-based ARP scanning prevention does not work.

Example: Set the port-based ARP scanning prevention threshold to 10 packets per second.

```
Switch(config)#anti-arpscan port-based threshold 10
```

4.8.3 anti-arpscan ip-based threshold

Command: anti-arpscan ip-based threshold <threshold-value>
no anti-arpscan ip-based level1|level2 threshold

Function: Sets the threshold for IP-based ARP scanning prevention. The default level-1 threshold is 4 packets per second.

Parameters: <threshold-value>: The rate threshold, from 1 to 200.

Default: The level-1 threshold is 4 packets per second.

Command Mode: Global Mode.

Usage Guidelines: The port-based threshold must be greater than the IP-based threshold; otherwise, IP-based ARP scanning prevention does not work.

Example: Set the IP-based ARP scanning prevention threshold to 6 packets per second.

```
Switch(Config)# anti-arpscan ip-based threshold 6
```

4.8.4 anti-arpscan trust

Command: anti-arpscan trust { port | supertrust-port | iptrust-port }
no anti-arpscan trust {port | supertrust-port | iptrust-port}

Function: Configures a port as a trusted, super trusted, or IP-trusted port. The **no** form of this command resets the port to untrusted.

Parameters: port: Trusted port. **supertrust-port**: Super trusted port. **iptrust-port**: IP-trusted port.

Default: All ports are untrusted.

Command Mode: Port Mode.

Usage Guidelines: ARP scanning prevention does not act on a trusted port: even if the rate of ARP messages received exceeds the threshold, the port is not shut down, but untrusted IP addresses on the port are still checked. ARP scanning prevention acts on neither a super trusted port nor its IP addresses. If a port has already been shut down by ARP scanning prevention, it is reopened immediately when it is set as a trusted port. On an IP-trusted port, IP addresses are not checked but the port is. If an IP address has already been blocked by ARP scanning prevention, it is unblocked immediately when the port is set as an IP-trusted port.

When managing the switch remotely (for example, through Telnet), set the uplink port as a super trusted port before enabling ARP scanning prevention so that the port is not shut down for receiving too many ARP messages. After ARP scanning prevention is disabled, the port returns to its default attribute (untrusted).

Example: Set port ethernet 1/0/5 as a trusted port.

```
Switch(config)#in e1/0/5
Switch(Config-If-Ethernet1/0/5)# anti-arpscan trust port
```

4.8.5 anti-arpscan trust ip

Command: anti-arpscan trust ip <ip-address> [<netmask>]
no anti-arpscan trust ip <ip-address> [<netmask>]

Function: Configures a trusted IP address. The **no anti-arpscan trust ip <ip-address> [<netmask>]** command resets the IP address to untrusted.

Parameters: <ip-address>: The trusted IP address. **<netmask>**: The network mask of the IP address.

Default: All IP addresses are untrusted. The default mask is 255.255.255.255.

Command Mode: Global Mode.

Usage Guidelines: ARP scanning prevention does not act on trusted IP addresses: even if the rate of ARP messages received from a trusted IP address exceeds the threshold, it is not blocked. If the IP address has already been blocked by ARP scanning prevention, its traffic is restored immediately.

Example: Set 192.168.1.0/24 as a trusted IP range.

```
Switch(config)#anti-arpscan trust ip 192.168.1.0 255.255.255.0
```

4.8.6 anti-arpscan recovery enable

Command: `anti-arpscan recovery enable`
`no anti-arpscan recovery enable`

Function: Enables automatic recovery. The **no anti-arpscan recovery enable** command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Configure this function if ports shut down by ARP scanning prevention should return to normal after a period of time.

Example: Enable automatic recovery on the switch.

```
Switch(config)#anti-arpscan recovery enable
```

4.8.7 anti-arpscan recovery time

Command: `anti-arpscan recovery time <seconds>`
`no anti-arpscan recovery time`

Function: Configures the automatic recovery time. The **no anti-arpscan recovery time** command restores the default.

Parameters: <seconds>: The automatic recovery time, from 5 to 86400 seconds.

Default: 300 seconds.

Command Mode: Global Mode.

Usage Guidelines: Enable automatic recovery first.

Example: Set the automatic recovery time to 3600 seconds.

```
Switch(config)#anti-arpscan recovery time 3600
```

4.8.8 anti-arpscan log enable

Command: `anti-arpscan log enable`
`no anti-arpscan log enable`

Function: Enables ARP scanning prevention logging. The **no anti-arpscan log enable** command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: After logging is enabled, you can check detailed information about ports shut down or automatically recovered, and IP addresses blocked or unblocked, by ARP scanning prevention. The log level is Warning.

Example: Enable ARP scanning prevention logging on the switch.

```
Switch(config)#anti-arpscan log enable
```

4.8.9 anti-arpscan trap enable

Command: `anti-arpscan trap enable`
`no anti-arpscan trap enable`

Function: Enables ARP scanning prevention SNMP traps. The **no anti-arpscan trap enable** command disables them.

Parameters: None.

Default: Level-1 rate-limiting and level-2 isolation traps are disabled.

Command Mode: Global Mode.

Usage Guidelines: After ARP scanning prevention SNMP traps are enabled, a trap is sent whenever a port or IP address is blocked or unblocked by ARP scanning prevention.

Example: Enable ARP scanning prevention SNMP traps on the switch.

```
Switch(config)#anti-arpscan trap enable
```

4.8.10 anti-arpscan FFP max-num <num>

Command: `anti-arpscan FFP max-num <num>`

Function: Sets the maximum number of FFP entries that ARP scanning prevention can use.

Parameters: <num>: From 1 to 1024. The default is 200.

Command Mode: Global Mode.

Usage Guidelines: If a port receives ARP packets from more source IP addresses than the maximum and the ARP rate of each source IP exceeds the level-1 or level-2 threshold, you can set a higher value after the FFP resources are exhausted.

Example: Set the maximum number of FFP entries to 1024.

```
Switch(config)#anti-arpscan ffp max-num 1024
```

4.8.11 debug anti-arpscan

Command: `debug anti-arpscan [port | ip]`
`no debug anti-arpscan [port | ip]`

Function: Enables ARP scanning prevention debugging. The **no debug anti-arpscan [port | ip]** command disables it.

Parameters: port: Port-based debugging. **ip**: IP-based debugging.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: After debugging is enabled (globally, or separately for port-based or IP-based prevention), you can check debugging information whenever a port or IP address is blocked or automatically recovered by ARP scanning prevention.

Example: Enable ARP scanning prevention debugging on the switch.

```
Switch#debug anti-arpscan
```

4.8.12 show anti-arpscan

Command: `show anti-arpscan [trust {ip | port | supertrust-port | iptrust-port} |prohibited {ip | port}]`

Function: Displays operating information of ARP scanning prevention.

Parameters: trust displays trusted entries of the specified type; **prohibited** displays blocked IP addresses or ports.

Default: Displays whether each port is trusted and whether it is shut down (and if so, for how long), and all trusted and blocked IP addresses.

Command Mode: Admin Mode.

Usage Guidelines: To display only trusted ports, use **show anti-arpscan trust port**; the other options work the same way.

Example: Check the operating state of ARP scanning prevention after it is enabled.

```
Switch(config)#show anti-arpscan
Total port: 28
Name          Port-property  beShut  shutTime(seconds)
Ethernet1/0/1      untrust        N       0
Ethernet1/0/2      untrust        N       0
Ethernet1/0/3      untrust        N       0
Ethernet1/0/4      untrust        N       0
Ethernet1/0/5      untrust        N       0
Ethernet1/0/6      untrust        N       0
Ethernet1/0/7      untrust        N       0
Ethernet1/0/8      untrust        N       0
Ethernet1/0/9      untrust        N       0
Ethernet1/0/10     untrust        N       0
Ethernet1/0/11     untrust        N       0
Ethernet1/0/12     untrust        N       0
Ethernet4/1      untrust        N       0
Ethernet4/2      untrust        N       0
Ethernet4/3      untrust        N       0
Ethernet4/4      trust          N       0
Ethernet4/5      untrust        N       0
Ethernet4/6      supertrust     N       0
Ethernet4/7      untrust        Y       30
Ethernet4/8      trust          N       0
Ethernet4/9      untrust        N       0
Ethernet4/10     untrust        N       0
Ethernet4/11     untrust        N       0
Ethernet4/12     untrust        N       0
Ethernet4/13     untrust        N       0
Ethernet4/14     untrust        N       0
Ethernet4/15     untrust        N       0
Ethernet4/16     untrust        N       0
Ethernet4/17     untrust        N       0
Ethernet4/18     untrust        N       0
Ethernet4/19     untrust        N       0
Ethernet4/20     untrust        N       0
Ethernet4/21     untrust        N       0
Ethernet4/22     untrust        N       0
Ethernet4/23     untrust        N       0
Ethernet4/24     untrust        N       0
Prohibited IP:
IP               shutTime(seconds)
1.1.1.2          132
Trust IP:
192.168.99.5     255.255.255.255
192.168.99.6     255.255.255.255
```

4.8.13 show anti-arpscan ip-based attack-list [history]

Command: `show anti-arpscan ip-based attack-list [history]`

Function: Displays information about current or past sources of ARP scanning attacks.

Parameters: history: Displays historical attack source information.

Default: Displays current attack source information.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: (1) Displays current attack source information, including the source IP address, port, VLAN, rate, and state. If the rate exceeds the level-1 threshold, the state is Speed-Limit. If it exceeds the level-2 threshold and the action is discard-arp, the state is Discard-Arp; if the action is isolate, the state is Isolate.

(2) Displays historical attack source information, including the source IP address, port, VLAN, number of attacks, state of the last attack, and duration. The states are the same as above.

Example:

```
Switch#show anti-arpscan ip-based attack-list
SIP-Addr                Port            VLAN      Speed     ARP-Count
State
30.1.1.6            Ethernet2/48          26        4         57
Speed-Limit
30.1.1.4            Ethernet2/48          26        4         56
Speed-Limit
Switch#show anti-arpscan ip-based attack-list history
SIP-Addr            Port                  VLAN      Attack-Times   State
Keep-Time
30.1.1.6            Ethernet2/48           26         6              Speed-
Limit    0 weeks,0 days,0 hours,8 minutes,46 seconds
30.1.1.4            Ethernet2/48           26         3              Speed-
Limit    0 weeks,0 days,0 hours,0 minutes,28 seconds
```

4.8.14 show anti-arpscan ip-based running-config

Command: `show anti-arpscan ip-based running-config`

Function: Displays the current IP-based ARP scanning prevention configuration.

Parameters: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the current configuration, including the level-1 and level-2 thresholds, the action taken above the level-2 threshold, the rate of ARP packets sent to the CPU after the level-1 threshold is exceeded, and the FFP entry size.

Example:

```
Switch(config)#show anti-arpscan ip-based running-config
level1 thrshould:   4
level2 thrshould:   8
level2 action:      Discard-Arp
arp-to-cpu speed:   2
actIp-num:          0
ffp-max:            1024
ffp-used:           0
```

4.9 Preventing ARP Spoofing

4.9.1 ip arp-security updateprotect

Command: `ip arp-security updateprotect`
`no ip arp-security updateprotect`

Function: Prevents automatic ARP table updates. The **no ip arp-security updateprotect** command re-enables automatic updates.

Parameters: None.

Default: The ARP table is updated automatically.

Command Mode: Global Mode and Interface Mode.

Usage Guidelines: When automatic ARP table updates are disabled, ARP packets that conflict with an existing ARP entry (for example, same IP address but different MAC address or port) are dropped; other ARP packets are still accepted to refresh the aging timer or create new entries. Existing ARP entries therefore remain unchanged, while new entries can still be learned.

Example:

```
Switch(Config-if-Vlan1)#ip arp-security updateprotect.
Switch(config)#ip arp-security updateprotect
```

4.9.2 ip arp-security learnprotect

Command: `ip arp-security learnprotect`
`no ip arp-security learnprotect`

Function: Disables IPv4 ARP learning. The **no ip arp-security learnprotect** command re-enables ARP learning.

Parameters: None.

Default: ARP learning is enabled.

Command Mode: Global Mode and Interface Mode.

Usage Guidelines: This command prevents automatic learning and updating of ARP entries. Unlike **ip arp-security updateprotect**, after this command is executed, entries still age out even if the switch keeps sending request and reply messages.

Example:

```
Switch(Config-if-Vlan1)# ip arp-security learnprotect
Switch(config)# ip arp-security learnprotect
```

4.9.3 ip arp-security convert

Command: `ip arp-security convert`

Function: Converts all dynamic ARP entries to static entries.

Parameters: None.

Command Mode: Global Mode and Interface Mode.

Usage Guidelines: This command converts dynamic ARP entries to static entries, which, combined with disabling automatic learning, helps prevent ARP spoofing. It takes effect once when executed and is not retained in the configuration.

Example:

```
Switch(Config-if-Vlan1)#ip arp -security convert
Switch(config)#ip arp -security convert
```

4.10 ARP GUARD

4.10.1 arp-guard ip

Command: `arp-guard ip <addr>`
`no arp-guard ip <addr>`

Function: Adds an ARP Guard address. The **no** form of this command deletes the ARP Guard address.

Parameters: <addr> is the protected IP address, in dotted decimal notation.

Default: No ARP Guard address is configured.

Command Mode: Port Mode.

Usage Guidelines: After an ARP Guard address is configured on a port, ARP messages received on the port are filtered. If the source IP address of an ARP message matches an ARP Guard address configured on the port, the message is treated as a spoofed ARP message and is dropped instead of being sent to the CPU or forwarded. Up to 16 ARP Guard addresses can be configured on each port.

Example:

Configure ARP Guard address 100.1.1.1 on port ethernet1/0/1.

```
switch(config)#interface ethernet1/0/1
switch(Config-If-Ethernet 1/0/1)#arp-guard ip 100.1.1.1
```

Delete ARP Guard address 100.1.1.1 from port ethernet1/0/1.

```
switch(config)#interface ethernet1/0/1
switch(Config-If-Ethernet 1/0/1)#no arp-guard ip 100.1.1.1
```

4.11 ARP Local Proxy

4.11.1 ip local proxy-arp

Command: `ip local proxy-arp`
`no ip local proxy-arp`

Function: Enables or disables local proxy ARP on the specified interface.

Parameters: None.

Default: Disabled on all interfaces.

Command Mode: VLAN Interface Mode.

Usage Guidelines: This function is disabled on all interfaces by default. Unlike standard proxy ARP, local proxy ARP acts as an ARP proxy within the same Layer 3 interface, so that traffic is forwarded at Layer 3 by the switch.

Example: Enable local proxy ARP on interface VLAN 1.

```
Switch(Config-if-Vlan1)# ip local proxy-arp
```

4.12 Gratuitous ARP

4.12.1 ip gratuitous-arp

Command: `ip gratuitous-arp [<interval-time>]`
`no ip gratuitous-arp`

Function: Enables gratuitous ARP and specifies the gratuitous ARP update interval. The **no** form of this command disables gratuitous ARP.

Parameters: <interval-time> is the gratuitous ARP update interval, from 5 to 1200 seconds. The default is 300 seconds.

Command Mode: Global Mode and Interface Mode.

Default: Disabled.

Usage Guidelines: When gratuitous ARP is configured in Global Mode, all Layer 3 interfaces of the switch send gratuitous ARP requests. When it is configured in Interface Mode, only the specified interface sends gratuitous ARP requests. The interval configured in Interface Mode takes precedence over that configured in Global Mode.

Example:

1) Enable gratuitous ARP in Global Mode and set the update interval to 400 seconds.

```
Switch>enable
Switch#config
Switch(config)#ip gratuitous-arp 400
```

2) Enable gratuitous ARP on interface VLAN 10 and set the update interval to 350 seconds.

```
Switch(config)#interface vlan 10
Switch(Config-if-Vlan10)#ip gratuitous-arp 350
```

4.12.2 show ip gratuitous-arp

Command: show ip gratuitous-arp [interface vlan <vlan-id>]

Function: Displays the gratuitous ARP configuration.

Parameters: <vlan-id> is the VLAN ID, from 1 to 4094.

Command Mode: All Configuration Modes.

Usage Guidelines: In all configuration modes, the **show ip gratuitous-arp** command displays the gratuitous ARP configuration in Global Mode and Interface Mode. The **show ip gratuitous-arp interface vlan <vlan-id>** command displays the gratuitous ARP configuration of the specified VLAN interface.

Example:

1) Display the gratuitous ARP configuration in both Global Mode and Interface Mode.

```
Switch#show ip gratuitous-arp
Gratuitous ARP send is Global enabled, Interval-Time is 300(s)
Gratuitous ARP send enabled interface vlan information:
Name            Interval-Time(seconds)
Vlan1            400
Vlan10           350
```

2) Display the gratuitous ARP configuration of interface VLAN 10.

```
Switch#show ip gratuitous-arp interface vlan 10
Gratuitous ARP send interface Vlan10 information:
Name            Interval-Time(seconds)
Vlan10           350
```

4.13 Keepalive Gateway

4.13.1 keepalive gateway

Command: keepalive gateway <ip-address> [{<interval-seconds> | msec <interval-millisecond>} [retry-count]]
no keepalive gateway

Function: Enables keepalive gateway detection and configures the interval for sending ARP requests and the retry count after detection fails. The **no** form of this command disables the function.

Parameters: <ip-address>: The IP address of the gateway.

<interval-seconds>: The interval for sending ARP requests, from 1 to 32767 seconds. The default is 10 seconds.

<interval-millisecond>: The interval for sending ARP requests, from 160 to 999 milliseconds.

retry-count: The number of retries after detection fails. The default is 5.

Default: Disabled.

Command Mode: Interface Mode.

Usage Guidelines: This command is supported on Layer 3 switches, and the detection method is used only in point-to-point topologies.

Example:

```
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#keealive gateway 1.1.1.1 3 10
```

4.13.2 show ip interface

Command: show ip interface [interface-name]

Function: Displays the IPv4 operating status of the specified interface.

Parameters: interface-name is the interface name. If no parameter is specified, the IPv4 operating status of all interfaces is displayed.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the IPv4 operating status of the interface.

Example:

```
Switch(config)#show ip interface brief
Index     Interface             IP-Address      Protocol
3001      Vlan1                 1.1.1.2         up
9000      Loopback              127.0.0.1       up
```

4.13.3 show keepalive gateway

Command: show keepalive gateway [interface-name]

Function: Displays the keepalive gateway operating status of the specified interface.

Parameters: interface-name is the interface name. If no parameter is specified, the status of all interfaces is displayed.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the keepalive gateway operating status of the interface.

Example:

```
Switch(config)#show keepalive gateway
interface Vlan1 gateway 1.1.1.1 time 10s retry 1 remain 4 now UP
```

4.14 Dynamic ARP Inspection

4.14.1 ip arp inspection

Command: ip arp inspection vlan <vlan-id>
no ip arp inspection vlan <vlan-id>

Function: Enables dynamic ARP inspection (DAI) on a VLAN basis.

Parameters: <vlan-id> is the VLAN on which dynamic ARP inspection is enabled.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: After dynamic ARP inspection is configured in Global Mode, the switch intercepts, logs, and drops ARP packets with invalid MAC or IP addresses. This command is generally used together with DHCP snooping.

Example: Enable dynamic ARP inspection on VLAN 10.

```
Switch(config)#
Switch(config)#ip arp inspection vlan 10
Switch(config)#exit
```

4.14.2 ip arp inspection port

Command: ip arp inspection port recovery-time <1-3600>
no ip arp inspection port recovery-time

Function: Configures the recovery time after a port is rate-limited by dynamic ARP inspection.

Parameters: <1-3600>: The recovery time, in seconds, after a port is rate-limited by dynamic ARP inspection.

Command Mode: Global Mode.

Default: 60 seconds.

Usage Guidelines: Use this command to change the recovery time after a port is rate-limited by dynamic ARP inspection. This command is generally used together with DHCP snooping.

Example: Change the recovery time after a port is rate-limited by dynamic ARP inspection in Global Mode.

```
Switch(config)#
Switch(config)#ip arp inspection port recovery-time 100
Switch(config)#exit
```

4.14.3 ip arp inspection trust

Command: ip arp inspection trust
no ip arp inspection trust

Function: Configures the port as a trusted port for dynamic ARP inspection.

Parameters: None.

Command Mode: Port Mode.

Default: All ports are untrusted.

Usage Guidelines: A port configured with this command does not inspect received ARP packets and forwards them directly. For ARP packets received on untrusted ports, the switch forwards only valid packets and drops and logs invalid ones. This command is generally used together with DHCP snooping.

Example: Configure port 1/0/1 as a trusted port.

```
Switch(config)#
Switch(config)#in e 1/0/1
Switch(config-if-ethernet1/0/1)#ip arp inspection trust
Switch(config-if-ethernet1/0/1)#exit
```

4.14.4 ip arp inspection limit-rate

Command: ip arp inspection limit-rate <rate>
no ip arp inspection limit-rate

Function: Limits the ARP packet rate on an untrusted port.

Parameters: <rate> is the ARP packet rate limit of the untrusted port, in pps.

Command Mode: Port Mode.

Default: The ARP packet rate of trusted and untrusted ports is not limited.

Usage Guidelines: This command limits the ARP packet rate of an untrusted port; valid ARP packets are forwarded within the limit. This command is generally used together with DHCP snooping.

Example: Limit the ARP packet rate of untrusted port 1/0/1 to 100 pps.

```
Switch(config)#
Switch(config)#in e 1/0/1
Switch(config-if-ethernet1/0/1)# ip arp inspection limit-rate 100
Switch(config-if-ethernet1/0/1)#exit
```

4.15 DHCP

4.15.1 DHCP Server

4.15.1.1 bootfile

Command: `bootfile <filename>`
`no bootfile`

Function: Sets the name of the boot file for DHCP clients. The **no bootfile** command deletes this setting.

Parameters: <filename> is the name of the file to import, up to 255 characters.

Command Mode: DHCP Address Pool Mode.

Usage Guidelines: Specifies the name of the file the client imports. This is typically used for diskless workstations that download a configuration file from a server at boot. Use this command together with the **next-server** command.

Example: Set the path and name of the file to import to "c:\temp\nos.img".

```
Switch(dhcp-1-config)#bootfile c:\temp\nos.img
```

Related Commands: next-server

4.15.1.2 clear ip dhcp binding

Command: `clear ip dhcp binding {<address> | all}`

Function: Deletes the specified IP address-to-hardware address binding record or all binding records.

Parameters: <address> is the IP address with a binding record, in dotted decimal notation. **all** specifies all IP addresses with binding records.

Command Mode: Admin Mode.

Usage Guidelines: Use the **show ip dhcp binding** command to view the bindings between IP addresses and DHCP client hardware addresses. If a DHCP client stops using its assigned IP address before the lease expires without notifying the DHCP server, the server does not remove the binding automatically. The administrator can use this command to delete the binding manually. If **all** is specified, all automatic bindings are deleted and all addresses in the DHCP address pool can be reallocated.

Example: Remove all IP address-to-hardware address bindings.

```
Switch#clear ip dhcp binding all
```

Related Commands: show ip dhcp binding

4.15.1.3 clear ip dhcp conflict

Command: `clear ip dhcp conflict {<address> | all }`

Function: Deletes an address from the address conflict log.

Parameters: <address> is an IP address with a conflict record; **all** specifies all addresses with conflict records.

Command Mode: Admin Mode.

Usage Guidelines: Use the **show ip dhcp conflict** command to check conflicting IP addresses and the **clear ip dhcp conflict** command to delete the conflict record of an address. If **all** is specified, all conflict records are removed from the log. Addresses removed from the log become available for allocation by the DHCP server.

Example: The network administrator finds that 10.1.128.160, which has a conflict record in the log, is no longer in use, and deletes the record from the address conflict log.

```
Switch#clear ip dhcp conflict 10.1.128.160
```

Related Commands: ip dhcp conflict logging, show ip dhcp conflict

4.15.1.4 clear ip dhcp server statistics

Command: `clear ip dhcp server statistics`

Function: Clears the DHCP server statistics and counters.

Parameters: None.

Command Mode: Admin Mode.

Usage Guidelines: DHCP server statistics are displayed with the **show ip dhcp server statistics** command and are cumulative. Use this command to clear the counters for easier checking.

Example: Clear the DHCP server counters.

```
Switch#clear ip dhcp server statistics
```

Related Commands: show ip dhcp server statistics

4.15.1.5 client-identifier

Command: `client-identifier <unique-identifier>`
`no client-identifier`

Function: Specifies the unique client identifier for manual address binding. The **no client-identifier** command deletes the identifier.

Parameters: <unique-identifier> is the client identifier, in dotted hexadecimal format.

Command Mode: DHCP Address Pool Mode.

Usage Guidelines: Use this command together with the **host** command for manual address binding. If the identifier of a requesting client matches the specified identifier, the DHCP server assigns the IP address defined with the **host** command to the client.

Example: Bind IP address 10.1.128.160 to the client with unique identifier 00-10-5a-60-af-12.

```
Switch(dhcp-1-config)#client-identifier 00-10-5a-60-af-12
Switch(dhcp-1-config)#host 10.1.128.160 24
```

Related Commands: host

4.15.1.6 debug ip dhcp client

Command: `debug ip dhcp client {event | packet}`
`no debug ip dhcp server {event | packet}`

Function: Enables DHCP client debugging. The **no** form of this command disables it.

Command Mode: Admin Mode.

Default: Disabled.

4.15.1.7 debug ip dhcp relay

Command: `debug ip dhcp server packet`
`no debug ip dhcp server packet`

Function: Enables DHCP relay debugging. The **no** form of this command disables it.

Command Mode: Admin Mode.

Default: Disabled.

4.15.1.8 debug ip dhcp server

Command: `debug ip dhcp server { events | linkage | packets |history| lookup}`
`no debug ip dhcp server { events | linkage | packets|history| lookup }`

Function: Enables DHCP server debugging. The **no debug ip dhcp server {events | linkage | packets | history | lookup}** command disables it.

Default: Disabled.

Command Mode: Admin Mode.

4.15.1.9 default-router

Command: `default-router <address1>[<address2>[…<address8>]]`
`no default-router`

Function: Configures default gateways for DHCP clients. The **no default-router** command deletes the default gateways.

Parameters: <address1>...<address8> are IP addresses in dotted decimal notation.

Default: No default gateway is configured for DHCP clients.

Command Mode: DHCP Address Pool Mode.

Usage Guidelines: Default gateway addresses must be in the same subnet as the DHCP client IP addresses. Up to 8 gateway addresses are supported. The address configured first has the highest priority: address1 has the highest priority, address2 the second highest, and so on.

Example: Configure 10.1.128.2 and 10.1.128.100 as default gateways for DHCP clients.

```
Switch(dhcp-1-config)#default-router 10.1.128.2 10.1.128.100
```

4.15.1.10 dns-server

Command: `dns-server <address1>[<address2>[…<address8>]]`
`no dns-server`

Function: Configures DNS servers for DHCP clients. The **no dns-server** command deletes the DNS servers.

Parameters: <address1>...<address8> are IP addresses in dotted decimal notation.

Default: No DNS server is configured for DHCP clients.

Command Mode: DHCP Address Pool Mode.

Usage Guidelines: Up to 8 DNS server addresses can be configured. The address configured first has the highest priority: address1 has the highest priority, address2 the second highest, and so on.

Example: Configure 10.1.128.3 as the DNS server for DHCP clients.

```
Switch(dhcp-1-config)#dns-server 10.1.128.3
```

4.15.1.11 domain-name

Command: `domain-name <domain>`
`no domain-name`

Function: Configures the domain name for DHCP clients. The **no domain-name** command deletes the domain name.

Parameters: <domain> is the domain name, up to 255 characters.

Command Mode: DHCP Address Pool Mode.

Default: None.

Usage Guidelines: Specifies a domain name for clients.

4.15.1.12 hardware-address

Command: `hardware-address <hardware-address> [{Ethernet | IEEE802|<type-number>}]`
`no hardware-address`

Function: Specifies the client hardware address for manual address binding. The **no hardware-address** command deletes the setting.

Parameters: <hardware-address> is the hardware address in hexadecimal. **Ethernet | IEEE802** is the protocol type. **<type-number>** is the RFC-defined protocol type number, from 1 to 255, for example, 0 for Ethernet and 6 for IEEE 802.

Default: Ethernet.

Command Mode: DHCP Address Pool Mode.

Usage Guidelines: Use this command together with the **host** command for manual address binding. If the hardware address of a requesting client matches the specified hardware address, the DHCP server assigns the IP address defined with the **host** command to the client.

Example: Bind IP address 10.1.128.160 to the client with hardware address 00-00-e2-3a-26-04.

```
Switch(dhcp-1-config)#hardware-address 00-00-e2-3a-26-04
Switch(dhcp-1-config)#host 10.1.128.160 24
```

Related Commands: host

4.15.1.13 host

Command: `host <address> [<mask> | <prefix-length>]`
`no host`

Function: Specifies the IP address assigned to the client for manual address binding. The **no host** command deletes the IP address.

Parameters: <address> is the IP address in dotted decimal notation. **<mask>** is the subnet mask in dotted decimal notation. **<prefix-length>** specifies the mask as a prefix length; for example, mask 255.255.255.0 is prefix length 24, and mask 255.255.255.252 is prefix length 30.

Command Mode: DHCP Address Pool Mode.

Default: None.

Usage Guidelines: If no mask or prefix length is configured with the IP address and the address pool contains no mask information, the system assigns a mask automatically based on the IP address class.

Use this command together with the **hardware-address** or **client-identifier** command for manual address binding. If the identifier or hardware address of a requesting client matches the specified identifier or hardware address, the DHCP server assigns the IP address defined with this command to the client.

Example: Bind IP address 10.1.128.160 to the client with hardware address 00-10-5a-60-af-12.

```
Switch(dhcp-1-config)#hardware-address 00-10-5a-60-af-12
Switch(dhcp-1-config)#host 10.1.128.160 24
```

Related Commands: hardware-address, client-identifier

4.15.1.14 ip dhcp conflict logging

Command: `ip dhcp conflict logging`
`no ip dhcp conflict logging`

Function: Enables logging of address conflicts detected by the DHCP server. The **no ip dhcp conflict logging** command disables the logging.

Default: Enabled.

Command Mode: Global Mode.

Usage Guidelines: When logging is enabled, conflicting addresses detected by the DHCP server are logged. Addresses in the conflict log are not assigned dynamically until their conflict records are deleted.

Example: Disable DHCP server conflict logging.

```
Switch(config)#no ip dhcp conflict logging
```

Related Commands: clear ip dhcp conflict

4.15.1.15 ip dhcp excluded-address

Command: **`ip dhcp excluded-address <low-address> [<high-address>]`**
`no ip dhcp excluded-address <low-address> [<high-address>]`

Function: Excludes addresses from dynamic assignment. The **no ip dhcp excluded-address <low-address> [<high-address>]** command cancels the setting.

Parameters: **<low-address>** is the start IP address; **<high-address>** is the end IP address.

Default: If only a start address is specified, only that address is excluded.

Command Mode: Global Mode.

Usage Guidelines: Use this command to exclude one or more consecutive addresses in the pool from dynamic assignment so that the administrator can use them for other purposes.

Example: Exclude addresses 10.1.128.1 to 10.1.128.10 from dynamic assignment.

```
Switch(config)#ip dhcp excluded-address 10.1.128.1 10.1.128.10
```

4.15.1.16 ip dhcp pool

Command: **`ip dhcp pool <name>`**
`no ip dhcp pool <name>`

Function: Configures a DHCP address pool and enters DHCP Address Pool Mode. The **no ip dhcp pool <name>** command deletes the specified address pool.

Parameters: **<name>** is the address pool name, up to 32 characters.

Command Mode: Global Mode.

Usage Guidelines: Use this command in Global Mode to configure a DHCP address pool and enter DHCP Address Pool Mode.

Example: Define an address pool named "1".

```
Switch(config)#ip dhcp pool 1
Switch(dhcp-1-config)#
```

4.15.1.17 ip dhcp conflict ping-detection enable

Command: **`ip dhcp conflict ping-detection enable`**
`no ip dhcp conflict ping-detection enable`

Function: Enables ping detection of address conflicts on the DHCP server. The **no** form of this command disables the function.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Ping detection of conflicts requires address conflict logging to be enabled; if logging is disabled, ping detection is also disabled. If a client cannot receive ping requests (for example, because of a firewall), the function checks the local ARP table for the IP address to be

allocated: if the address has an ARP entry, a conflict exists; otherwise, the address is allocated to the client.

Example: Enable ping detection of address conflicts.

```
Switch(config)#ip dhcp conflict ping-detection enable
```

Related Commands: ip dhcp conflict logging, ip dhcp ping packets, ip dhcp ping timeout

4.15.1.18 ip dhcp ping packets

Command: `ip dhcp ping packets <request-num>`
`no ip dhcp ping packets`

Function: Sets the maximum number of ping requests (Echo Requests) sent by the DHCP server for conflict detection. The default is 2. The **no** form of this command restores the default.

Parameters: <request-num> is the number of ping requests sent for conflict detection.

Default: 2.

Command Mode: Global Mode.

Example: Set the maximum number of ping requests sent by the DHCP server for conflict detection to 3.

```
Switch(config)#ip dhcp ping packets 3
```

Related Commands: ip dhcp conflict ping-detection enable, ip dhcp ping timeout

4.15.1.19 ip dhcp ping timeout

Command: `ip dhcp ping timeout <timeout-value>`
`no ip dhcp ping timeout`

Function: Sets the time, in milliseconds, that the DHCP server waits for a reply (Echo Reply) after each ping request (Echo Request) during conflict detection. The default is 500 ms. The **no** form of this command restores the default.

Parameters: <timeout-value> is the time to wait for a reply after each ping request during conflict detection.

Default: 500 ms.

Command Mode: Global Mode.

Example: Set the time to wait for each reply during ping conflict detection to 600 ms.

```
Switch(config)# ip dhcp ping timeout 600
```

Related Commands: ip dhcp conflict ping-detection enable, ip dhcp ping packets

4.15.1.20 lease

Command: `lease { [<days>] [<hours>][<minutes>] | infinite }`
`no lease`

Function: Sets the lease time of addresses in the address pool. The **no lease** command restores the default.

Parameters: <days> is the number of days, from 0 to 365; **<hours>** is the number of hours, from 0 to 23; **<minutes>** is the number of minutes, from 0 to 59; **infinite** specifies an unlimited lease.

Default: 1 day.

Command Mode: DHCP Address Pool Mode.

Usage Guidelines: DHCP assigns network addresses dynamically rather than permanently, which is why leases are used. Set the lease time according to network conditions: a lease that is too long reduces the flexibility of DHCP, while a lease that is too short increases network traffic and overhead. The default lease time of the switch is 1 day.

Example: Set the lease time of DHCP pool "1" to 3 days, 12 hours, and 30 minutes.

```
Switch(dhcp-1-config)#lease 3 12 30
```

4.15.1.21 max-lease-time

Command: `max-lease-time {[<days>] [<hours>] [<minutes>] | infinite}`
`no max-lease-time`

Function: Sets the maximum lease time of addresses in the address pool. The **no** form of this command restores the default.

Parameters: <days> is the number of days, from 0 to 365; **<hours>** is the number of hours, from 0 to 23; **<minutes>** is the number of minutes, from 0 to 59; **infinite** specifies an unlimited lease.

Default: 1 day.

Command Mode: DHCP Address Pool Mode.

Usage Guidelines: This command applies to DHCP request packets that carry option 51. If the lease time requested by the client exceeds the configured maximum lease time, the DHCP server assigns the address with the configured maximum lease time. If the requested lease time is less than the configured maximum, the server assigns the address with the requested lease time. The administrator can set the maximum lease time according to network conditions; the default is 1 day.

Example: Set the maximum lease time of DHCP address pool 1 to 3 days, 12 hours, and 30 minutes.

```
Switch(dhcp-1-config)#max-lease-time 3 12 30
```

4.15.1.22 netbios-name-server

Command: `netbios-name-server <address1>[<address2>[…<address8>]]`
`no netbios-name-server`

Function: Configures WINS server addresses. The **no netbios-name-server** command deletes the WINS servers.

Parameters: <address1>...<address8> are IP addresses in dotted decimal notation.

Default: No WINS server is configured.

Command Mode: DHCP Address Pool Mode.

Usage Guidelines: Specifies WINS servers for clients. Up to 8 WINS server addresses can be configured. The address configured first has the highest priority: address1 has the highest priority, address2 the second highest, and so on.

Example: Set the WINS server address of DHCP pool "1" to 192.168.1.1.

```
Switch(dhcp-1-config)#netbios-name-server 192.168.1.1
```

4.15.1.23 netbios-node-type

Command: `netbios-node-type {b-node | h-node | m-node | p-node | <type-number>}`
`no netbios-node-type`

Function: Sets the NetBIOS node type for clients. The **no netbios-node-type** command cancels the setting.

Parameters: b-node: Broadcast node. **h-node**: Hybrid node that uses point-to-point communication first and then broadcast. **m-node**: Hybrid node that uses broadcast first and then point-to-point communication. **p-node**: Point-to-point node. **<type-number>**: The node type in hexadecimal, from 0 to FF.

Default: No client node type is specified.

Command Mode: DHCP Address Pool Mode.

Usage Guidelines: If a client node type is to be specified, we recommend h-node (point-to-point first, then broadcast).

Example: Set the node type of clients in pool 1 to broadcast node.

```
Switch(dhcp-1-config)#netbios-node-type b-node
```

4.15.1.24 network-address

Command: `network-address <network-number> [<mask> | <prefix-length>]`
`no network-address`

Function: Sets the range of addresses in the pool available for assignment. The **no network-address** command cancels the setting.

Parameters: <network-number> is the network number. **<mask>** is the subnet mask in dotted decimal notation. **<prefix-length>** specifies the mask as a prefix length; for example, mask 255.255.255.0 is prefix length 24, and mask 255.255.255.252 is prefix length 30. Note: When the DHCP server is used, the pool mask must be longer than or equal to the mask of the Layer 3 interface IP address in the corresponding subnet.

Default: If no mask is specified, a default mask is assigned according to the address class.

Command Mode: DHCP Address Pool Mode.

Usage Guidelines: This command sets the range of addresses that the DHCP server can assign dynamically. An address pool can have only one corresponding subnet. This command is mutually exclusive with the manual binding commands **hardware-address** and **host**.

Example: Set the assignable addresses in pool 1 to 10.1.128.0/24.

```
Switch(dhcp-1-config)#network-address 10.1.128.0 24
```

4.15.1.25 next-server

Command: `next-server <address1>[<address2>[…<address8>]]`
`no next-server`

Function: Sets the address of the server that stores the client boot file. The **no next-server** command cancels the setting.

Parameters: <address1>...<address8> are IP addresses in dotted decimal notation.

Command Mode: DHCP Address Pool Mode.

Usage Guidelines: Configures the address of the server that hosts the client boot file. This is typically used for diskless workstations that download configuration files from a server at boot. Use this command together with the **bootfile** command.

Example: Set the boot file server address to 10.1.128.4.

```
Switch(dhcp-1-config)#next-server 10.1.128.4
```

4.15.1.26 option

Command: `option <code> {ascii <string> | hex <hex> | ipaddress <ipaddress>}`
`no option <code>`

Function: Sets the network parameter specified by the option code. The **no option <code>** command cancels the option setting.

Parameters: <code> is the option code of the network parameter. **<string>** is an ASCII string of up to 255 characters. **<hex>** is a hexadecimal value of up to 510 characters and must have an even length. **<ipaddress>** is an IP address in dotted decimal notation; up to 63 IP addresses can be configured.

Command Mode: DHCP Address Pool Mode.

Default: None.

Usage Guidelines: In addition to the common network parameter commands, the switch provides this command for configuring other parameters to meet different needs. Option codes are defined in RFC 2132.

Example: Set the WWW server address to 10.1.128.240.

```
Switch(dhcp-1-config)#option 72 ip 10.1.128.240
```

4.15.1.27 service dhcp

Command: `service dhcp`
`no service dhcp`

Function: Enables the DHCP service. The **no service dhcp** command disables the DHCP service.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: The DHCP service includes both the DHCP server and DHCP relay. When the DHCP service is enabled, both are enabled. The switch can assign IP addresses to DHCP clients and act as a DHCP relay only when the DHCP service is enabled.

Example: Enable the DHCP service.

```
Switch(config)#service dhcp
```

4.15.1.28 show ip dhcp binding

Command: `show ip dhcp binding [[<ip-addr>] [type {all | manual | dynamic}] [count] ]`

Function: Displays IP-MAC binding information.

Parameters: <ip-addr> is a specified IP address in dotted decimal notation. **all** displays all binding types (manual binding and dynamic assignment). **manual** displays manual bindings. **dynamic** displays dynamic assignments. **count** displays statistics of DHCP address binding entries.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch# show ip dhcp binding
IP address          Hardware address          Lease expiration    Type
10.1.1.233          00-00-E2-3A-26-04           Infinite        Manual
10.1.1.254          00-00-E2-3A-5C-D3           60           Automatic
```

Field	Description
IP address	IP address assigned to the DHCP client
Hardware address	MAC address of the DHCP client
Lease expiration	Time for which the DHCP client can hold the IP address
Type	Assignment type: manual binding or dynamic assignment

4.15.1.29 show ip dhcp conflict

Command: `show ip dhcp conflict`

Function: Displays the log of addresses with conflict records.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch# show ip dhcp conflict
IP Address              Detection method      Detection Time
```

```
10.1.1.1                    Ping                    FRI JAN 02 00:07:01 2002
```

Field	Description
IP Address	Conflicting IP address
Detection method	Method by which the conflict was detected
Detection Time	Time when the conflict was detected

4.15.1.30 show ip dhcp relay information option

Command: `show ip dhcp relay information option`

Function: Displays the DHCP relay option 82 configuration.

Parameters: None.

Command Mode: Admin Mode and Configuration Mode.

Default: None.

Usage Guidelines: None.

Example: Display the DHCP relay option 82 configuration.

```
Switch#show ip dhcp relay information option
ip dhcp server relay information option(i.e. option 82) is enabled
ip dhcp relay information option(i.e. option 82) is enabled
```

4.15.1.31 show ip dhcp server statistics

Command: `show ip dhcp server statistics`

Function: Displays statistics of all DHCP packets on the DHCP server.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch# show ip dhcp server statistics
Address pools3
Database agents  0
Automatic bindings  2
Manual bindings  0
Conflict bindings   0
Expired bindings 0
Malformed message   0
Message   Received
BOOTREQUEST  3814
DHCPDISCOVER 1899
DHCPREQUEST  6
DHCPDECLINE  0
DHCPRELEASE  1
DHCPINFORM   1
Message   Send
BOOTREPLY 1911
DHCPOFFER 6
DHCPACK   6
DHCPNAK   0
DHCPRELAY 1907
DHCPFORWARD  0
Switch#
```

Field	Description
Address pools	Number of DHCP address pools configured
Database agents	Number of database agents
Automatic bindings	Number of addresses assigned automatically
Manual bindings	Number of addresses bound manually
Conflict bindings	Number of conflicting addresses
Expired bindings	Number of addresses whose leases have

	expired
Malformed message	Number of malformed messages
Message Received	Statistics of DHCP packets received
BOOTREQUEST	Total number of packets received
DHCPDISCOVER	Number of DHCPDISCOVER packets
DHCPREQUEST	Number of DHCPREQUEST packets
DHCPDECLINE	Number of DHCPDECLINE packets
DHCPRELEASE	Number of DHCPRELEASE packets
DHCPINFORM	Number of DHCPINFORM packets
Message Send	Statistics of DHCP packets sent
BOOTREPLY	Total number of packets sent
DHCPOFFER	Number of DHCPOFFER packets
DHCPACK	Number of DHCPACK packets
DHCPNAK	Number of DHCPNAK packets
DHCPRELAY	Number of DHCPRELAY packets
DHCPFORWARD	Number of DHCPFORWARD packets

4.15.2 DHCP Relay

4.15.2.1 ip dhcp broadcast suppress

Command: `ip dhcp broadcast suppress`
`no ip dhcp broadcast suppress`

Function: Enables DHCP broadcast suppression. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Suppresses forwarding of DHCP broadcast packets; that is, DHCP broadcast packets are dropped or copied to the CPU.

Example: Enable DHCP broadcast suppression.

```
Switch(config)#ip dhcp broadcast suppress
```

4.15.2.2 ip dhcp relay share-vlan <vlanid> sub-vlan <vlanlist>

Command: `ip dhcp relay share-vlan <vlanid> sub-vlan <vlanlist>`
`no ip dhcp relay share-vlan`

Function: Specifies the sub VLANs of a shared VLAN. The **no** form of this command removes the sub VLANs of the shared VLAN.

Parameters: <vlanid> is the shared VLAN ID. **<vlanlist>** is the list of sub VLANs.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: A shared VLAN can have many sub VLANs, but a sub VLAN can belong to only one shared VLAN. When a Layer 2 DHCP relay device receives a DHCP request, it first checks whether the VLAN of the packet has a Layer 3 interface. If it does, that Layer 3 interface is used for DHCP relay. If it does not but the VLAN is a sub VLAN of a shared VLAN, the Layer 3 interface of the shared VLAN is used for DHCP relay.

4.15.2.3 ip forward-protocol udp bootps

Command: `ip forward-protocol udp bootps`
`no ip forward-protocol udp bootps`

Function: Enables DHCP relay to forward UDP broadcast packets. The **no ip forward-protocol udp bootps** command disables this service.

Parameters: bootps: Forwards DHCP broadcast packets on UDP port 67.

Default: UDP broadcast packets are not forwarded.

Command Mode: Global Mode.

Usage Guidelines: The forwarding destination address is set with the **ip helper-address** command, described below.

Example: Forward DHCP packets to 192.168.1.5.

```
Switch(config)#ip forward-protocol udp boots
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip helper-address 192.168.1.5
```

4.15.2.4 ip helper-address

Command: `ip helper-address <ip-address>`
`no ip helper-address <ip-address>`

Function: Specifies the destination address to which the DHCP relay forwards UDP packets. The **no ip helper-address <ip-address>** command cancels the setting.

Default: None.

Command Mode: Interface Configuration Mode.

Usage Guidelines: The DHCP relay forwarding server address corresponds to the forwarded UDP port; that is, the DHCP relay forwards UDP packets of that port only to the corresponding server, rather than forwarding all UDP packets to all servers. When this command is configured after the **ip forward-protocol udp <port>** command, the configured address receives UDP packets of **<port>**. Use this command together with the **ip forward-protocol udp <port>** command.

4.15.2.5 show ip forward-protocol

Command: `show ip forward-protocol`

Function: Displays the configured UDP port numbers of protocols whose broadcast packets are forwarded, that is, the port used to forward DHCP packets.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch#show ip forward-protocol
Forward protocol(UDP port): 67(active)
```

4.15.2.6 show ip helper-address

Command: `show ip helper-address`

Function: Displays the relationship between the UDP port of the forwarded protocol, the interface with forwarding enabled, and the destination IP address of forwarding.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch#show ip helper-address
Forward protocol    Interface                    Forward server
67(active)          Vlan1                        192.168.1.1
```

4.16 DHCP Option 82

4.16.1 debug ip dhcp relay packet

Command: debug ip dhcp relay packet

Function: Displays information about packet processing by the DHCP relay agent, including option 82 insertion and removal.

Parameters: None.

Command Mode: Admin Mode.

Usage Guidelines: Use this command during operation to display packet processing and the corresponding option 82 operations, including the option 82 information identified in request messages and returned in reply messages.

Example: Display information about packet processing by the DHCP relay agent.

```
Switch(config)# debug ip dhcp relay packet
```

4.16.2 ip dhcp relay information option

Command: ip dhcp relay information option
no ip dhcp relay information option

Function: Enables option 82 on the switch relay agent. The **no ip dhcp relay information option** command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Only DHCP relay agents configured with this command add option 82 to DHCP request messages for the server to process. Before enabling this function, make sure that the DHCP service is enabled and that the relay agent forwards UDP broadcast messages with destination port 67.

Example: Enable option 82 on the relay agent.

```
Switch(config)#service dhcp
Switch(config)# ip forward-protocol udp bootps
Switch(config)# ip dhcp relay information option
```

4.16.3 ip dhcp relay information option delimiter

Command: ip dhcp relay information option delimiter [colon | dot | slash | space]
no ip dhcp relay information option delimiter

Function: Sets the delimiter between parameters in option 82 suboptions in Global Mode. The **no** form of this command restores the default delimiter (slash).

Parameters: colon | dot | slash | space: The delimiter.

Default: Slash ("/").

Command Mode: Global Mode.

Usage Guidelines: The configured delimiter separates the user-defined parameters used to build option 82 suboptions (remote-id and circuit-id) in Global Mode.

Example: Set the delimiter for option 82 suboptions to dot (".").

```
Switch(config)#ip dhcp relay information option delimiter dot
```

4.16.4 ip dhcp relay information option remote-id

Command: ip dhcp relay information option remote-id {standard | <remote-id>}
no ip dhcp relay information option remote-id

Function: Sets the content of suboption 2 (remote ID) of option 82 added to DHCP request packets received on the interface. The **no** form of this command restores the standard format.

Parameters: standard uses the default VLAN MAC format. **<remote-id>** is the user-specified remote-id content of option 82, up to 64 characters.

Command Mode: Global Mode.

Default: The standard format is used.

Usage Guidelines: The added option 82 information must work with third-party DHCP servers. Use this command to specify the remote-id content when the standard remote-id format does not meet the server's requirements.

Example: Set the remote-id suboption of DHCP option 82 to street-1-1.

```
Switch(config)#ip dhcp relay information option remote-id street-1-1
```

4.16.5 ip dhcp relay information option remote-id format

Command: ip dhcp relay information option remote-id format {default | vs-hp}

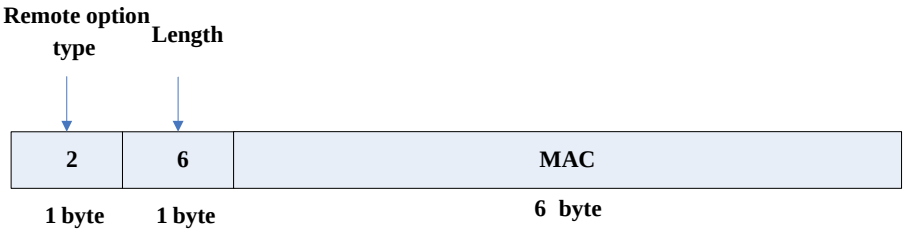
Function: Sets the remote-id format of the relay agent option 82.

Parameters: default: The remote-id is the VLAN MAC address in hexadecimal format. **vs-hp**: The remote-id is compatible with the HP remote-id format.

Default: default.

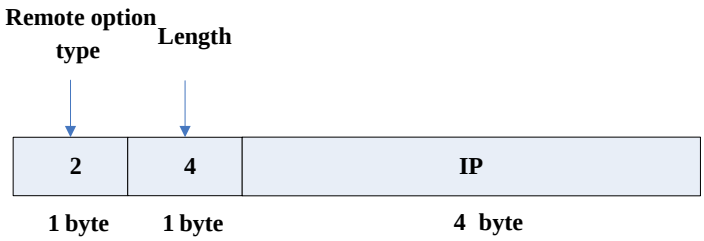
Command Mode: Global Mode.

Usage Guidelines: The default remote-id format is as follows:



MAC is the VLAN MAC address.

The HP-compatible remote-id format is as follows:



IP is the primary IP address of the Layer 3 interface on which the DHCP packets are received.

Example: Set the remote-id format of the relay agent option 82 to the HP-compatible format.

```
Switch(config)#ip dhcp relay information option remote-id format vs-hp
```

4.16.6 ip dhcp relay information option self-defined remote-id

Command: ip dhcp relay information option self-defined remote-id {hostname | mac | string WORD}
no ip dhcp relay information option self-defined remote-id

Function: Sets the self-defined method for building option 82, allowing users to define the parameters of the remote-id suboption.

Parameters: hostname: The host name. **mac**: The MAC address. **string WORD**: A user-defined remote-id string, up to 64 characters.

Command Mode: Global Mode.

Default: The standard method is used.

Usage Guidelines: After this command is configured, if no remote-id is configured on the interface, the remote-id suboption of option 82 is built using the self-defined method. In ASCII format, a MAC address is filled as, for example, 00-02-d1-2e-3a-0d; in hexadecimal format, it occupies 6 bytes. Each item is filled into packets in the configured order of the commands and separated by the delimiter configured with the **ip dhcp relay information option delimiter** command.

Example: Set the self-defined remote-id suboption of option 82 to the host name and the string "abc".

```
Switch(config)#ip dhcp relay information option self-defined remote-id
hostname string abc
```

4.16.7 ip dhcp relay information option self-defined remote-id format

Command: ip dhcp relay information option self-defined remote-id format [ascii | hex]

Function: Sets the format of the self-defined remote-id for relay option 82.

Parameters: ascii | hex: The format.

Command Mode: Global Mode.

Default: ASCII.

Usage Guidelines: The self-defined format applies to the remote-id built with the self-defined remote-id command.

Example: Set the self-defined remote-id format of relay option 82 to hexadecimal.

```
Switch(config)# ip dhcp relay information option self-defined remote-id
format hex
```

4.16.8 ip dhcp relay information option self-defined subscriber-id

Command: ip dhcp relay information option self-defined subscriber-id {vlan | port | id (switch-id (mac | hostname)| remote-mac)| string WORD }
no ip dhcp relay information option self-defined subscriber-id

Function: Sets the self-defined method for building option 82, allowing users to define the parameters of the circuit-id suboption.

Parameters: vlan, **port**, **id** (switch-id mac or hostname, or remote-mac): The items included. **string WORD**: A user-defined circuit-id string, up to 64 characters.

Command Mode: Global Mode.

Default: The standard method is used.

Usage Guidelines: After this command is configured, if no circuit-id is configured on the interface, the circuit-id suboption of option 82 is built using the self-defined method. In ASCII format, a VLAN is filled as, for example, "Vlan2"; a port as "Ethernet1/0/1"; and a MAC or remote MAC address as "00-

02-d1-2e-3a-0d". In hexadecimal format, a VLAN occupies 2 bytes; a port occupies 4 bytes: 1 byte for the slot (the slot ID on chassis switches, or 1 on box switches), 1 byte for the module (0 by default), and 2 bytes for the port number starting from 1; a MAC or remote MAC address occupies 6 bytes. Each item is filled into packets in the configured order of the commands and separated by the delimiter configured with the **ip dhcp relay information option delimiter** command.

Example: Set the self-defined circuit-id suboption of option 82 to port and MAC address.

```
Switch(config)# ip dhcp relay information option self-defined subscriber-id
port id switch-id mac
```

4.16.9 ip dhcp relay information option self-defined subscriber-id format

Command: ip dhcp relay information option self-defined subscriber-id format [ascii | hex]

Function: Sets the format of the self-defined circuit-id for relay option 82.

Parameters: ascii | hex: The format.

Command Mode: Global Mode.

Default: ASCII.

Usage Guidelines: The self-defined format applies to the circuit-id built with the self-defined subscriber-id command.

Example: Set the self-defined circuit-id format of relay option 82 to hexadecimal.

```
Switch(config)# ip dhcp relay information option self-defined subscriber-id
format hex
```

4.16.10 ip dhcp relay information option subscriber-id

Command: ip dhcp relay information option subscriber-id {standard | <circuit-id>}
no ip dhcp relay information option subscriber-id

Function: Sets the format of option 82 suboption 1 (circuit ID) added to DHCP request messages received on the interface. **standard** uses the standard VLAN name and physical port name format, such as "Vlan2+Ethernet1/0/12". **<circuit-id>** is the user-specified circuit-id content of option 82, up to 64 characters. The **no ip dhcp relay information option subscriber-id** command restores the standard format.

Parameters: standard: The standard format. **<circuit-id>**: A user-specified circuit-id string.

Command Mode: Interface Mode.

Default: The standard format is used.

Usage Guidelines: The option 82 information added by the switch must work with third-party DHCP servers. If the standard circuit-id format of the switch does not meet the server's requirements, use this command to specify the circuit-id content.

Example: Set the circuit-id suboption of DHCP option 82 to "foobar".

```
Switch(config-if-vlan1)#ip dhcp relay information option subscriber-id foobar
```

4.16.11 ip dhcp relay information option subscriber-id format

Command: ip dhcp relay information option subscriber-id format {hex | acsii | vs-hp|vs-cisco}

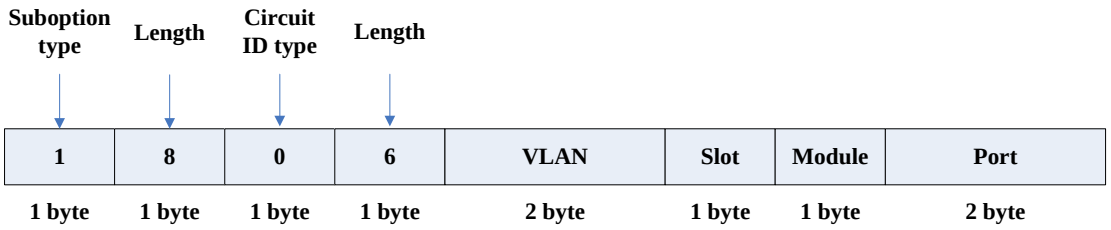
Function: Sets the subscriber-id format of the relay agent option 82.

Parameters: hex: The subscriber-id is VLAN and port information in hexadecimal format. **acsii**: The subscriber-id is VLAN and port information in ASCII format. **vs-hp**: The subscriber-id is compatible with the HP format. **vs-cisco**: The subscriber-id is compatible with the Cisco format.

Command Mode: Global Mode.

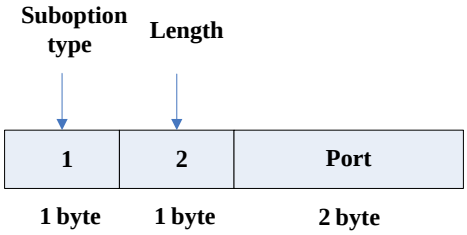
Default: ASCII.

Usage Guidelines: In ASCII format, the VLAN and port information is, for example, "Vlan1+Ethernet1/0/11". In hexadecimal format, the VLAN and port information is defined as follows:



The VLAN field contains the VLAN ID. Slot is the slot number on chassis switches and 1 on box switches; Module is 0 by default; Port is the port number, starting from 1.

The HP-compatible subscriber-id format is as follows:



Port is the port number, starting from 1.

Example: Set the subscriber-id format of the relay agent option 82 to hexadecimal.

```
Switch(config)#ip dhcp relay information option subscriber-id format hex
```

4.16.12 ip dhcp relay information policy

Command: `ip dhcp relay information policy {drop | keep | replace}`
`no ip dhcp relay information policy`

Function: Sets the forwarding policy for received DHCP request messages that contain option 82. In **drop** mode, messages with option 82 are dropped without processing. In **keep** mode, the original option 82 field is kept and the message is forwarded to the server. In **replace** mode, the existing option 82 field is replaced with the switch's own option 82 and the message is forwarded to the server. The **no ip dhcp relay information policy** command restores the replace policy.

Parameters: drop | keep | replace: The forwarding policy.

Command Mode: Interface Mode.

Default: Replace mode: the option 82 field in the message is replaced with the switch's own option 82.

Usage Guidelines: Because DHCP client messages may pass through several DHCP relay agents on the way to the DHCP server, relay agents later on the path must have a policy for handling option 82 added by earlier relay agents. Choose the option 82 forwarding policy according to the DHCP server's policy.

Example: Set the option 82 forwarding policy for DHCP messages to keep.

```
Switch(Config-if-Vlan1)# ip dhcp relay information policy keep
```

4.16.13 ip dhcp server relay information enable

Command: `ip dhcp server relay information enable`
`no ip dhcp server relay information enable`

Function: Enables the switch DHCP server to recognize option 82. The **no ip dhcp server relay information enable** command makes the server ignore option 82.

Parameters: None.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: Configure this command if the switch DHCP server should recognize option 82 and return option 82 information in reply messages; otherwise, the switch DHCP server ignores option 82.

Example: Configure the DHCP server to support option 82.

```
Switch(Config-if-Vlan1)# ip dhcp server relay information enable
```

4.16.14 show ip dhcp relay information option

Command: `show ip dhcp relay information option`

Function: Displays the DHCP option 82 status of the system, including whether option 82 is enabled, the interface forwarding policy, the circuit ID mode, and whether option 82 is enabled on the switch DHCP server.

Parameters: None.

Command Mode: Admin Mode and Global Mode.

Usage Guidelines: Use this command to check the status of relay agent option 82 during operation.

Example:

```
Switch#show ip dhcp relay information option
ip dhcp server relay information option(i.e. option 82) is disabled
ip dhcp relay information option(i.e. option 82) is enabled
Vlan2:
        ip dhcp relay information policy keep
        ip dhcp relay information option subscriber-id standard
Vlan3:
        ip dhcp relay information policy replace
        ip dhcp relay information option subscriber-id foobar
```

4.17 DHCP Snooping

4.17.1 debug ip dhcp snooping binding

Command: `debug ip dhcp snooping binding`
`no debug ip dhcp snooping binding`

Function: Enables DHCP snooping binding debugging to debug the status of DHCP snooping binding data.

Command Mode: Admin Mode.

Usage Guidelines: This command is mainly used to debug the DHCP snooping task when it adds ARP entries, 802.1X users, and trusted user entries based on binding data.

4.17.2 debug ip dhcp snooping event

Command: `debug ip dhcp snooping event`
`no debug ip dhcp snooping event`

Function: Enables DHCP snooping event debugging to debug the status of the DHCP snooping task.

Command Mode: Admin Mode.

Usage Guidelines: This command is mainly used to debug the DHCP snooping task and outputs information such as binding data checks and port actions.

4.17.3 debug ip dhcp snooping packet

Command: `debug ip dhcp snooping packet`
`no debug ip dhcp snooping packet`

Function: Enables DHCP snooping packet debugging to debug the message processing of DHCP snooping.

Command Mode: Admin Mode.

Usage Guidelines: Displays debugging information for each step of DHCP snooping message processing, including adding alarm information, adding binding information, forwarding DHCP messages, and adding or removing option 82.

4.17.4 debug ip dhcp snooping packet interface

Command: `debug ip dhcp snooping packet interface {[ethernet] <InterfaceName>}`
`no debug ip dhcp snooping packet {[ethernet] <InterfaceName>}`

Function: Enables DHCP snooping debugging for packets received on the specified interface.

Parameters: <InterfaceName>: The interface name.

Command Mode: Admin Mode.

Usage Guidelines: Displays information about messages received by DHCP snooping on the specified port.

4.17.5 debug ip dhcp snooping ha

Command: `debug ip dhcp snooping ha`
`no debug ip dhcp snooping ha`

Function: Enables DHCP snooping HA debugging to debug how DHCP snooping handles HA.

Command Mode: Admin Mode.

Usage Guidelines: Displays debugging information for each step of DHCP snooping HA processing, such as sending and receiving HA messages.

4.17.6 debug ip dhcp snooping update

Command: `debug ip dhcp snooping update`
`no debug ip dhcp snooping update`

Function: Enables debugging of communication between DHCP snooping and the helper server.

Command Mode: Admin Mode.

Usage Guidelines: Displays information about messages exchanged between DHCP snooping and the helper server.

4.17.7 ip dhcp snooping

Command: `ip dhcp snooping enable`
`no ip dhcp snooping enable`

Function: Enables DHCP snooping.

Parameters: None.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: When this function is enabled, the switch monitors all DHCP server packets on untrusted ports.

Example: Enable DHCP snooping.

```
switch(config)#ip dhcp snooping enable
```

4.17.8 ip dhcp snooping action

Command: `ip dhcp snooping action {shutdown | blackhole} [recovery <second>]`
`no ip dhcp snooping action`

Function: Sets or deletes the automatic defense action of a port.

Parameters:

shutdown: The port is shut down when it detects a rogue DHCP server.

blackhole: When the port detects a rogue DHCP server, the VLAN ID and source MAC address of the rogue packet are used to block traffic from that MAC address.

recovery: Recovers after the automatic defense action is executed (the port is re-enabled or the corresponding blackhole entry is deleted).

<second>: The time after the defense action at which recovery occurs, from 10 to 3600 seconds.

Command Mode: Port Mode.

Default: No defense action is configured.

Usage Guidelines: This command can be configured only when DHCP snooping is enabled globally. Trusted ports do not detect rogue DHCP servers and therefore never trigger defense actions. When an untrusted port becomes a trusted port, its defense action is deleted automatically.

Example: Set the DHCP snooping defense action of port ethernet1/0/1 to blackhole with a recovery time of 30 seconds.

```
switch(config)#interface ethernet 1/0/1
switch(Config-Ethernet1/0/1)#ip dhcp snooping action blackhole recovery 30
```

4.17.9 ip dhcp snooping action MaxNum

Command: `ip dhcp snooping action {<maxNum>|default}`

Function: Sets the maximum number of defense actions that can be in effect at the same time.

Parameters: <maxNum>: The number of defense actions on each port, from 1 to 200. The default is 10. **default** restores the default value.

Command Mode: Global Mode.

Default: 10.

Usage Guidelines: Set a maximum number of defense actions to prevent attacks from exhausting switch resources. If the number of alarms exceeds the configured value, the earliest defense action is recovered forcibly so that new defense actions can be applied.

Example: Set the maximum number of port defense actions to 100.

```
switch(config)#ip dhcp snooping action 100
```

4.17.10 ip dhcp snooping binding

Command: **`ip dhcp snooping binding enable`**
`no ip dhcp snooping binding enable`

Function: Enables DHCP snooping binding.

Parameters: None.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: When this function is enabled, the switch records the binding information assigned by DHCP servers on all trusted ports. Binding can be enabled only after DHCP snooping is enabled.

Example: Enable DHCP snooping binding.

```
switch(config)#ip dhcp snooping binding enable
```

Related Commands: ip dhcp snooping enable

4.17.11 ip dhcp snooping binding arp

Command: **`ip dhcp snooping binding arp`**
`no ip dhcp snooping binding arp`

Function: Enables DHCP snooping binding ARP.

Parameters: None.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: When this function is enabled, DHCP snooping adds binding ARP entries based on the binding information. Binding ARP can be enabled only after binding is enabled. Binding ARP entries are static entries that are not saved in the configuration and are added directly to the neighbor table. They have lower priority than static ARP entries configured by the administrator and can be overwritten by them; however, when the static ARP entries are deleted, the binding ARP entries are not restored until DHCP snooping captures the binding information again. Binding ARP entries protect these entries from ARP spoofing attacks. Because these static entries do not need to be reauthenticated, they also prevent ARP reauthentication failures when the switch is under an ARP scanning attack.

Binding ARP can be configured only after DHCP snooping binding is enabled.

Example: Enable DHCP snooping binding ARP.

```
switch(config)#ip dhcp snooping binding arp
```

Related Commands: ip dhcp snooping binding enable

4.17.12 ip dhcp snooping binding dot1x

Command: **`ip dhcp snooping binding dot1x`**
`no ip dhcp snooping binding dot1x`

Function: Enables DHCP snooping binding 802.1X.

Parameters: None.

Command Mode: Port Mode.

Default: Disabled on all ports.

Usage Guidelines: When this function is enabled, DHCP snooping notifies the 802.1X module of the captured binding information as 802.1X-controlled users. This command is mutually exclusive with the **ip dhcp snooping binding user-control** command.

Binding 802.1X can be configured only after DHCP snooping binding is enabled.

Example: Enable binding 802.1X on port ethernet1/0/1.

```
switch(config)#interface ethernet 1/0/1
switch(Config-Ethernet 1/0/1)# ip dhcp snooping binding dot1x
```

Related Commands: ip dhcp snooping binding enable, ip dhcp snooping binding user-control

4.17.13 ip dhcp snooping binding user

Command: ip dhcp snooping binding user <mac> address <ipaddress> vlan <vid> interface [Ethernet] <ifname>

no ip dhcp snooping binding user <mac> interface [Ethernet] <ifname>

Function: Configures static binding users.

Parameters:

<mac>: The MAC address of the static binding user, which uniquely identifies the binding user.

<ipaddress>: The IP address of the static binding user.

<vid>: The VLAN ID to which the static binding user belongs.

<ifname>: The access interface of the static binding user.

Command Mode: Global Mode.

Default: No static binding entry is configured.

Usage Guidelines: Static binding users are handled in the same way as dynamic binding users captured by DHCP snooping; they can be reported to 802.1X as controlled users, added directly as trusted user entries, or added as binding ARP entries. Static binding users never age out and have higher priority than dynamic binding users. Static binding users can be configured only after DHCP snooping binding is enabled.

Example: Configure a static binding user.

```
switch(config)#ip dhcp snooping binding user 00-03-0f-12-34-56 address
192.168.1.16 interface Ethernet 1/0/16
```

Related Commands: ip dhcp snooping binding enable

4.17.14 ip dhcp snooping binding user-control

Command: ip dhcp snooping binding user-control

no ip dhcp snooping binding user-control

Function: Enables the binding user function.

Parameters: None.

Command Mode: Port Mode.

Default: Disabled on all ports.

Usage Guidelines: When this function is enabled, DHCP snooping treats the captured binding information as trusted users that can access all resources. This command is mutually exclusive with the **ip dhcp snooping binding dot1x** command.

The binding user function can be configured only after DHCP snooping binding is enabled. It is not restricted by VLAN-based DHCP snooping settings but only by the global **ip dhcp snooping enable** command.

Example: Enable the binding user function on port ethernet1/0/1.

```
switch(config)#interface ethernet 1/0/1
switch(Config-Ethernet 1/0/1)# ip dhcp snooping binding user-control
```

Related Commands: ip dhcp snooping binding enable, ip dhcp snooping binding dot1x

4.17.15 ip dhcp snooping binding user-control max-user

Command: `ip dhcp snooping binding user-control max-user <number>`
`no ip dhcp snooping binding user-control max-user`

Function: Sets the maximum number of users allowed to access the port when the DHCP snooping binding user function is enabled. The **no** form of this command restores the default.

Parameters: <number> is the maximum number of users allowed on the port, from 0 to 1024.

Command Mode: Port Mode.

Default: 1024.

Usage Guidelines: This command sets the maximum number of trusted users installed from binding information when **ip dhcp snooping binding user-control** is enabled on the port. The default is 1024. Because switch hardware resources are limited, the actual number of trusted users installed depends on available resources. If a larger maximum is set, DHCP snooping installs binding information of untrusted users in hardware as trusted users as long as resources are available. If a smaller maximum is set, DHCP snooping adjusts the installed binding entries to the new maximum. When the number of installed binding entries reaches the maximum, no new DHCP users can become trusted users or access other network resources through the switch.

Example: Enable the DHCP snooping binding user function on port ethernet1/0/1 and set the maximum number of users on the port to 5.

```
Switch(Config-If-Ethernet1/0/1)# ip dhcp snooping binding user-control max-
user 5
```

Related Commands: ip dhcp snooping binding user-control

4.17.16 ip dhcp snooping information enable

Command: `ip dhcp snooping information enable`
`no ip dhcp snooping information enable`

Function: Enables option 82 for DHCP snooping on the switch. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: DHCP snooping adds standard option 82 to DHCP request messages and forwards them only after this command is configured. The format of suboption 1 (circuit ID) is the standard VLAN name plus physical port name, such as vlan1+ethernet1/0/12. The format of suboption 2 (remote ID) is the CPU MAC address of the switch, such as 00030f023301. If a DHCP request message with option 82 is received, DHCP snooping replaces those options with its own. If a DHCP reply message with option 82 is received, DHCP snooping removes those options and forwards the message.

Example: Enable option 82 for DHCP snooping on the switch.

```
Switch(config)#ip dhcp snooping enable
Switch(config)# ip dhcp snooping binding enable
Switch(config)# ip dhcp snooping information enable
```

4.17.17 ip dhcp snooping information option allow-untrusted (replace|)

Command: ip dhcp snooping information option allow-untrusted (replace|)
no ip dhcp snooping information option allow-untrusted (replace|)

Function: Allows untrusted DHCP snooping ports to receive DHCP packets with option 82. If **replace** is specified, option 82 is replaced. When this command is disabled, all untrusted ports drop DHCP packets with option 82.

Parameters: replace: Replaces option 82 in received packets.

Command Mode: Global Mode.

Default: Untrusted ports drop DHCP packets with option 82.

Usage Guidelines: A switch with DHCP snooping usually connects directly to end users, so this function is disabled by default to prevent users from adding option 82 themselves. When DHCP snooping is enabled, configure the uplink port as a trusted port.

Example: Allow untrusted ports to receive DHCP packets with option 82.

```
Switch(config)#ip dhcp snooping information option allow-untrusted
```

4.17.18 ip dhcp snooping information option delimiter

Command: ip dhcp snooping information option delimiter [colon | dot | slash | space]
no ip dhcp snooping information option delimiter

Function: Sets the delimiter between parameters in option 82 suboptions in Global Mode. The **no** form of this command restores the default delimiter (slash).

Parameters: colon | dot | slash | space: The delimiter.

Default: Slash ("/").

Command Mode: Global Mode.

Usage Guidelines: The configured delimiter separates the user-defined parameters used to build option 82 suboptions (remote-id and circuit-id) in Global Mode.

Example: Set the delimiter for option 82 suboptions to dot (".").

```
Switch(config)# ip dhcp snooping information option delimiter dot
```

4.17.19 ip dhcp snooping information option remote-id

Command: ip dhcp snooping information option remote-id {standard | <remote-id>}
no ip dhcp snooping information option remote-id

Function: Sets the content of suboption 2 (remote ID) of option 82 added to DHCP request packets received on the port. The **no** form of this command restores the standard format.

Parameters: standard uses the default VLAN MAC format. **<remote-id>** is the user-specified remote-id content of option 82, up to 64 characters.

Command Mode: Global Mode.

Default: The standard format is used.

Usage Guidelines: The added option 82 must work with third-party DHCP servers. Use this command to specify the remote-id content when the standard remote-id format does not meet the server's requirements.

Example: Set the remote-id suboption of DHCP option 82 to street-1-1.

```
Switch(config)#ip dhcp snooping information option remote-id street-1-1
```

4.17.20 ip dhcp snooping information option self-defined remote-id

Command: ip dhcp snooping information option self-defined remote-id {hostname | mac | string WORD}

no ip dhcp snooping information option self-defined remote-id

Function: Sets the self-defined method for building option 82, allowing users to define the parameters of the remote-id suboption.

Parameters: hostname: The host name. **mac**: The MAC address. **string WORD**: A user-defined remote-id string, up to 64 characters.

Command Mode: Global Mode.

Default: The standard method is used.

Usage Guidelines: After this command is configured, if **ip dhcp snooping information option remote-id** is not configured globally, the remote-id suboption of option 82 is built using the self-defined method. In ASCII format, a MAC address is filled as, for example, 00-02-d1-2e-3a-0d; in hexadecimal format, it occupies 6 bytes. Each item is filled into packets in the configured order of the commands and separated by the delimiter configured with the **ip dhcp snooping information option delimiter** command.

Example: Set the self-defined remote-id suboption of option 82 to the MAC address and the string "abc".

```
Switch(config)# ip dhcp snooping information option self-defined remote-id
mac string abc
```

4.17.21 ip dhcp snooping information option self-defined remote-id format

Command: ip dhcp snooping information option self-defined remote-id format [ascii | hex]

Function: Sets the format of the self-defined remote-id for DHCP snooping option 82.

Parameters: ascii | hex: The format.

Command Mode: Global Mode.

Default: ASCII.

Usage Guidelines: The self-defined format applies to the remote-id built with the self-defined remote-id command.

Example: Set the self-defined remote-id format of DHCP snooping option 82 to hexadecimal.

```
Switch(config)# ip dhcp snooping information option self-defined remote-id
format hex
```

4.17.22 ip dhcp snooping information option self-defined subscriber-id

Command: ip dhcp snooping information option self-defined subscriber-id {vlan | port | id (switch-id (mac | hostname)| remote-mac) | string WORD}

no ip dhcp snooping information option type self-defined subscriber-id

Function: Sets the self-defined method for building option 82, allowing users to define the parameters of the circuit-id suboption.

Parameters: vlan, **port**, **id** (switch-id mac or hostname, or remote-mac): The items included. **string WORD**: A user-defined circuit-id string, up to 64 characters.

Command Mode: Global Mode.

Default: The standard method is used.

Usage Guidelines: After this command is configured, if no circuit-id is configured on the port, the circuit-id suboption of option 82 is built using the self-defined method. In ASCII format, a VLAN is filled as, for example, "Vlan2"; a port as "Ethernet1/0/1"; and a MAC or remote MAC address as "00-02-d1-2e-3a-0d". In hexadecimal format, a VLAN occupies 2 bytes; a port occupies 4 bytes: 1 byte for the slot (the slot ID on chassis switches, or 1 on box switches), 1 byte for the module (0 by default), and 2 bytes for the port number starting from 1; a MAC or remote MAC address occupies 6 bytes. Each item is filled into packets in the configured order of the commands and separated by the delimiter configured with the **ip dhcp snooping information option delimiter** command.

Example: Set the self-defined circuit-id suboption of option 82 to VLAN, port, and remote MAC address.

```
Switch(config)#ip dhcp snooping information option self-defined subscriber-id
vlan port id remote-mac
```

4.17.23 ip dhcp snooping information option self-defined subscriber-id format

Command: `ip dhcp snooping information option self-defined subscriber-id format [ascii | hex]`

Function: Sets the format of the self-defined circuit-id for DHCP snooping option 82.

Parameters: ascii | hex: The format.

Command Mode: Global Mode.

Default: ASCII.

Usage Guidelines: The self-defined format applies to the circuit-id built with the self-defined subscriber-id command.

Example: Set the self-defined circuit-id format of DHCP snooping option 82 to hexadecimal.

```
Switch(config)#ip dhcp snooping information option self-defined subscriber-id
format hex
```

4.17.24 ip dhcp snooping information option subscriber-id format

Command: `ip dhcp snooping information option subscriber-id format {hex | acsii | vs-hp}`

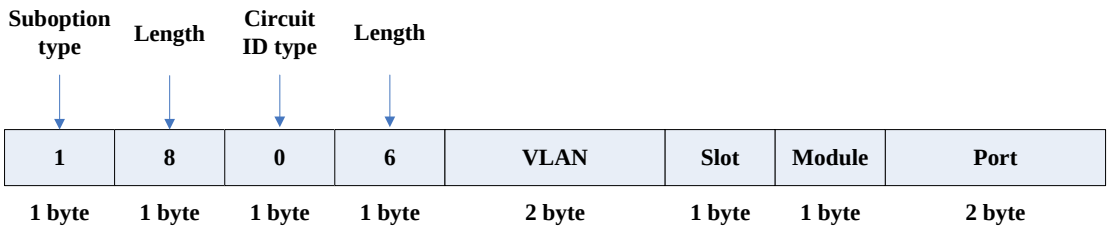
Function: Sets the subscriber-id format of DHCP snooping option 82.

Parameters: hex: The subscriber-id is VLAN and port information in hexadecimal format. **acsii**: The subscriber-id is VLAN and port information in ASCII format. **vs-hp**: The subscriber-id is compatible with the HP format.

Command Mode: Global Mode.

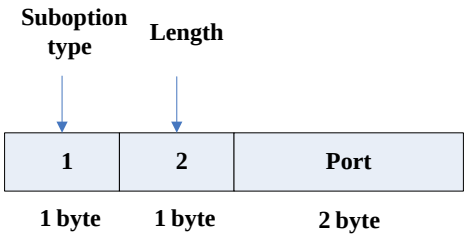
Default: ASCII.

Usage Guidelines: In ASCII format, the VLAN and port information is, for example, Vlan1+Ethernet1/0/11. In hexadecimal format, the VLAN and port information is defined as follows:



The VLAN field contains the VLAN ID. Slot is the slot number on chassis switches and 1 on box switches; Module is 0 by default; Port is the port number, starting from 1.

The HP-compatible subscriber-id format is as follows:



Port is the port number, starting from 1.

Example: Set the subscriber-id format of DHCP snooping option 82 to hexadecimal.

```
Switch(config)#ip dhcp snooping information option subscriber-id format hex
```

4.17.25 ip dhcp snooping timeout detection

Command: ip dhcp snooping timeout detection <0-7200>
no ip dhcp snooping timeout detection

Function: Sets the traffic monitoring timeout for binding table entries.

Parameters: <0-7200>: The traffic monitoring timeout, from 0 to 7200 seconds. The default is 3 seconds.

Command Mode: Global Mode.

Usage Guidelines: When a binding table entry is in protected mode, the switch checks at the end of each period whether traffic from the source MAC address passed during that period. If traffic passed, the entry remains in protected mode. If not, a quiet timer starts and the entry remains in protected mode during the quiet period. If no traffic passes during the quiet period, the protected mode of the entry is removed.

Example:

```
(Config)#ip dhcp snooping timeout detection 100
```

4.17.26 ip dhcp snooping timeout quiet

Command: ip dhcp snooping timeout quiet <0-4294967295>
no ip dhcp snooping timeout quiet

Function: Sets the traffic monitoring quiet time for binding table entries.

Parameters: <0-4294967295>: The traffic monitoring quiet time, from 0 to 4294967295 seconds. The default is 0.

Command Mode: Global Mode.

Usage Guidelines: When a binding table entry is in protected mode, the switch checks at the end of each period whether traffic from the source MAC address passed during that period. If traffic passed, the entry remains in protected mode. If not, a quiet timer starts and the entry remains in protected mode during the quiet period. If no traffic passes during the quiet period, the protected mode of the entry is removed.

Example:

```
(Config)#ip dhcp snooping timeout quiet 1000
```

4.17.27 ip dhcp snooping trust

Command: ip dhcp snooping trust
no ip dhcp snooping trust

Function: Sets or removes the DHCP snooping trust attribute of a port.

Parameters: None.

Command Mode: Port Mode.

Default: All ports are untrusted.

Usage Guidelines: This command can be configured only when DHCP snooping is enabled globally. When an untrusted port becomes a trusted port, its defense action is deleted automatically, and all of its security history records are cleared (except information in the system log).

Example: Set port ethernet1/0/1 as a DHCP snooping trusted port.

```
switch(config)#interface ethernet 1/0/1
switch(Config- Ethernet 1/0/1)#ip dhcp snooping trust
```

4.17.28 ip dhcp snooping vlan

Command: IP DHCP snooping VLAN (WORD |)
no ip dhcp snooping vlan (WORD |)

Function: Enables DHCP snooping in VLANs.

Parameters: WORD: The VLAN list. If no parameter is specified, DHCP snooping is enabled on all VLANs; otherwise, it is enabled on the specified VLANs.

Command Mode: Global Mode.

Default: DHCP snooping is not enabled in VLANs.

Usage Guidelines: no ip dhcp snooping vlan <vlan-id> disables DHCP snooping on the specified VLAN.

Example: Enable DHCP snooping on VLAN 10, and then disable it.

```
switch(config)#ip dhcp snooping vlan 10
switch(config)#no ip dhcp snooping vlan 10
```

4.17.29 ip user helper-address

Command: ip user helper-address <svr_addr> [port <udp_port>] source <src_addr> [secondary]
no ip user helper-address [secondary]

Function: Sets the address and port of the helper server.

Parameters:

<svr_addr>: The IP address of the helper server, in dotted decimal notation.

<udp_port>: The UDP port of the helper server, from 1 to 65535. The default is 9119.

<src_addr>: The local management IP address of the switch, in dotted decimal notation.

secondary: Specifies that the address is the secondary server address.

Command Mode: Global Mode.

Default: No helper server address is configured.

Usage Guidelines: DHCP snooping sends the monitored binding information to the helper server for storage. If the switch restarts abnormally, it can recover the binding data from the helper server. DHCP snooping and the helper server communicate over UDP with retransmission to ensure delivery. The helper server configuration can also be used to send 802.1X user data from the server; for details, see the 802.1X section.

Two helper server addresses are allowed. DHCP snooping first tries to connect to the primary server; only if the primary server is unreachable does the switch connect to the secondary server.

Note: The source address is the active management IP address of the switch. If the management IP address of the switch changes, update this configuration promptly.

Example: Set the local management IP address to 100.1.1.1 and the primary helper server address to 100.1.1.100, using the default port.

```
switch(config)#interface vlan 1
switch(Config- If-Vlan1)#ip address 100.1.1.1 255.255.255.0
switch(Config-if-Vlan1)exit
switch(config)#ip user helper-address 100.1.1.100 source 100.1.1.1
```

4.17.30 show ip dhcp snooping

Command: `show ip dhcp snooping [interface [ethernet] <interfaceName>]`

Function: Displays the current DHCP snooping configuration or the defense action records of the specified port.

Parameters: <interfaceName>: The port name.

Command Mode: Admin Mode and Global Mode.

Default: None.

Usage Guidelines: If no port is specified, the current DHCP snooping configuration is displayed; otherwise, the defense action records of the specified port are displayed.

Example:

```
switch#show ip dhcp snooping
DHCP Snooping is enabled
DHCP Snooping binding arp: disabled
DHCP Snooping maxnum of action info:10
DHCP Snooping limit rate: 100(pps), switch ID: 0003.0F12.3456
DHCP Snooping droped packets: 0, discarded packets: 0
DHCP Snooping alarm count: 0, binding count: 0,
expired binding: 0, request binding: 0
interface       trust      action     recovery   alarm num  bind num
--------------- --------- --------- ---------- --------- ----------
Ethernet1/0/1    trust     none      0second    0         0
Ethernet1/0/2    untrust   none      0second    0         0
Ethernet1/0/3    untrust   none      0second    0         0
Ethernet1/0/4    untrust   none      0second    0         1
Ethernet1/0/5    untrust   none      0second    2         0
Ethernet1/0/6    untrust   none      0second    0         0
Ethernet1/0/7    untrust   none      0second    0         0
Ethernet1/0/8    untrust   none      0second    0         1
Ethernet1/0/9    untrust   none      0second    0         0
Ethernet1/0/10   untrust   none      0second    0         0
Ethernet1/0/11   untrust   none      0second    0         0
Ethernet1/0/12   untrust   none      0second    0         0
Ethernet1/0/13   untrust   none      0second    0         0
Ethernet1/0/14   untrust   none      0second    0         0
Ethernet1/0/15   untrust   none      0second    0         0
Ethernet1/0/16   untrust   none      0second    0         0
Ethernet1/0/17   untrust   none      0second    0         0
Ethernet1/0/18   untrust   none      0second    0         0
Ethernet1/0/19   untrust   none      0second    0         0
Ethernet1/0/20   untrust   none      0second    0         0
Ethernet1/0/21   untrust   none      0second    0         0
Ethernet1/0/22   untrust   none      0second    0         0
Ethernet1/0/23   untrust   none      0second    0         0
Ethernet1/0/24   untrust   none      0second    0         0
```

Field	Description
DHCP Snooping is enable	Whether DHCP snooping is enabled globally
DHCP Snooping binding arp	Whether ARP binding is enabled
DHCP Snooping maxnum of action info	Maximum number of port defense actions

DHCP Snooping limit rate	Rate limit for received packets
switch ID	Switch ID, which identifies the switch (usually the CPU MAC address)
DHCP Snooping droped packets	Number of DHCP messages dropped because the rate limit was exceeded
discarded packets	Number of packets discarded because of internal communication failures; this may occur if the switch CPU is too busy to schedule the DHCP snooping task to process received DHCP messages
DHCP Snooping alarm count:	Number of alarms
binding count	Number of binding entries
expired binding	Number of binding entries that have expired but have not been deleted. Expired entries may not be deleted immediately if the switch must notify the helper server and the helper server has not acknowledged the notification.
request binding	Number of REQUEST entries
interface	Port name
trust	Trust attribute of the port
action	Automatic defense action of the port
recovery	Automatic recovery time of the port
alarm num	Number of history records of automatic defense actions on the port
bind num	Number of binding entries associated with the port

```
switch#show ip dhcp snooping int Ethernet1/0/1
interface Ethernet1/0/1 user config:
trust attribute: untrust
action: none
binding dot1x: disabled
binding user: disabled
recovery interval:0(s)
Alarm info: 0
Binding info: 0
Expired Binding: 0
Request Binding: 0
```

Field	Description
interface	Port name
trust attribute	Trust attribute of the port
action	Automatic defense action of the port
recovery interval	Automatic recovery time of the port
maxnum of alarm info	Maximum number of automatic defense actions that can be recorded on the port
binding dot1x	Whether binding 802.1X is enabled on the port
binding user	Whether the binding user function is enabled on the port
Alarm info	Number of alarms
Binding info	Number of binding entries
Expired Binding	Expired binding entries
Request Binding	REQUEST entries

4.17.31 show ip dhcp snooping binding all

Command: `show ip dhcp snooping binding all`

Function: Displays the current global DHCP snooping binding information.

Parameters: None.

Command Mode: Admin Mode and Global Mode.

Default: None.

Usage Guidelines: Use this command to check the global DHCP snooping binding information. Each entry includes the MAC address, IP address, port name, VLAN ID, and binding state flag. DHCP snooping must be enabled globally before this command can be used.

Example:

```
switch#show ip dhcp snooping binding all
ip dhcp snooping static binding count:1169, dynamic binding count:0
MAC             IP address      Interface     Vlan ID  Flag
--------------------------------------------------------------------------
00-00-00-00-11-11  192.168.40.1    Ethernet1/0/1    1      S
00-00-00-00-00-10  192.168.40.10   Ethernet1/0/2    1      D
00-00-00-00-00-11  192.168.40.11   Ethernet1/0/4    1      D
00-00-00-00-00-12  192.168.40.12   Ethernet1/0/4    1      D
00-00-00-00-00-13  192.168.40.13   Ethernet1/0/4    1      SU
00-00-00-00-00-14  192.168.40.14   Ethernet1/0/4    1      SU
00-00-00-00-00-15  192.168.40.15   Ethernet1/0/5    1      SL
00-00-00-00-00-16  192.168.40.16   Ethernet1/0/5    1      SL
--------------------------------------------------------------------------
The flag explanation of the binding state:
S The static binding is configured by shell command
D The dynamic binding type
U The binding is uploaded to the server
R The static binding is configured by the server
O DHCP response with the option82
L The hardware drive is announced by the binding
X Announcing dot1x module is successful
E Announcing dot1x module is failing
```

4.18 DHCP option 60 and option 43

4.18.1 option 43 ascii LINE

Command: `option 43 ascii LINE`
`no option 43`

Function: Configures an option 43 string in ASCII format in DHCP Address Pool Mode. The **no** form of this command deletes the configured option 43.

Parameters: LINE: The option 43 string in ASCII format, from 1 to 255 characters.

Default: No option 43 string is configured.

Command Mode: DHCP Address Pool Mode.

Usage Guidelines: None.

Example: Configure option 43 in ASCII format as "AP 1000".

```
switch(config)#ip dhcp pool a
switch (dhcp-a-config)#option 43 ascii AP 1000
```

4.18.2 option 43 hex WORD

Command: `option 43 hex WORD`
`no option 43`

Function: Configures an option 43 string in hexadecimal format in DHCP Address Pool Mode. The **no** form of this command deletes the configured option 43.

Parameters: WORD: The option 43 string in hexadecimal format, such as a1241b.

Default: No option 43 is configured.

Command Mode: DHCP Address Pool Mode.

Usage Guidelines: When option 43 is configured in hexadecimal format, the string must be written in TLV (type-length-value) format. For example, to deliver IP address 10.1.1.1 through option 43, use the string 01040A010101, where Type = 0x01 (IP address), Length = 0x04 (the IP address is 4 bytes long), and Value = 0x0A010101 (10.1.1.1 in hexadecimal).

Example: Configure option 43 in hexadecimal format as "01040a010101".

```
switch(config)#ip dhcp pool a
switch (dhcp-a-config)#option 43 hex 01040a010101
```

4.18.3 option 43 ip A.B.C.D

Command: `option 43 ip A.B.C.D`
`no option 43`

Function: Configures option 43 in IP address format in DHCP Address Pool Mode. The **no** form of this command deletes the configured option 43.

Parameters: A.B.C.D: Option 43 in IP address format, such as 192.168.1.1.

Default: No option 43 is configured.

Command Mode: DHCP Address Pool Mode.

Usage Guidelines: If option 43 is configured with this command as, for example, "192.168.1.1", the option 43 value filled into packets is "C0A80101".

Example: Configure option 43 in IP address format as "192.168.1.1".

```
switch(config)#ip dhcp pool a
switch (dhcp-a-config)#option 43 ip 192.168.1.1
```

4.18.4 option 60 ascii LINE

Command: `option 60 ascii LINE`
`no option 60`

Function: Configures an option 60 string in ASCII format in DHCP Address Pool Mode. The **no** form of this command deletes the configured option 60.

Parameters: LINE: The option 60 string in ASCII format, from 1 to 255 characters.

Default: No option 60 string is configured.

Command Mode: DHCP Address Pool Mode.

Usage Guidelines: None.

Example: Configure option 60 in ASCII format as "AP 1000".

```
switch(config)#ip dhcp pool a
switch (dhcp-a-config)#option 60 ascii AP 1000
```

4.18.5 option 60 hex WORD

Command: `option 60 hex WORD`
`no option 60`

Function: Configures an option 60 string in hexadecimal format in DHCP Address Pool Mode. The **no** form of this command deletes the configured option 60.

Parameters: WORD: The option 60 string in hexadecimal format, such as a1241b.

Default: No option 60 is configured.

Command Mode: DHCP Address Pool Mode.

Usage Guidelines: None.

Example: Configure option 60 in hexadecimal format as "41502031303030".

```
switch(config)#ip dhcp pool a
switch(dhcp-a-config)#option 60 hex 41502031303030
```

4.18.6 option 60 ip A.B.C.D

Command: `option 60 ip A.B.C.D`
`no option 60`

Function: Configures option 60 in IP address format in DHCP Address Pool Mode. The **no** form of this command deletes the configured option 60.

Parameters: A.B.C.D: Option 60 in IP address format, such as 192.168.1.1.

Default: No option 60 is configured.

Command Mode: DHCP Address Pool Mode.

Usage Guidelines: If option 60 is configured with this command as, for example, "192.168.1.1", packets whose option 60 is "C0A80101" match the configured option 60.

Example: Configure option 60 in IP address format as "192.168.1.1".

```
switch(config)#ip dhcp pool a
switch (dhcp-a-config)#option 60 ip 192.168.1.1
```

Chapter 5 Commands for Routing Protocols

5.1 Routing Protocol Overview

5.1.1 ip prefix-list description

Command: ip prefix-list <list_name> description <description>
no ip prefix-list <list_name> description

Function: Configures the description of a prefix list. The **no ip prefix-list <list_name> description** command deletes the description.

Parameters: <list_name> is the prefix list name; **<description>** is the description text.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: Use this command to describe a prefix list, for example, its purpose and points to note.

Example:

```
Switch#config terminal
Switch(config)#ip prefix-list 3 description This list is used by BGP
```

5.1.2 ip prefix-list seq

Command: ip prefix-list <list_name> [seq <sequence_number>] <deny | permit> < any | ip_addr/mask_length [ge <min_prefix_len>] [le <max_prefix_len>]>
no ip prefix-list <list_name> [seq <sequence_number>] [<deny | permit> < any | ip_addr/mask_length [ge <min_prefix_len>] [le <max_prefix_len>]>]

Function: Configures a prefix list. The **no** form of this command deletes the prefix list or entry.

Parameters: <list_name> is the prefix list name. **seq** indicates that a sequence number follows; **<sequence_number>** is the sequence number. **deny** denies the route; **permit** permits the route. **any** matches any prefix with any mask length. **ip_addr/mask_length** is the prefix address (in dotted decimal notation) and mask length. **ge** means greater than or equal to; **<min_prefix_len>** is the minimum prefix length to match, from 0 to 32. **le** means less than or equal to; **<max_prefix_len>** is the maximum prefix length to match, from 0 to 32.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: A prefix list is identified by its name. Each prefix list can contain several entries, each of which specifies a network prefix matching range and is identified by a sequence number. The sequence number determines the order of matching checks: the switch checks the entries in ascending order of sequence number, and once an entry matches, the route passes the prefix list filter without checking further entries.

Note that when a prefix list has more than one entry, at least one entry must be in permit mode. Deny entries can be defined first to quickly remove unwanted routing information, but if all entries are in deny mode, no route can pass the prefix list. You can define a "permit 0.0.0.0/0 ge 0 le 32" entry after several deny entries to allow all other routing information to pass.

Example:

```
Switch#config terminal
Switch(config)#ip prefix-list mylist seq 12345 deny 10.0.0.0/8 le 22 ge 14
```

5.1.3 ip prefix-list sequence-number

Command: `ip prefix-list sequence-number`
`no ip prefix-list sequence-number`

Function: Enables automatic generation of prefix list sequence numbers. The **no ip prefix-list sequence-number** command disables it.

Parameters: None.

Default: Enabled.

Command Mode: Global Mode.

Usage Guidelines: Use the **no** form of this command to disable automatic generation of prefix list sequence numbers.

Example:

```
Switch(config)#no ip prefix-list sequence-number
```

5.1.4 match as-path

Command: `match as-path <list-name>`
`no match as-path [<list-name>]`

Function: Configures matching of the AS path attribute of BGP routes. The **no match as-path [<list-name>]** command deletes this configuration.

Parameters: <list-name> is the name of the AS path access list.

Command Mode: Route-Map Mode.

Usage Guidelines: This command matches the AS path attribute of BGP routes against the rules in the AS path list. If the match succeeds, the permit or deny action of the route map is performed.

Example:

```
Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#match as-path 60
```

5.1.5 match community

Command: `match community <community-list-name | community-list-num> [exact-match]`
`no match community [<community-list-name | community-list-num> [exact-match]]`

Function: Configures matching of the community attribute of BGP routes. The **no match community [...]** command deletes this configuration.

Parameters: <community-list-name> is the name of the community list. **<community-list-num>** is the community list number, from 1 to 99 (standard) or 100 to 199 (extended). **exact-match** requires an exact match.

Command Mode: Route-Map Mode.

Usage Guidelines: This command matches the community attribute of BGP routes against the rules in the community list. If the match succeeds, the permit or deny action of the route map is performed.

Example:

```
Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#match community 100 exact-match
```

5.1.6 match interface

Command: `match interface <interface-name >`
`no match interface [<interface-name >]`

Function: Configures matching of interfaces. The **no match interface [<interface-name>]** command deletes this configuration.

Parameters: <interface-name> is the interface name.

Command Mode: Route-Map Mode.

Usage Guidelines: This command matches routes by their next-hop interface. If the match succeeds, the permit or deny action of the route map is performed. This command is used only with RIP and OSPF.

Example:

```
Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#match interface vlan1
```

5.1.7 match ip

Command: `match ip <address | next-hop> <ip-acl -name | ip-acl -num | prefix-list list-name>`
`no match ip <address | next-hop> [<ip-acl -name | ip-acl -num | prefix-list list-name>]`

Function: Configures matching of the route prefix or next hop. The **no match ip <address | next-hop> [...]** command deletes this configuration.

Parameters: address matches the route prefix; **next-hop** matches the route next hop. **<ip-acl-name>** is the name of an IP access list. **<ip-acl-num>** is the IP access list number, from 1 to 199 or 1300 to 2699 (extended range). **prefix-list** matches according to the prefix list rules; **<list-name>** is the prefix list name.

Command Mode: Route-Map Mode.

Usage Guidelines: This command matches routes by next hop or route prefix. If the match succeeds, the permit or deny action of the route map is performed.

Example:

```
Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#match ip address prefix-list mylist
```

5.1.8 match ipv6 address

Command: `match ipv6 address <ipv6-acl-name | prefix-list list-name>`
`no match ipv6 address [<ipv6-acl-name | prefix-list list-name>]`

Function: Configures matching of IPv6 route prefixes. The **no** form of this command deletes the configuration.

Parameters: address matches the route prefix. **<ipv6-acl-name>** is the name of an IPv6 access list. If **prefix-list** is specified, **<list-name>** is the name of the prefix list to match.

Command Mode: Route-map Mode.

Usage Guidelines: When this command is configured, routes are matched against the specified access list or prefix list. If the match succeeds, the permit or deny action of the route map is performed.

Example:

```
Switch#config terminal
```

```
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#match ipv6 address prefix-list mylist
```

5.1.9 match ipv6 next-hop

Command: match ipv6 next-hop <ipv6-address>
no match ipv6 next-hop [<ipv6-address>]

Function: Configures matching of the IPv6 route next hop. The **no** form of this command deletes the configuration.

Parameters: next-hop matches the next hop of the route. **<ipv6-address>** is the IPv6 address of the next-hop interface.

Command Mode: Route-map Mode.

Usage Guidelines: When this command is configured, routes are matched by the next-hop information in the routing table. If the match succeeds, the permit or deny action of the route map is performed.

Example:

```
Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)# match ipv6 next-hop 2000::1
```

5.1.10 match metric

Command: match metric <metric-val >
no match metric [<metric-val >]

Function: Matches the metric value of routes. The **no match metric [<metric-val>]** command deletes the configuration.

Parameters: <metric-val> is the metric value, from 0 to 4294967295.

Command Mode: Route-Map Mode.

Usage Guidelines: This command matches routes by metric value. If the match succeeds, the permit or deny action of the route map is performed.

Example:

```
Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#match metric 60
```

5.1.11 match origin

Command: match origin <egp | igp | incomplete >
no match origin <egp | igp | incomplete >

Function: Configures matching of the origin attribute of BGP routes. The **no match origin <egp | igp | incomplete>** command deletes the configuration.

Parameters: egp: The route was learned from an exterior gateway protocol. **igp**: The route was learned from an interior gateway protocol. **incomplete**: The route origin is unknown.

Command Mode: Route-Map Mode.

Usage Guidelines: This command matches BGP routes by origin. If the match succeeds, the permit or deny action of the route map is performed.

Example:

```
Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#match origin egp
```

5.1.12 match route-type

Command: match route-type external <type-1 | type-2 >
no match route-type external [<type-1 | type-2 >]

Function: Configures matching of the route type of OSPF routes. The **no match route-type external [<type-1 | type-2>]** command deletes the configuration.

Parameters: type-1 matches OSPF type 1 external routes; **type-2** matches OSPF type 2 external routes.

Command Mode: Route-Map Mode.

Usage Guidelines: This command matches OSPF routes by type (the type of the OSPF AS-external LSA: type 1 or type 2). If the match succeeds, the permit or deny action of the route map is performed.

Example:

```
Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#match route-type external type-1
```

5.1.13 match tag

Command: match tag <tag-val >
no match tag [<tag-val >]

Function: Configures matching of the tag of OSPF routes. The **no match tag [<tag-val>]** command deletes this configuration.

Parameters: <tag-val> is the tag value, from 0 to 4294967295.

Command Mode: Route-Map Mode.

Usage Guidelines: This command matches OSPF routes by tag value. If the match succeeds, the permit or deny action of the route map is performed.

Example:

```
Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#match tag 60
```

5.1.14 route-map

Command: route-map <map_name> {deny | permit} <sequence_num>
no route-map <map_name> [{deny | permit} <sequence_num>]

Function: Configures a route map and enters Route-map Mode. The **no route-map <map_name> [{deny | permit} <sequence_num>]** command deletes the route map.

Parameters: <map_name> is the route map name. **permit** sets the matching mode of the route map node to permit. **deny** sets the matching mode to deny (set clauses are not executed in this mode). **<sequence_num>** is the sequence number of the route map node, from 1 to 65535.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: A route map can consist of several nodes, each of which is a check unit. The order in which nodes are checked is determined by their sequence numbers. In permit mode, if a route meets all match clauses of a node, it passes the node filter, all set clauses of the node are executed, and no further nodes are checked; if the route does not meet the match clauses, the next node is checked. Nodes have an OR relationship: the switch checks each node of the route map in turn, and the route passes the route map filter as soon as it passes one node.

Note that when more than one node is defined, at least one node must be in permit mode. When a route map is used to filter routing information, a route that passes no node is considered denied by the route map. If all nodes of a route map are in deny mode, no routing information can pass the route map.

Example:

```
Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#match as-path 60
Switch(config-route-map)#set weight 30
```

5.1.15 set aggregator

Command: `set aggregator as <as-number> <ip_addr>`
`no set aggregator as [<as-number> <ip_addr>]`

Function: Configures the AS number of the BGP aggregator. The **no set aggregator as [<as-number> <ip_addr>]** command deletes this configuration.

Parameters: <as-number> is the AS number. **<ip_addr>** is the IP address of the aggregator, in dotted decimal notation.

Command Mode: Route-Map Mode.

Usage Guidelines: At least one match clause must be defined before this command is used.

Example:

```
Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#set aggregator as 200 10.1.1.1
```

5.1.16 set as-path

Command: `set as-path prepend <as-num>`
`no set as-path prepend [<as-num>]`

Function: Prepends AS numbers to the AS path attribute of BGP routes. The **no set as-path prepend [<as-num>]** command deletes this configuration.

Parameters: <as-num> is the AS number, from 1 to 4294967295, in plain notation (such as 6553700) or dotted notation (such as 100.100). Multiple AS numbers can be entered.

Command Mode: Route-Map Mode.

Usage Guidelines: Prepending AS numbers lengthens the AS path and thus influences BGP best-path selection by neighbors. At least one match clause must be defined before this command is used.

Example:

```
Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#set as-path prepend 200 100.100
```

5.1.17 set atomic-aggregate

Command: `set atomic-aggregate`
`no set atomic-aggregate`

Function: Configures the atomic aggregate attribute. The **no set atomic-aggregate** command deletes this configuration.

Parameters: None.

Command Mode: Route-Map Mode.

Usage Guidelines: BGP uses the atomic aggregate attribute to inform other BGP speakers that the local system selected a less specific route instead of the more specific routes it contains. At least one match clause must be defined before this command is used.

Example:

```
Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#set atomic-aggregate
```

5.1.18 set comm-list

Command: set comm-list <community-list-name | community-list-num > delete
no set comm-list <community-list-name | community-list-num > delete

Function: Deletes community attributes from inbound or outbound routes. The **no set comm-list <...> delete** command deletes the configuration.

Parameters: <community-list-name> is the name of the community list. **<community-list-num>** is the community list number, from 1 to 99 (standard) or 100 to 199 (extended).

Command Mode: Route-Map Mode.

Example:

```
Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#set comm-list 100 delete
```

5.1.19 set community

Command: set community [AA:NN] [internet] [local-AS] [no-advertise] [no-export] [none] [additive]
no set community [AA:NN] [internet] [local-AS] [no-advertise] [no-export] [none] [additive]

Function: Configures the community attribute of BGP routes. The **no set community [...]** command deletes this configuration.

Parameters: AA:NN is the community attribute value. **internet** specifies the Internet community. **local-AS** specifies that the route is not advertised outside the local AS (but can be advertised to sub-ASs within a confederation). **no-advertise** specifies that the route is not advertised to any neighbor. **no-export** specifies that the route is not advertised to EBGP neighbors. **none** removes the community attribute from the route prefix. **additive** adds the attribute to the existing community attributes.

Command Mode: Route-Map Mode.

Usage Guidelines: At least one match clause must be defined before this command is used.

Example:

```
Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#set community local-as additive
```

5.1.20 set extcommunity

Command: set extcommunity <rt | soo> <AA:NN>
no set extcommunity <rt | soo> [<AA:NN>]

Function: Configures the extended community attribute of BGP routes. The **no set extcommunity <rt | soo> [<AA:NN>]** command deletes this configuration.

Parameters: rt is the route target. **soo** is the site of origin. **<AA:NN>** is the community attribute value, where AA is the AS number, from 1 to 4294967295, in plain notation (such as 6553700) or dotted notation (such as 100.100), and NN is an arbitrary 2-byte number.

Command Mode: Route-Map Mode.

Usage Guidelines: At least one match clause must be defined before this command is used.

Example: Set the route target to 100:10.

```
Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#set extcommunity rt 100:10
```

Set the site of origin to 200.200:10.

```
Switch(config)#route-map r1 permit 10
Switch(config-route-map)#set extcommunity soo 200.200:10
```

5.1.21 set ip next-hop

Command: set ip next-hop <ip_addr>
no set ip next-hop [<ip_addr>]

Function: Configures the next hop of routes. The **no set ip next-hop [<ip_addr>]** command deletes the configuration.

Parameters: <ip_addr> is the next-hop IP address, in dotted decimal notation.

Command Mode: Route-Map Mode.

Example:

```
Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#set ip next-hop 10.2.2.2
```

5.1.22 set local-preference

Command: set local-preference <pre_val>
no set local-preference [<pre_val>]

Function: Configures the local preference of BGP routes. The **no set local-preference [<pre_val>]** command deletes this configuration.

Parameters: <pre_val> is the local preference value, from 0 to 4294967295.

Command Mode: Route-Map Mode.

Usage Guidelines: The local preference attribute indicates the preference of a route. Among routes to the same destination, the route with the higher local preference is preferred. Local preference applies only within the local AS and is not sent to EBGP neighbors. At least one match clause must be defined before this command is used.

Example:

```
Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#set local-preference 60
```

5.1.23 set metric

Command: set metric < metric_val>
no set metric [< metric_val>]

Function: Configures the metric value of routes. The **no set metric [<metric_val>]** command deletes the configuration.

Parameters: <metric_val> is the metric value, from 1 to 4294967295.

Command Mode: Route-Map Mode.

Usage Guidelines: The metric value affects only path selection from external neighbors into the local AS; the lower the metric, the higher the priority. Normally, only the metrics of paths from neighbors in the same AS are compared. To also compare the metrics of paths from different neighbors, configure the **bgp always-compare-med** command. At least one match clause must be defined before this command is used.

Example:

```
Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#set metric 60
```

5.1.24 set metric-type

Command: set metric-type <type-1 | type-2>
no set metric-type [<type-1 | type-2>]

Function: Configures the metric type of OSPF routes. The **no set metric-type [<type-1 | type-2>]** command deletes this configuration.

Parameters: type-1 sets OSPF type 1 external routes; **type-2** sets OSPF type 2 external routes.

Command Mode: Route-Map Mode.

Usage Guidelines: At least one match clause must be defined before this command is used.

Example:

```
Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#set metric-type type-1
```

5.1.25 set origin

Command: set origin <egp | igp | incomplete >
no set origin [<egp | igp | incomplete >]

Function: Configures the origin code of BGP routes. The **no set origin [<egp | igp | incomplete>]** command deletes this configuration.

Parameters: egp: The route was learned from an exterior gateway protocol. **igp**: The route was learned from an interior gateway protocol. **incomplete**: The route origin is unknown.

Command Mode: Route-Map Mode.

Usage Guidelines: At least one match clause must be defined before this command is used.

Example:

```
Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#set origin egp
```

5.1.26 set originator-id

Command: set originator-id <ip_addr>
no set originator-id [<ip_addr>]

Function: Configures the originator IP address of BGP routes. The **no set originator-id [<ip_addr>]** command deletes the configuration.

Parameters: <ip_addr> is the IP address of the route originator, in dotted decimal notation.

Command Mode: Route-Map Mode.

Usage Guidelines: At least one match clause must be defined before this command is used.

Example:

```
Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#set originator-id 10.1.1.1
```

5.1.27 set tag

Command: `set tag <tag_val>`
`no set tag [<tag_val>]`

Function: Configures the tag of OSPF routes. The **no set tag [<tag_val>]** command deletes this configuration.

Parameters: <tag_val> is the tag value, from 0 to 4294967295.

Command Mode: Route-Map Mode.

Usage Guidelines: AS-external LSAs contain a route tag field, which is normally set by other routing protocols. At least one match clause must be defined before this command is used.

Example:

```
Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#set tag 60
```

5.1.28 set vpnv4 next-hop

Command: `set vpnv4 next-hop <ip_addr>`
`no set vpnv4 next-hop [<ip_addr>]`

Function: Configures the next hop of BGP VPNv4 routes. The **no** form of this command deletes the configuration.

Parameters: <ip_addr> is the next-hop IP address of VPNv4 routes, in dotted decimal notation.

Command Mode: Route-Map Mode.

Usage Guidelines: At least one match clause must be defined before this command is used.

Example:

```
Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#set vpnv4 next-hop 10.1.1.1
```

5.1.29 set weight

Command: `set weight <weight_val>`
`no set weight [<weight_val>]`

Function: Configures the weight of BGP routes. The **no set weight [<weight_val>]** command deletes this configuration.

Parameters: <weight_val> is the weight value, from 0 to 4294967295.

Command Mode: Route-Map Mode.

Usage Guidelines: The weight is used in best-path selection and applies only to the local switch. Among several routes to the same destination, the route with the higher weight is preferred. At least one match clause must be defined before this command is used.

Example:

```
Switch#config terminal
Switch(config)#route-map r1 permit 5
Switch(config-route-map)#set weight 60
```

5.1.30 show ip prefix-list <list-name>

Command: show ip prefix-list [<list-name> [<ip_addr/len> [first-match | longer] | seq <sequence-number>]]

Function: Displays prefix lists by name.

Parameters: <list-name> is the prefix list name. **<ip_addr/len>** is the prefix IP address and mask length. **first-match** displays the first entry that matches the specified IP address. **longer** displays entries with longer prefixes. **seq** displays entries by sequence number; **<sequence-number>** is the sequence number, from 0 to 4294967295.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: If no prefix list name is specified, all prefix lists are displayed.

Example:

```
Switch#show ip prefix-list
ip prefix-list 1: 1 entries
   deny any
ip prefix-list mylist: 1 entries
   deny 1.1.1.1/8
Switch#show ip prefix-list mylist 1.1.1.1/8
   seq 5 deny 1.1.1.1/8 (hit count: 0, recount: 0)
```

Field	Description
ip prefix-list mylist: 1 entries	A prefix list named mylist with 1 entry.
seq 5 deny 1.1.1.1/8 (hit count: 0, recount: 0)	The prefix list entry with sequence number 5. "hit count: 0" means the entry has been matched 0 times; "recount: 0" means it has been referenced 0 times.

5.1.31 show ip prefix-list <detail | summary>

Command: show ip prefix-list [<detail | summary> [<list-name>]]

Function: Displays the contents of prefix lists.

Parameters: detail displays detailed prefix list information; **summary** displays summary information. **<list-name>** is the prefix list name.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: If no prefix list name is specified, all prefix lists are displayed.

Example:

```
Switch#show ip prefix-list detail mylist
ip prefix-list mylist:
count: 2, range entries: 0, sequences: 5 - 10
seq 5 deny 1.1.1.1/8 (hit count: 0, refcount: 0)
seq 10 permit 2.2.2.2/8 (hit count: 0, refcount: 0)
Switch#show ip prefix-list summary mylist
ip prefix-list mylist:
count: 2, range entries: 0, sequences: 5 – 10
```

Output	Description
ip prefix-list mylist:	Displays the prefix list named mylist.
count: 2, range entries: 0, sequences: 5 - 10	**count: 2** indicates that there are two prefix list entries. **sequences: 5 - 10** indicates the sequence numbers; 5 is the first and 10 is the last.
deny 1.1.1.1/8 (hit count: 0, refcount: 0)	**deny 1.1.1.1/8** is the content of the prefix list entry. **hit count: 0** indicates that the rule has

	been matched 0 times, and **refcount: 0** indicates that the rule has been referenced 0 times.

5.1.32 show route-map

Command: `show route-map`

Function: Displays the route maps.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example:

```
Switch# show route-map
route-map a, deny, sequence 10
  Match clauses:
    as-path 60
  Set clauses:
    metric 10
```

Output	Description
route-map a, deny, sequence 10	**route-map a** is the route map name, **deny** is the matching mode, and **sequence 10** is the sequence number.
Match clauses:	Match clauses
as-path 60	Contents of the match clause
Set clauses:	Set clauses
metric 10	Contents of the set clause

5.1.33 show router-id

Command: `show router-id`

Function: Displays the router ID.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
1:
Switch#show router-id
Router ID: 20.1.1.1 (automatic)
2:
Switch#show router-id
Router ID: 20.1.1.2 (config)
```

5.2 Static Route

5.2.1 ip route

Command: `ip route {<ip-prefix> <mask> | <ip-prefix>/<prefix-length>} {<gateway-address> | <gateway-interface>} [<distance>]`
`no ip route {<ip-prefix> <mask> | <ip-prefix>/<prefix-length>} [<gateway-address> | <gateway-interface>] [<distance>]`

Function: Configures a static route. The **no ip route** command deletes the static route.

Parameters: <ip-prefix> and **<mask>** are the destination IP address and subnet mask in dotted decimal notation. **<ip-prefix>/<prefix-length>** is the destination IP address and prefix length. **<gateway-address>** is the next-hop IP address in dotted decimal notation. **<gateway-interface>** is the next-hop (egress) interface. **<distance>** is the administrative distance of the route, ranging from 1 to 255.

Default: The administrative distance of a static route is 1.

Command Mode: Global Mode.

Usage Guidelines: When you configure a static route, you can specify either the next-hop IP address or the egress interface.

The default administrative distances of the route types are listed below:

Route Type	Distance
Direct route	0
Static route	1
OSPF	110
RIP	120
IBGP	200
EBGP	20

With the default administrative distances, direct routes have the highest priority, followed by static routes, EBGP, OSPF, RIP, and IBGP routes.

Example:

Example 1: Add a static route.

```
Switch(config)#ip route 1.1.1.0 255.255.255.0 2.1.1.1
```

Example 2: Add a default route.

```
Switch(config)#ip route 0.0.0.0 0.0.0.0 2.2.2.1
```

5.2.2 ip route vrf

Command: ip route vrf <vrf-name> {<ip-prefix> <mask>|<ip-prefix/prefix-length>} {<gateway-address>|null0} [<1-255>]
no ip route vrf <vrf-name> {<ip-prefix> <mask>|<ip-prefix/prefix-length>} {<gateway-address>|null0} [<1-255>]

Function: Configures a static route for the specified VRF. A VPN routing and forwarding (VRF) instance must be configured before you use this command. The **no** form of this command deletes the configuration.

Parameters: <vrf-name>: The VRF name.

<ip-prefix>: The destination IP address.

<mask>: The subnet mask in dotted decimal notation.

<prefix-length>: The prefix length.

<gateway-address>: The next-hop address.

null0: A black-hole route.

<1-255>: The administrative distance.

Default: Not configured.

Command Mode: Global Mode.

Usage Guidelines: The following example configures a static route for VRF-A with destination 10.1.1.10, a 24-bit mask, next hop 10.1.1.1, and the default administrative distance:

```
Switch(config)# ip route vrf VRF-A 10.1.1.10 255.255.255.0 10.1.1.1
Switch(config)#
```

5.2.3 show ip route

Command: show ip route [<destination>|<destination >|<length>|connected | static | rip| ospf | bgp | isis| kernel| statistics| database [connected | static | rip| ospf | bgp | isis| kernel] | fib[statistics]]

Function: Displays the routing table.

Parameters: <destination> is the destination network address. **<destination>/<length>** is the destination network address and prefix length. **connected**: direct routes. **static**: static routes. **rip**: RIP routes. **ospf**: OSPF routes. **bgp**: BGP routes. **isis**: IS-IS routes. **kernel**: kernel routes. **statistics**: displays the number of routes. **database**: the route database. **fib**: the kernel routing table.

Command Mode: All Modes.

Usage Guidelines: Displays the contents of the routing table, including the route type, destination network, mask, next-hop address, and interface.

Example:

```
switch#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default
Gateway of last resort is 210.0.0.3 to network 0.0.0.0
S*     0.0.0.0/0 [1/0] via 210.0.0.3, Vlan1
C     127.0.0.0/8 is directly connected, Loopback
O IA   172.16.11.0/24 [110/40] via 210.14.0.1, Vlan3014, 00:00:47
O IA   172.16.12.0/24 [110/40] via 210.14.0.1, Vlan3014, 00:00:47
O IA   172.16.13.0/24 [110/40] via 210.14.0.1, Vlan3014, 00:00:47
O IA   172.16.14.0/24 [110/40] via 210.14.0.1, Vlan3014, 00:00:47
O IA   172.16.15.0/24 [110/50] via 210.14.0.1, Vlan3014, 00:00:47
O E2  172.16.100.0/24 [110/0] via 210.14.0.1, Vlan3014, 00:00:46
```

Output	Description
C –connected	Direct route: a network segment directly connected to the Layer 3 switch
S –static	Static route: a route manually configured by the user
R - RIP derived	RIP route: a route learned through the RIP protocol
O - OSPF derived	OSPF route: a route learned through the OSPF protocol
A- OSPF ASE	Route imported by OSPF
B- BGP derived	BGP route: a route learned through the BGP protocol
Destination	Destination network
Mask	Destination network mask
Nexthop	Next-hop IP address
Interface	Layer 3 switch interface through which the next hop is reached
Preference	Route priority. If routes of other types to the same destination network exist, the kernel routing table shows only the route with the highest priority.

5.2.4 show ip route vrf

Command: show ip route vrf <name> [connected | static | rip| ospf | bgp | isis| kernel|statistics| database[connected | static | rip| ospf | bgp | isis|kernel]]
show ip route fib vrf <name> [default|main|local]

Function: Displays the routing table entries of a VRF.

Parameters: <name> is the name of the VPN routing and forwarding instance. **<destination>** is the destination address. **<destination>/<length>** is the destination network address and prefix length. **connected**: direct routes. **static**: static routes. **rip**: RIP routes. **ospf**: OSPF routes. **bgp**: BGP routes. **isis**: IS-IS routes. **kernel**: kernel routes. **statistics**: displays the number of route entries. **database**: the route database. **fib**: the kernel routing table.

Command Mode: All Modes.

Usage Guidelines: Displays the contents of the VPN routing table, including the route type, destination network address, mask, and next-hop address and interface.

5.3 RIP

5.3.1 accept-lifetime

Command: accept-lifetime <start-time> {<end-time>| duration<seconds>| infinite}
no accept-lifetime

Function: Specifies the period during which a key on the key chain is accepted as valid. The **no accept-lifetime** command deletes this configuration.

Parameters: <start-time> specifies the start of the period in the following format:

<start-time>={<hh:mm:ss> <month> <day> <year>|<hh:mm:ss> <day> <month> <year>}

<hh:mm:ss>: The time of day, in hours, minutes, and seconds.

<day>: The day of the month, ranging from 1 to 31.

<month>: The month, given as the first three letters of its name, such as Jan.

<year>: The year, ranging from 1993 to 2035.

<end-time> specifies the end of the period in the following format:

<end-time>={<hh:mm:ss> <month> <day> <year>|<hh:mm:ss> <day> <month> <year>}

<hh:mm:ss>: The time of day, in hours, minutes, and seconds.

<day>: The day of the month, ranging from 1 to 31.

<month>: The month, given as the first three letters of its name, such as Jan.

<year>: The year, ranging from 1993 to 2035.

<seconds>: The validity period of the key in seconds, ranging from 1 to 2147483646.

infinite: The key never expires.

Default: None.

Command Mode: Keychain-Key Mode.

Usage Guidelines: None.

Example: Configure the accept lifetime of key 1 on the key chain named mychain.

```
Switch# config terminal
Switch(config)# key chain mychain
Switch(config-keychain)# key 1
```

```
Switch(config-keychain-key)# accept-lifetime 03:03:01 Dec 3 2004 04:04:02 Oct
6 2006
```

Related Commands:

key

key-string

key chain

send-lifetime

5.3.2 address-family ipv4

Command: address-family ipv4 vrf <vrf-name>
no address-family ipv4 vrf <vrf-name>

Function: Enables routing information exchange for the specified VRF and enters Address-family Mode. The **no** form of this command deletes the RIP instance associated with the VRF.

Parameters: <vrf-name> is the name of the VPN routing and forwarding instance.

Command Mode: Router Mode.

Usage Guidelines: This command is used only on PE routers. Before using this command, create the VRF with the **ip vrf** command; this command then associates the VRF with a RIP instance.

Example:

```
Switch# config terminal
Switch(config)# router rip
Switch(config-router)# address-family ipv4 vrf VRF1
Switch(config-router-af)#
```

5.3.3 clear ip rip route

Command: clear ip rip route {<A.B.C.D/M> | kernel | static | connected | rip | ospf | isis | bgp | all}

Function: Clears the specified routes from the RIP routing table.

Parameters: <A.B.C.D/M>: Clears the routes that match the destination address (IP address prefix and prefix length) from the RIP routing table.

kernel: Deletes kernel routes from the RIP routing table.

static: Deletes static routes from the RIP routing table.

connected: Deletes direct routes from the RIP routing table.

rip: Deletes only RIP routes from the RIP routing table.

ospf: Deletes only OSPF routes from the RIP routing table.

isis: Deletes only IS-IS routes from the RIP routing table.

bgp: Deletes only BGP routes from the RIP routing table.

all: Deletes all routes from the RIP routing table.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: When **all** is specified, all learned routes are deleted from the RIP routing table. All routes except RIP routes are restored immediately; dynamically learned RIP routes are restored only when they are learned again.

Example:

```
Switch# clear ip rip route 10.0.0.0/8
Switch# clear ip rip route ospf
```

5.3.4 debug rip

Command: debug rip [events| nsm| packet[recv|send][detail]| all]
no debug rip [events| nsm| packet[recv|send][detail]| all]

Function: Enables RIP debugging and displays the corresponding debugging messages. The **no debug rip** command disables the corresponding debugging.

Parameters: events: Displays debugging messages for RIP events.

nsm: Displays messages exchanged between RIP and the NSM.

packet: Displays debugging messages for RIP packets.

recv: Displays messages for received packets.

send: Displays messages for sent packets.

detail: Displays detailed messages for received or sent packets.

Default: Disabled.

Command Mode: Admin Mode and Global Mode.

Example:

```
Switch# debug rip packet
Switch#1970/01/01 01:01:43 IMI: SEND[Vlan1]: Send to 224.0.0.9:520
1970/01/01 01:01:43 IMI: SEND[Vlan1]: Send to 224.0.0.9:520
1970/01/01 01:01:47 IMI: RECV[Vlan1]: Receive from 20.1.1.2:520
```

5.3.5 debug rip redistribute message send

Command: debug rip redistribute message send
no debug rip redistribute message send

Function: Enables debugging of the redistribution messages that RIP sends for routes from OSPF or BGP. The **no** form of this command disables this debugging.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example:

```
Switch#debug rip redistribute message send
Switch#no debug rip redistribute message send
```

5.3.6 debug rip redistribute route receive

Command: debug rip redistribute route receive
no debug rip redistribute route receive

Function: Enables debugging of messages that RIP receives from the NSM. The **no** form of this command disables this debugging.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example:

```
Switch#debug rip redistribute route receive
Switch#no debug rip redistribute route receive
```

5.3.7 default-information originate

Command: `default-information originate`
`no default-information originate`

Function: Allows the default route (0.0.0.0) to be redistributed into RIP. The **no default-information originate** command disables this function.

Parameters: None.

Default: Disabled.

Command Mode: Router Mode and Address Family Mode.

Example:

```
Switch# config terminal
Switch(config)# router rip
Switch(config-router)# default-information originate
```

5.3.8 default-metric

Command: `default-metric <value>`
`no default-metric`

Function: Sets the default metric for redistributed routes. The **no default-metric** command restores the default value of 1.

Parameters: <value> is the metric, ranging from 1 to 16.

Default: 1.

Command Mode: Router Mode and Address Family Mode.

Usage Guidelines: The **default-metric** command sets the default metric for routes from other routing protocols that are redistributed into RIP. When routes are imported with the **redistribute** command and no metric is specified, the metric set by **default-metric** is used.

Example: Set the default metric to 3 for routes redistributed into RIP from other routing protocols.

```
Switch(config-router)#default-metric 3
```

Related Commands: redistribute

5.3.9 distance

Command: `distance <number> [<A.B.C.D/M>] [<access-list-name | access-list-number >]`
`no distance [<A.B.C.D/M> ]`

Function: Sets the administrative distance. The **no distance [<A.B.C.D/M>]** command restores the default value of 120.

Parameters: <number> specifies the distance, ranging from 1 to 255. **<A.B.C.D/M>** specifies the network prefix and prefix length. **<access-list-name | access-list-number>** specifies the name or number of the access list to apply.

Default: The default administrative distance of RIP is 120.

Command Mode: Router Mode and Address Family Mode.

Usage Guidelines: When two routing protocols provide routes to the same destination, the administrative distance is used to select the route. The lower the administrative distance of a routing protocol, the more reliable its routes are considered.

Example:

```
Switch# config terminal
Switch(config)# router rip
Switch(config-router)# distance 8 10.0.0.0/8 mylist
```

5.3.10 distribute-list

Command: distribute-list {<access-list-number | access-list-name> | prefix<prefix-list-name>} {in|out} [<ifname>]
no distribute-list {<access-list-number| access-list-name> | prefix<prefix-list-name>} {in|out} [<ifname>]

Function: Uses an access list or prefix list to filter the routing updates sent and received. The **no distribute-list** command cancels this route filtering.

Parameters: <access-list-number | access-list-name> is the number or name of the access list to apply. **<prefix-list-name>** is the name of the prefix list to apply. **<ifname>** specifies the interface on which route filtering is applied.

Default: Disabled.

Command Mode: Router Mode and Address Family Mode.

Usage Guidelines: If no interface is specified, the filter is applied to all interfaces.

Example:

```
Switch# config terminal
Switch(config)# router rip
Switch(config-router)# distribute-list prefix myfilter in vlan 1
```

5.3.11 exit-address-family

Command: exit-address-family

Function: Exits Address-family Mode.

Command Mode: Address Family Mode.

Example:

```
Switch(config)# router rip
Switch(config-router)# address-family ipv4 vrf IPI
Switch(config-router-af)# exit-address-family
Switch(config-router)#
```

5.3.12 ip rip aggregate-address

Command: ip rip aggregate-address A.B.C.D/M
no ip rip aggregate-address A.B.C.D/M

Function: Configures a RIP aggregate route. The **no** form of this command deletes the configuration.

Parameters: A.B.C.D/M: The IPv4 address and mask length.

Command Mode: Router Mode or Interface Mode.

Default: Disabled.

Usage Guidelines: To configure an aggregate route in Router Mode, RIP must be enabled. In Interface Mode, the aggregate route can be configured before RIP is enabled on the interface, and it takes effect after RIP is enabled on the interface.

Example: Configure the aggregate route 192.168.20.0/22 globally.

```
Switch(config)#router rip
Switch(config-router) #ip rip agg 192.168.20.0/22
```

5.3.13 ip rip authentication key-chain

Command: `ip rip authentication key <name-of-chain>`
`no ip rip authentication key-chain`

Function: Enables RIPv2 authentication on an interface and specifies the key chain to use. The **no ip rip authentication key-chain** command cancels the authentication.

Parameters: <name-of-chain> is the name of the key chain. The string may contain spaces, ends with Enter, and can be up to 256 bytes long.

Default: Not configured.

Command Mode: Interface Mode.

Usage Guidelines: If authentication is enabled but no key chain or password is configured for the interface, authentication has no effect. If no authentication mode has been configured before this command, the mode is set to plaintext authentication. The **no ip rip authentication key** command cancels authentication only for packets sent and received; it does not set the interface to non-authentication mode.

Example:

```
Switch# config terminal
Switch(config)# interface vlan 1
Switch(Config-if-Vlan1)# ip rip authentication key my key
```

Related Commands: key, key chain

5.3.14 ip rip authentication mode

Command: `ip rip authentication mode {text|md5}`
`no ip rip authentication mode {ext|md5}`

Function: Configures the authentication mode. The **no ip rip authentication mode** command restores the default mode, text authentication.

Parameters: text: Text (simple) authentication. **md5**: MD5 authentication.

Default: No authentication is configured.

Command Mode: Interface Mode.

Usage Guidelines: RIPv1 does not support authentication. RIPv2 supports two authentication modes: text authentication (simple authentication) and MD5 authentication. Use this command together with **ip rip authentication key** or **ip rip authentication string**; configured on its own, it does not start authentication.

Example:

```
Switch# config terminal
Switch(config)# interface vlan 1
Switch(Config-if-Vlan1)# ip rip authentication mode md5
```

Related Commands: ip rip authentication key-chain, ip rip authentication string

5.3.15 ip rip authentication string

Command: `ip rip authentication string <text>`
`no ip rip authentication string`

Function: Sets the password used for RIP authentication. The **no ip rip authentication string** command cancels the authentication.

Parameters: <text> is the authentication password, 1 to 16 characters long; spaces are allowed. The password ends with Enter.

Command Mode: Interface Mode.

Usage Guidelines: When this command is configured, **ip rip authentication key** cannot be configured. MD5 authentication requires a key ID, which is 1 when this command is used. If no mode is configured, the mode is set to plaintext authentication. The **no ip rip authentication string** command cancels authentication only for packets sent and received; it does not set the interface to non-authentication mode. For example, entering **ip rip authentication string aaa aaa** sets the password to "aaa aaa" (7 characters).

Example:

```
Switch# config terminal
Switch(config)# interface vlan 1
Switch(Config-if-Vlan1)# ip rip authentication string guest
```

Related Commands: ip rip authentication mode

5.3.16 ip rip authentication cisco-compatible

Command: ip rip authentication cisco-compatible
no ip rip authentication cisco-compatible

Function: After this command is configured, the switch can receive RIP packets from Cisco devices that use plaintext or MD5 authentication.

Parameters: None.

Default: Not configured.

Command Mode: Interface Mode.

Usage Guidelines: When authentication is configured on a Cisco router and the number of route entries exceeds 25, its RIP packets exceed the standard length defined by the protocol. With this command configured, these oversized RIP packets are accepted instead of discarded.

Example:

```
Switch# config terminal
Switch(config)# interface vlan 1
Switch(Config-if-Vlan1)# ip rip authentication cisco-compatible
```

Related Commands: ip rip authentication mode

5.3.17 ip rip receive-packet

Command: ip rip receive-packet
no ip rip receive-packet

Function: Enables the interface to receive RIP packets. The **no ip rip receive-packet** command disables the interface from receiving RIP packets.

Default: The interface receives RIP packets.

Command Mode: Interface Mode.

Example:

```
Switch# config terminal
Switch(config)# interface vlan 1
Switch(Config-if-Vlan1)# ip rip receive-packet
```

Related Commands: ip rip send-packet

5.3.18 ip rip receive version

Command: ip rip receive version { 1 | 2|1 2 }
no ip rip receive version

Function: Sets the RIP version of packets that the interface receives. The default version is 2. The **no ip rip receive version** command restores the value set by the **version** command.

Parameters: 1 and **2** indicate RIP version 1 and RIP version 2; **1 2** indicates both RIP versions 1 and 2.

Default: Version 2.

Command Mode: Interface Mode.

Example:

```
Switch# config terminal
Switch(config)# interface vlan 1
Switch(Config-if-Vlan1)# ip rip receive version 1 2
```

Related Commands: version

5.3.19 ip rip send-packet

Command: ip rip send-packet
no ip rip send-packet

Function: Enables the interface to send RIP packets. The **no ip rip send-packet** command disables the interface from sending RIP packets.

Default: The interface sends RIP packets.

Command Mode: Interface Mode.

Example:

```
Switch# config terminal
Switch(config)# interface vlan 1
Switch(Config-if-Vlan1)# ip rip send-packet
```

Related Commands: ip rip receive-packet

5.3.20 ip rip send version

Command: ip rip send version { 1 | 2 | 1-compatible | 1 2}
no ip rip send version

Function: Sets the RIP version of packets that the interface sends. The default version is 2. The **no ip rip send version** command restores the value set by the **version** command.

Parameters: 1 and **2** indicate RIP version 1 and RIP version 2; **1 2** indicates both RIP versions 1 and 2. **1-compatible** indicates RIPv1-compatible mode.

Default: Version 2.

Command Mode: Interface Mode.

Example:

```
Switch# config terminal
Switch(config)# interface vlan 1
Switch(Config-if-Vlan1)# ip rip send version 1
```

Related Commands: version

5.3.21 ip rip split-horizon

Command: ip rip split-horizon [poisoned]
no ip rip split-horizon

Function: Enables split horizon. The **no ip rip split-horizon** command disables split horizon.

Parameters: poisoned enables split horizon with poison reverse.

Default: Split horizon with poison reverse.

Command Mode: Interface Mode.

Usage Guidelines: Split horizon prevents routing loops by stopping the Layer 3 switch from advertising a route out of the interface on which the route was learned.

Example:

```
Switch# config terminal
Switch(config)# interface vlan 1
Switch(Config-if-Vlan1)# ip rip split-horizon poisoned
```

5.3.22 key

Command: key <keyid>
no key <keyid>

Function: Adds and manages keys in the key chain. The **no key <keyid>** command deletes a key.

Parameters: <keyid> is the key ID, ranging from 0 to 2147483647.

Command Mode: Keychain Mode and Keychain-Key Mode.

Usage Guidelines: This command enters Keychain-key Mode, where you can set the password for the key.

Example:

```
Switch# config terminal
Switch(config)# key chain mychain
Switch(config-keychain)# key 1
Switch(config-keychain-key)#
```

Related Commands: key chain, key-string, accept-lifetime, send-lifetime

5.3.23 key chain

Command: key chain <name-of-chain>
no key chain < name-of-chain >

Function: Enters Keychain Mode and configures a key chain. The **no key chain <name-of-chain>** command deletes a key chain.

Parameters: <name-of-chain> is the name of the key chain. Its length has no specific limit.

Command Mode: Global Mode.

Example:

```
Switch# config terminal
Switch(config)# key chain mychain
Switch(config-keychain)#
```

Related Commands: key, key-string, accept-lifetime, send-lifetime

5.3.24 key-string

Command: key-string <text>
no key-string <text>

Function: Configures the password for a key. The **no key-string <text>** command deletes the password.

Parameters: <text> is a character string with no length limit. When it is used for RIP authentication, only the first 16 characters are used.

Command Mode: Keychain-Key Mode.

Usage Guidelines: Use this command to configure different passwords for keys with different IDs.

Example:

```
Switch# config terminal
Switch(config)# key chain mychain
```

```
Switch(config-keychain)# key 1
Switch(config-keychain-key)# key-string prime
```

Related Commands: key, key chain, accept-lifetime, send-lifetime

5.3.25 maximum-prefix

Command: `maximum-prefix <maximum-prefix> [<threshold>]`
`no maximum-prefix`

Function: Configures the maximum number of RIP routes in the routing table. The **no maximum-prefix** command removes the limit.

Parameters: <maximum-prefix> is the maximum number of RIP routes, ranging from 1 to 65535. **<threshold>** is the percentage of the maximum at which a warning is generated, ranging from 1 to 100; the default is 75.

Command Mode: Router Mode.

Usage Guidelines: The limit applies only to routes learned through RIP; it does not include direct routes or RIP static routes configured with the **route** command. The count compared against the limit is the number of routes marked R in **show ip route database**, which is also the number of RIP routes shown by **show ip route statistics**.

Example:

```
Switch# config terminal
Switch(config)# router rip
Switch(config-router)# maximum-prefix 150
```

5.3.26 neighbor

Command: `neighbor <A.B.C.D>`
`no neighbor <A.B.C.D>`

Function: Specifies a neighbor to which RIP updates are sent as unicast (targeted peer). The **no neighbor <A.B.C.D>** command removes the specified neighbor.

Parameters: <A.B.C.D> is the neighbor address in dotted decimal notation.

Default: No neighbor is configured.

Command Mode: Router Mode.

Usage Guidelines: When used with the **passive-interface** command, this command restricts routing updates to the specified neighbors only.

Example:

```
Switch# config terminal
Switch(config)# router rip
Switch(config-router)# neighbor 1.1.1.1
```

Related Commands: passive-interface

5.3.27 network

Command: `network <A.B.C.C/M|ifname>`
`no network <A.B.C.C/M|ifname>`

Function: Configures the networks on which RIP runs.

Parameters: <A.B.C.C/M> is the network IP address prefix and prefix length.

<ifname> is the interface name.

Default: RIP is not running.

Command Mode: Router Mode and Address Family Mode.

Usage Guidelines: Use this command to specify the networks on which RIP update packets are sent and received. Interfaces on networks that are not configured do not send or receive RIP packets.

Example:

```
Switch# config terminal
Switch(config)# router rip
Switch(config-router)# network 10.0.0.0/8
Switch(config-router)# network vlan 1
```

Related Commands: show ip rip, clear ip rip

5.3.28 offset-list

Command: offset-list <access-list-number |access-list-name> {in|out} <number > [<ifname>]
no offset-list <access-list-number |access-list-name> {in|out} <number > [<ifname>]

Function: Adds an offset to the metric of routes learned by RIP. The **no offset-list** command disables this function.

Parameters: <access-list-number | access-list-name> is the number or name of the access list to apply. **<number>** is the offset to add, ranging from 0 to 16. **<ifname>** is the interface name.

Default: No offset is added; the metric defined by the system is used.

Command Mode: Router Mode and Address Family Mode.

Example:

```
Switch# config terminal
Switch(config)# router rip
Switch(config-router)# offset-list 1 in 5 vlan 1
```

Related Commands: access-list

5.3.29 passive-interface

Command: passive-interface <ifname>
no passive-interface <ifname>

Function: Suppresses RIP broadcast updates on the specified interface; RIP packets on that interface are sent only to configured neighbors. The **no passive-interface** command cancels this setting.

Parameters: <ifname> is the interface name.

Default: Not configured.

Command Mode: Router Mode.

Example:

```
Switch# config terminal
Switch(config)# router rip
Switch(config-router)# passive-interface vlan 1
```

Related Commands: show ip rip

5.3.30 recv-buffer-size

Command: recv-buffer-size<size>
no recv-buffer-size

Function: Configures the size of the RIP UDP receive buffer. The **no recv-buffer-size** command restores the default.

Parameters: <size> is the buffer size in bytes, ranging from 8192 to 2147483647.

Default: 8192 bytes.

Command Mode: Router Mode.

Example:

```
Switch# config terminal
Switch(config)# router rip
Switch(config-router)# recv-buffer-size 23456789
```

5.3.31 redistribute

Command: redistribute {kernel |connected| static| ospf [<process-id>] | isis| bgp} [metric<value>] [route-map<word>]
no redistribute {kernel |connected| static| ospf [<process-id>] | isis| bgp} [metric<value>] [route-map<word>]

Function: Redistributes routes learned from other routing protocols into RIP.

Parameters: kernel: Redistributes kernel routes.

connected: Redistributes direct routes.

static: Redistributes static routes.

ospf: Redistributes OSPF routes. **<process-id>** is the OSPF process ID, ranging from 1 to 65535; if it is omitted, the default process is used.

isis: Redistributes IS-IS routes.

bgp: Redistributes BGP routes.

<value>: The metric assigned to redistributed routes, ranging from 0 to 16.

<word>: The route map applied to the redistributed routes.

Command Mode: Router Mode and Address Family Mode.

Usage Guidelines: In Address-family Mode, the **kernel** and **isis** parameters are unavailable.

Example:

```
Switch# config terminal
Switch(config)# router rip
Switch(config-router)# redistribute kernel route-map ipi
```

Redistribute OSPF process 2 routes into RIP.

```
Switch(config)# router rip
Switch(config-router)# redistribute ospf 2
```

5.3.32 route

Command: route <A.B.C.D/M>
no route <A.B.C.D/M>

Function: Configures a static RIP route. The **no route <A.B.C.D/M>** command deletes the route.

Parameters: <A.B.C.D/M> specifies the destination IP address prefix and prefix length.

Command Mode: Router Mode.

Usage Guidelines: This command adds a static RIP route and is mainly used for debugging. Routes configured with this command appear in the RIP route database but not in the kernel routing table.

Example:

```
Switch# config terminal
Switch(config)# router rip
Switch(config-router)# route 1.0.0.0/8
```

5.3.33 router rip

Command: router rip
no router rip

Function: Enables the RIP routing process and enters Router Mode. The **no router rip** command disables RIP.

Default: RIP is not running.

Command Mode: Global Mode.

Usage Guidelines: This command starts the RIP routing protocol. It must be configured before any other RIP command.

Example: Enable RIP and enter Router Mode.

```
Switch(config)#router rip
Switch(config-router)#
```

5.3.34 send-lifetime

Command: send-lifetime <start-time> {<end-time>| duration<seconds>| infinite}
no send-lifetime

Function: Specifies the period during which a key on the key chain is sent. The **no send-lifetime** command cancels this configuration.

Parameters: <start-time> specifies the start of the period in the following format:

<start-time>={<hh:mm:ss> <month> <day> <year>|<hh:mm:ss> <day> <month> <year>}

<hh:mm:ss>: The time of day, in hours, minutes, and seconds.

<day>: The day of the month, ranging from 1 to 31.

<month>: The month, given as the first three letters of its name, such as Jan.

<year>: The year, ranging from 1993 to 2035.

<end-time> specifies the end of the period in the following format:

<end-time>={<hh:mm:ss> <month> <day> <year>|<hh:mm:ss> <day> <month> <year>}

<hh:mm:ss>: The time of day, in hours, minutes, and seconds.

<day>: The day of the month, ranging from 1 to 31.

<month>: The month, given as the first three letters of its name, such as Jan.

<year>: The year, ranging from 1993 to 2035.

<seconds>: The validity period of the key in seconds, ranging from 1 to 2147483646.

Default: None.

Command Mode: Keychain-Key Mode.

Usage Guidelines: For details, see the RIP authentication section of the Configuration Guide.

Example: Configure the send lifetime of key 1 on the key chain named mychain.

```
Switch# config terminal
Switch(config)# key chain mychain
Switch(config-keychain)# key 1
Switch(config-keychain-key)# send-lifetime 03:03:01 Dec 3 2004 04:04:02 Oct 6
2006
```

Related Commands: key, key-string, key chain, accept-lifetime

5.3.35 show debugging rip

Command: `show debugging rip`

Function: Displays the status of RIP event, packet, and NSM debugging.

Command Mode: All Modes.

Example:

```
Switch# show debugging rip
RIP debugging status:
RIP event debugging is on
RIP packet detail debugging is on
RIP NSM debugging is on
```

5.3.36 show ip protocols rip

Command: `show ip protocols rip`

Function: Displays RIP process parameters and statistics.

Command Mode: All Modes.

Example:

```
show ip protocols rip
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 8 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing: static
  Default version control: send version 2, receive version 2
    Interface        Send  Recv   Key-chain
    Vlan1    2     2
  Routing for Networks:
    Vlan1
    Vlan2
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
    20.1.1.1              120  00:00:31              0           0
Distance: (default is 120)
```

Output	Description
Sending updates every 30 seconds with +/-50%, next due in 8 seconds	Updates are sent every 30 seconds.
Timeout after 180 seconds, garbage collect after 120 seconds	The route timeout period is 180 seconds, and the garbage collection time is 120 seconds.
Outgoing update filter list for all interface is not set	No outgoing update filter list is set for any interface.
Incoming update filter list for all interface is not set	No incoming update filter list is set for any interface.
Default redistribution metric is 1	The default redistribution metric is 1.
Redistributing: static	Static routes are redistributed into RIP.
Default version control: send version 2, receive version 2 Interface Send Recv Key-chain Ethernet1/0/3 2 2	Send and receive versions configured on the interface: both are version 2, and no key chain is configured.
Routing for Networks: Vlan1	RIP runs on VLAN 1 and VLAN 2.

Vlan2	
Routing Information Sources: Gateway Distance Last Update Bad Packets Bad Routes 20.1.1.1 120 00:00:31 0 0	Routing information sources Routing information sources: for gateway 20.1.1.1, the bad packet and bad route counts are both 0, 31 seconds have passed since the last update, and the administrative distance is 120.
Distance: (default is 120)	The default administrative distance is 120.

5.3.37 show ip rip

Command: show ip rip

Function: Displays the routes in the RIP route database.

Command Mode: All Modes.

Example:

```
show ip rip
Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS,
       B - BGP
   Network            Next Hop         Metric From            If     Time
R  12.1.1.0/24        20.1.1.1              2 20.1.1.1          Vlan1 02:51
R  20.1.1.0/24                               1                 Vlan1
```

In this output, R indicates a RIP route: the destination network is 12.1.1.0 with a prefix length of 24 and next hop 20.1.1.1. The route was learned on interface Vlan1 with a metric of 2 and times out in 2 minutes 51 seconds.

5.3.38 show ip rip database

Command: show ip rip database

Function: Displays the routes in the RIP route database.

Command Mode: All Modes.

Example:

```
Switch# show ip rip database
Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS,
       B -BGP
   Network            Next Hop         Metric From            If     Time
R  10.1.1.0/24                               1                 Vlan1
R  20.1.1.0/24                               1                 Vlan2
```

5.3.39 show ip rip database vrf

Command: show ip rip database vrf <vrf-name>

Function: Displays the RIP database information of the specified VRF.

Parameters: <vrf-name> specifies the name of the VPN routing and forwarding instance.

Command Mode: All Modes.

Example:

```
Switch# show ip rip database vrf IPI
Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS,
       B - BGP
   Network            Next Hop         Metric From            If     Time
R 10.1.1.0/24                               1                Vlan1    00:46
```

5.3.40 show ip rip interface

Command: `show ip rip interface [<ifname>]`

Function: Displays RIP information for interfaces.

Parameters: <ifname> is the interface name.

Command Mode: All Modes.

Example:

```
Switch# show ip rip interface vlan 1
Vlan1 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:10.1.1.1/24
```

5.3.41 show ip rip interface vrf

Command: `show ip rip interface vrf <vrf-name> [<ifname>]`

Function: Displays RIP interface information for the specified VRF.

Parameters: <vrf-name> specifies the name of the VPN routing and forwarding instance.

<ifname> is the interface name.

Command Mode: All Modes.

Example:

```
Switch# show ip rip interface vrf IPI Vlan1
Ethernet1/1 is up, line protocol is up
  Routing Protocol: RIP
    VPN Routing/Forwarding: vpnb
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      11.1.1.1/24
```

Output	Description
Vlan1 is up, line protocol is up	The interface is up.
Routing Protocol: RIP	RIP runs on the interface.
VPN Routing/Forwarding: vpnb	The VRF with which the interface is associated
Receive RIP packets	The interface can receive RIP packets.
Send RIP packets	The interface can send RIP packets.
Passive interface: Disabled	Passive interface is disabled.
Split horizon: Enabled with Poisoned Reversed	Split horizon with poison reverse is configured.
IP interface address: 11.1.1.1/24	IP address of the interface

5.3.42 show ip rip aggregate

Command: `show ip rip aggregate`

Function: Displays IPv4 RIP aggregate route information.

Parameters: None.

Command Mode: Admin Mode and Configuration Mode.

Default: None.

Usage Guidelines: Displays the interface on which each aggregate route is configured, and its Metric, Count, and Suppress values. For an aggregate route configured globally (in Router Mode), the interface is shown as "----". **Metric** is the metric, **Count** is the number of learned routes that are aggregated, and **Suppress** is the number of times the route has been aggregated.

Example: Display IPv4 RIP aggregate route information.

```
Switch(Config-if-Vlan1)#show ip rip agg
 Aggregate information of rip
       Network            Aggregated Ifname     Metric Count Suppress
       192.168.0.0/16       Vlan1                  1      2     0
       192.168.4.0/22         ----                   1      2     0
       192.168.4.0/24         ----                   1      1     1
                             Vlan1                  1      1     1
```

Output	Description
Network	Route prefix and prefix length
Aggregated Ifname	Name of the interface on which the aggregate route is configured. For a globally configured aggregate route, "----" is displayed.
Metric	Metric of the aggregate route
Count	Number of learned routes that are aggregated
Suppress	Number of times the route has been aggregated

5.3.43 show ip rip redistribute

Command: `show ip rip redistribute [vrf <NAME>]`

Function: Displays routing information that RIP has imported from external processes.

Parameters: vrf <NAME>: The VRF name. If no parameter is specified, the redistribution information of RIP for all VRFs is displayed.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: None.

Example:

```
Switch#show ip rip redistribute
```

5.3.44 show ip vrf

Command: `show ip vrf [<vrf-name>]`

Function: Displays the RIP instance information associated with VPN routing and forwarding instances.

Parameters: <vrf-name> specifies the name of the VPN routing and forwarding instance.

Command Mode: All Modes.

Usage Guidelines: This command also exists in other routing protocols; the output also includes information about other routing protocol processes associated with the VRF.

Example:

```
Switch# show ip vrf IPI
VRF IPI, FIB ID 1
Router ID: 11.1.1.1 (automatic)
Interfaces:
  Vlan1
!
VRF IPI; (id=1); RIP enabled Interfaces:
```

```
Ethernet1/8
Name             Interfaces
IPI                 Vlan1
Name                    Default RD           Interfaces
IPI                                            Vlan1
```

5.3.45 timers basic

Command: `timers basic <update> <invalid> <garbage>`
`no timers basic`

Function: Adjusts the RIP update, timeout, and garbage collection timers. The **no timers basic** command restores the default values.

Parameters: <update> is the interval at which update packets are sent, in seconds, ranging from 5 to 2147483647. **<invalid>** is the time after which a RIP route is declared invalid, in seconds, ranging from 5 to 2147483647. **<garbage>** is the time an invalid route remains in the routing table before it is deleted, in seconds, ranging from 5 to 2147483647.

Default: <update> is 30, **<invalid>** is 180, and **<garbage>** is 120.

Command Mode: Router Mode.

Usage Guidelines: By default, the system broadcasts RIP update packets every 30 seconds. A route is considered invalid after 180 seconds and remains in the routing table for another 120 seconds before it is deleted.

Example: Set the RIP update time to 20 seconds, the timeout to 80 seconds, and the garbage collection time to 60 seconds.

```
Switch(Config-Router)#timers basic 20 80 60
```

5.3.46 version

Command: `version {1| 2}`
`no version`

Function: Configures the RIP version of all packets sent and received by router interfaces. The **no version** command restores the default.

Parameters: 1: RIP version 1. **2**: RIP version 2.

Default: Packets are sent and received as version 2.

Command Mode: Router Mode and Address Family Mode.

Usage Guidelines: With **1**, each interface of the Layer 3 switch sends and receives only RIPv1 packets. With **2**, each interface sends and receives only RIPv2 packets. RIPv2 is the default.

Example: Set the version of all RIP packets sent and received by router interfaces to version 2.

```
Switch(config-router)#version 2
```

Related Commands: ip rip receive version, **ip rip send version**

5.4 OSPF

5.4.1 area authentication

Command: `area <id> authentication [message-digest md5]`
`no area <id> authentication`

Function: Configures the authentication mode of an OSPF area. The **no area <id> authentication** command restores the default.

Parameters: <id> is the area ID, given as a number from 0 to 4294967295 or in IP address format. **message-digest md5** specifies MD5 authentication; if it is omitted, simple plaintext authentication is used.

Default: No authentication.

Command Mode: OSPF Router Mode.

Usage Guidelines: Sets the authentication mode to plaintext or MD5 authentication. The authentication mode can also be configured in Interface Mode, which takes precedence over the area setting. If no authentication mode is configured on the interface and the area uses plaintext authentication, use **ip ospf authentication-key** to set the password; if the area uses MD5 authentication, use **ip ospf message-digest-key** to configure the MD5 key. The area authentication mode does not change the authentication mode configured on interfaces in the area.

Example: Set the authentication mode of area 0 to MD5.

```
Switch(config-router)#area 0 authentication message-digest
```

5.4.2 area default-cost

Command: area <id> default-cost <cost>
no area <id> default-cost

Function: Configures the cost of the default summary route sent into a stub or NSSA area. The **no area <id> default-cost** command restores the default.

Parameters: <id> is the area ID, given as a number from 0 to 16777214 or in IP address format. **<cost>** ranges from 0 to 16777214.

Default: 1.

Command Mode: OSPF Router Mode.

Usage Guidelines: This command applies only to ABRs connected to a stub or NSSA area.

Example: Set the default cost of area 1 to 10.

```
Switch(config-router)#area 1 default-cost 10
```

5.4.3 area filter-list

Command: area <id> filter-list {access|prefix} {in|out}
no area <id> filter-list {access|prefix} {in|out}

Function: Configures filtering of summary routes advertised by the ABR. The **no area <id> filter-list** command restores the default.

Parameters: <id> is the area ID, given as a number from 0 to 4294967295 or in IP address format. **access** specifies an access list and **prefix** specifies a prefix list. **<name>** is the filter name, 1 to 256 characters long. **in** filters routes advertised from other areas into this area; **out** filters routes advertised from this area to other areas.

Default: No filter is configured.

Command Mode: OSPF Router Mode.

Usage Guidelines: Use this command to restrict which routes are propagated between this area and other areas.

Example: Configure a filter on area 1.

```
Switch(config)#access-list 1 deny 172.22.0.0 0.0.0.255
Switch(config)#access-list 1 permit any
Switch(config)#router ospf 100
Switch(config-router)#area 1 filter-list access 1 in
```

5.4.4 area nssa

Command: area <id> nssa [TRANSLATOR| no-redistribution |DEFAULT-ORIGINATE | no-summary]
no area <id> nssa [TRANSLATOR| no-redistribution | DEFAULT-ORIGINATE | no-summary]

Function: Configures the area as a not-so-stubby area (NSSA).

Parameters: <id> is the area ID, given as a number from 0 to 4294967295 or in IP address format.

TRANSLATOR = translator-role {candidate|never|always} specifies the LSA translation role. **candidate**: If the router is elected as translator, it translates Type 7 LSAs into Type 5 LSAs. The default is **candidate**.

never: The router never translates Type 7 LSAs into Type 5 LSAs.

always: The router always translates Type 7 LSAs into Type 5 LSAs.

no-redistribution: Redistributed external routes are not imported into the NSSA.

DEFAULT-ORIGINATE = default-information-originate [metric <0-16777214>] [metric-type <1-2>]: Generates a Type 7 default LSA.

metric <0-16777214>: Specifies the metric.

metric-type <1-2>: Specifies the external metric type. The default is 2.

no-summary: Inter-area routes are not injected into the NSSA.

Default: No NSSA is defined.

Command Mode: OSPF Router Mode.

Usage Guidelines: An area cannot be both an NSSA and a stub area.

Example: Configure area 3 as an NSSA.

```
Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#area 0.0.0.51 nssa
Switch(config-router)#area 3 nssa default-information-originate metric 34
metric-type 2 translator-role candidate no-redistribution
```

5.4.5 area range

Command: area <id> range <address> [advertise| not-advertise| substitute]
no area <id> range <address>

Function: Summarizes OSPF routes at the area border. The **no area <id> range <address>** command cancels this function.

Parameters: <id> is the area ID, given as a number from 0 to 4294967295 or in IP address format.

<address> = <A.B.C.D/M>: Specifies the network prefix and prefix length of the range.

advertise: Advertises the range (default).

not-advertise: Does not advertise the range.

substitute <A.B.C.D/M>: Advertises the range as a different prefix.

<A.B.C.D/M>: The prefix advertised in place of the range.

Default: Not set.

Command Mode: OSPF Router Mode.

Usage Guidelines: Use this command to summarize routes within an area. If the network numbers in an area are contiguous, configure this command on the ABR to advertise one summary route that covers all individual networks in the specified range.

Example:

```
Switch#config terminal
```

```
Switch(config)# router ospf 100
Switch(config-router)# area 1 range 192.16.0.0/24
```

5.4.6 area stub

Command: area <id> stub [no-summary]
no area <id> stub [no-summary]

Function: Configures an area as a stub area. The **no area <id> stub [no-summary]** command cancels this setting.

Parameters: <id> is the area ID, given as a number from 0 to 4294967295 or in IP address format.

no-summary: The ABR stops sending summary LSAs into the stub area.

Default: Not defined.

Command Mode: OSPF Router Mode.

Usage Guidelines: Configure **area stub** on all routers in the stub area. Routers in a stub area use two commands: **area stub** and **area default-cost**. All routers connected to the stub area must be configured with **area stub**; on ABRs connected to the stub area, the cost of the default route is set with **area default-cost**.

Example:

```
Switch # config terminal
Switch (config)# router ospf 100
Switch (config-router)# area 1 stub
```

Related Commands: area default-cost

5.4.7 area virtual-link

Command: area <id> virtual-link A.B.C.D {AUTHENTICATION |AUTH_KEY | INTERVAL}
no area <id> virtual-link A.B.C.D [AUTHENTICATION | AUTH_KEY | INTERVAL]

Function: Configures a logical link between two parts of the backbone area that are physically separated by a non-backbone area. The **no area <id> virtual-link A.B.C.D** command removes the virtual link.

Parameters: <id> is the area ID, given as a number from 0 to 4294967295 or in IP address format.

AUTHENTICATION = authentication [message-digest [message-digest-key <1-255> md5 <LINE>] | null | AUTH_KEY].

authentication: Enables authentication on the virtual link.

message-digest: Uses MD5 authentication.

null: Uses null authentication, overriding the password or message digest.

AUTH_KEY = authentication-key <key>.
<key>: A password of fewer than 8 characters.

INTERVAL = [dead-interval | hello-interval | message-digest-key <1-255> md5 <LINE> | retransmit-interval | transmit-delay] <value>.

<value>: The delay or interval in seconds, ranging from 1 to 65535.

dead-interval: If no Hello packets are received from a neighbor within this interval, the neighbor is considered down. The default is 40 seconds.

hello-interval: The interval at which the router sends Hello packets. The default is 10 seconds.

message-digest-key: The MD5 authentication key.

retransmit-interval: The interval before the router retransmits a packet. The default is 5 seconds.

transmit-delay: The delay before the router sends a packet. The default is 1 second.

Default: None.

Command Mode: OSPF Router Mode.

Usage Guidelines: In OSPF, all non-backbone areas must connect to the backbone area. If the connection to the backbone area is lost, a virtual link can restore it. You can configure a virtual link between any two ABRs that share a common non-backbone area. The protocol treats routers connected by a virtual link as a point-to-point network.

Example:

```
Switch#config terminal
Switch(config) #router ospf 100
Switch(config-router) #area 1 virtual-link 10.10.11.50 hello 5 dead 20
```

Related Commands: area authentication, show ip ospf, show ip ospf virtual-links

5.4.8 auto-cost reference-bandwidth

Command: `auto-cost reference-bandwidth <bandwith>`
`no auto-cost reference-bandwidth`

Function: Sets the reference bandwidth that OSPF uses to calculate the default interface metric. The **no auto-cost reference-bandwidth** command assigns costs to interfaces according to interface type only.

Parameters: <bandwith> is the reference bandwidth in Mbps, ranging from 1 to 4294967.

Default: 100 Mbps.

Command Mode: OSPF Router Mode.

Usage Guidelines: The interface metric is calculated by dividing the reference bandwidth by the interface bandwidth. This command is mainly used to differentiate high-bandwidth links: when there are several high-bandwidth links, configure a larger reference bandwidth to distinguish their costs.

Example:

```
Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#auto-cost reference-bandwidth 50
```

Related Commands: **ip ospf cost**

5.4.9 compatible rfc1583

Command: `compatible rfc1583`
`no compatible rfc1583`

Function: Enables RFC 1583 compatibility. The **no compatible rfc1583** command disables it.

Default: RFC 2328 compatible.

Command Mode: OSPF Router Mode.

Example:

```
Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#compatible rfc1583
```

5.4.10 clear ip ospf process

Command: `clear ip ospf [<process-id>] process`

Function: Clears and restarts OSPF routing processes. If a process ID is specified, only that OSPF process is cleared; otherwise, all OSPF processes are cleared.

Default: None.

Command Mode: Admin Mode.

Example:

```
Switch#clear ip ospf process
```

5.4.11 debug ospf events

Command: debug ospf events [abr|asbr|lsa|nssa|os|router|vlink]
no debug ospf events [abr|asbr|lsa|nssa|os|router|vlink]

Function: Enables debugging of OSPF event messages. The **no debug ospf events** command disables this debugging.

Default: Disabled.

Command Mode: Admin Mode and Global Mode.

Example:

```
Switch#debug ospf events router
```

5.4.12 debug ospf ifsm

Command: debug ospf ifsm [status|events|timers]
no debug ospf ifsm [status|events|timers]

Function: Enables debugging of the OSPF interface state machine. The **no debug ospf ifsm** command disables this debugging.

Default: Disabled.

Command Mode: Admin Mode and Global Mode.

Example:

```
Switch#debug ospf ifsm events
```

5.4.13 debug ospf lsa

Command: debug ospf lsa [generate|flooding|install|maxage|refresh]
no debug ospf lsa [generate|flooding|install|maxage|refresh]

Function: Enables debugging of OSPF link-state advertisements. The **no debug ospf lsa** command disables this debugging.

Default: Disabled.

Command Mode: Admin Mode and Global Mode.

Example:

```
Switch#debug ospf lsa generate
```

5.4.14 debug ospf nfsm

Command: debug ospf nfsm [status|events|timers]
no debug ospf nfsm [status|events|timers]

Function: Enables debugging of the OSPF neighbor state machine. The **no debug ospf nfsm** command disables this debugging.

Default: Disabled.

Command Mode: Admin Mode and Global Mode.

Example:

```
Switch#debug ospf nfsm events
```

5.4.15 debug ospf nsm

Command: **debug ospf nsm [interface|redistribute]**
no debug ospf nsm [interface|redistribute]

Function: Enables debugging of OSPF NSM messages. The **no debug ospf nsm** command disables this debugging.

Default: Disabled.

Command Mode: Admin Mode and Global Mode.

Example:

```
Switch#debug ospf nsm interface
```

5.4.16 debug ospf packet

Command: **debug ospf packet [dd | detail | hello | ls-ack | ls-request | ls-update | recv | detail]**
no debug ospf packet [dd | detail | hello | ls-ack | ls-request | ls-update | recv | detail]

Function: Enables debugging of OSPF packets. The **no debug ospf packet** command disables this debugging.

Default: Disabled.

Command Mode: Admin Mode and Global Mode.

Example:

```
Switch#debug ospf packet hello
```

5.4.17 debug ospf route

Command: **debug ospf route [ase|ia|install|spf]**
no debug ospf route [ase|ia|install|spf]

Function: Enables debugging of OSPF routes. The **no debug ospf route** command disables this debugging.

Default: Disabled.

Command Mode: Admin Mode and Global Mode.

Example:

```
Switch#debug ospf route spf
```

5.4.18 debug ospf redistribute message send

Command: **debug ospf redistribute message send**
no debug ospf redistribute message send

Function: Enables debugging of the redistribution messages that an OSPF process sends to other OSPF processes. The **no** form of this command disables this debugging.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example: Enable debugging of the redistribution messages that an OSPF process sends to other OSPF processes.

```
Switch#debug ospf redistribute message send
```

5.4.19 debug ospf redistribute route receive

Command: `debug ospf redistribute route receive`
`no debug ospf redistribute route receive`

Function: Enables or disables debugging of routing messages that OSPF processes receive from the NSM.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example: Enable debugging of routing messages that OSPF processes receive from the NSM.

```
Switch# debug ospf redistribute route receive
```

5.4.20 default-information originate

Command: `default-information originate [always | METRIC | METRICTYPE | ROUTEMAP]`
`no default-information originate`

Function: Generates a default external route into the OSPF routing domain. The **no default-information originate** command disables this function.

Parameters: always: Always advertises the default route, whether or not a default route exists in the software.

METRIC = metric <value>: Sets the metric of the generated default route. **<value>** ranges from 0 to 16777214.

METRICTYPE = metric-type {1|2}: Sets the OSPF external type of the default route.

1: OSPF external type 1 metric.

2: OSPF external type 2 metric.

ROUTEMAP = route-map <WORD>.
<WORD> specifies the name of the route map to apply.

Default: The default metric is 10, and the default OSPF external type is 2.

Command Mode: OSPF Router Mode.

Usage Guidelines: When this command imports a default route into the OSPF routing domain, the system acts as an ASBR.

Example:

```
Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#default-information originate always metric 23 metric-
type 2 route-map myinfo
```

Related Commands: route-map

5.4.21 default-metric

Command: `default-metric <value>`
`no default-metric`

Function: Sets the default metric for OSPF. The **no default-metric** command restores the default.

Parameters: <value> is the metric, ranging from 0 to 16777214.

Default: Built-in; the metric is converted automatically.

Command Mode: OSPF Router Mode.

Usage Guidelines: Route redistribution continues even when metrics are incompatible: if a metric cannot be converted, the default metric is used instead. With this command, all redistributed routes use the same metric. Use this command together with **redistribute**.

Example:

```
Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#default-metric 100
```

5.4.22 distance

Command: distance {<value>|ROUTEPARAMETER}
no distance ospf

Function: Configures the OSPF administrative distance by route type. The **no distance ospf** command restores the default.

Parameters: <value> is the OSPF administrative distance, ranging from 1 to 255.

ROUTEPARAMETER = ospf {ROUTE1|ROUTE2|ROUTE3}.

ROUTE1 = external <external-distance>: Sets the distance for routes learned from other routing domains.

<external-distance>: The distance, ranging from 1 to 255.

ROUTE2 = inter-area <inter-distance>: Sets the distance for routes from one area to another.

<inter-distance>: The distance, ranging from 1 to 255.

ROUTE3 = intra-area <intra-distance>: Sets the distance for all routes within an area.

<intra-distance>: The distance, ranging from 1 to 255.

Default: 110.

Command Mode: OSPF Router Mode.

Usage Guidelines: The administrative distance indicates the reliability of the source of routing information. It ranges from 1 to 255; the higher the value, the lower the reliability.

Example:

```
Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#distance ospf inter-area 20 intra-area 10 external 40
```

5.4.23 distribute-list

Command: distribute-list <access-list-name> out {kernel |connected| static| rip| isis| bgp}
no distribute-list out {kernel |connected| static| rip| isis| bgp}

Function: Filters networks in outgoing routing updates. The **no distribute-list out** command disables this function.

Parameters: <access-list-name> is the name of the access list to apply.

out: Filters outgoing route updates.

kernel: Kernel routes.

connected: Direct routes.

static: Static routes.

rip: RIP routes.

isis: IS-IS routes.

bgp: BGP routes.

Command Mode: OSPF Router Mode.

Usage Guidelines: Use this command when routes from other routing protocols are redistributed into the OSPF routing table.

Example: Advertise BGP routes based on access list 1.

```
Switch#config terminal
Switch(config)#access-list l1 permit 172.10.0.0 0.0.255.255
Switch(config)#router ospf 100
Switch(config-router)#redistribute bgp
Switch(config-router)#distribute-list 1 out bgp
```

5.4.24 filter-policy

Command: `filter-policy <access-list-name>`
`no filter-policy`

Function: Uses an access list to filter the routes obtained by OSPF. The **no** form of this command cancels the route filtering.

Parameters: <access-list-name>: The access list to apply. Both numbered and named standard IP access lists can be used.

Default: None.

Command Mode: OSPF Router Mode.

Usage Guidelines: This command filters the routes obtained by OSPF. If the specified access list does not exist, no routes are filtered; otherwise, routes that do not match a permit rule of the access list are filtered. Only one access list can be set with this command; if it is configured more than once, only the last configuration takes effect.

Example: Use access list 1 to filter out routes that do not belong to the 172.10.0.0/16 segment.

```
Switch#config terminal
Switch(config)#access-list 1 permit 172.10.0.0 0.0.255.255
Switch(config)#router ospf
Switch(config-router)#filter-policy 1
```

5.4.25 host area

Command: `host <host-address> area <area-id> [cost <cost>]`
`no host <host-address> area <area-id> [cost <cost>]`

Function: Configures a stub host entry that belongs to the specified area. The **no host <host-address> area <area-id> [cost <cost>]** command cancels this configuration.

Parameters: <host-address> is the host IP address in dotted decimal notation.

<area-id>: The area ID, in dotted decimal notation or as an integer from 0 to 4294967295.

<cost>: The cost of the entry, an integer from 0 to 65535. The default is 0.

Default: No entry is configured.

Command Mode: OSPF Router Mode.

Usage Guidelines: Use this command to advertise a specific host route as a stub link. Because the stub host belongs to the specific router, the host setting has little effect on other routers.

Example:

```
Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#host 172.16.10.100 area 1
Switch(config-router)#host 172.16.10.101 area 2 cost 10
```

5.4.26 ip ospf authentication

Command: `ip ospf [<ip-address>] authentication [message-digest md5|sm3]`
`no ip ospf [<ip-address>] authentication`

Function: Specifies the authentication mode used for sending and receiving OSPF packets on the interface. The **no ip ospf [<ip-address>] authentication** command cancels the authentication.

Parameters: <ip-address> is the interface IP address in dotted decimal notation.

md5: Uses MD5 authentication.

sm3: Uses SM3 authentication.

Default: No authentication is required for OSPF packets received on the interface.

Command Mode: Interface Mode.

Example:

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf authentication message-digest
```

5.4.27 ip ospf authentication-key

Command: `ip ospf [<ip-address>] authentication-key <0 LINE | 7 WORD | LINE>`
`no ip ospf [<ip-address>] authentication`

Function: Specifies the authentication key used for sending and receiving OSPF packets on the interface. The **no** form of this command cancels the authentication key.

Parameters: <ip-address> is the interface IP address in dotted decimal notation. **<LINE>** specifies the authentication key. Key option 0 specifies a plaintext key, and key option 7 specifies an encrypted string. If no option is given, the key is plaintext.

Default: No authentication is required for OSPF packets received on the interface.

Command Mode: Interface Mode.

Example:

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf authentication-key 0 password
```

5.4.28 ip ospf cost

Command: `ip ospf [<ip-address>] cost <cost>`
`no ip ospf [<ip-address>] cost`

Function: Specifies the OSPF cost of the interface. The **no ip ospf [<ip-address>] cost** command restores the default.

Parameters: <ip-address> is the interface IP address in dotted decimal notation.

<cost> is the OSPF cost, ranging from 1 to 65535.

Default: The OSPF cost of the interface is calculated automatically from the bandwidth.

Command Mode: Interface Mode.

Example:

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf cost 3
```

5.4.29 ip ospf database-filter

Command: ip ospf [<ip-address>] database-filter all out
no ip ospf [<ip-address>] database-filter

Function: Enables LSA database filtering on the interface. The **no ip ospf [<ip-address>] database-filter** command disables the filtering.

Parameters: <ip-address> is the interface IP address in dotted decimal notation.

all: All LSAs.

out: Outgoing LSAs.

Default: Disabled.

Command Mode: Interface Mode.

Example:

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf database-filter all out
```

5.4.30 ip ospf dead-interval

Command: ip ospf [<ip-address>] dead-interval <time >
no ip ospf [<ip-address>] dead-interval

Function: Specifies the dead interval for neighboring Layer 3 switches. The **no ip ospf [<ip-address>] dead-interval** command restores the default.

Parameters: <ip-address> is the interface IP address in dotted decimal notation.

<time> is the dead interval for neighboring Layer 3 switches, in seconds, ranging from 1 to 65535.

Default: 40 seconds (normally four times the hello interval).

Command Mode: Interface Mode.

Usage Guidelines: If no Hello packet is received from a neighbor within the dead interval, the neighbor is considered unreachable. Use this command to adjust the dead interval according to the actual link conditions. The configured dead interval is carried in Hello packets. For OSPF to operate normally, the dead interval must be the same on adjacent Layer 3 switches and at least four times the hello interval.

Example:

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf dead-interval 80
```

5.4.31 ip ospf disable all

Command: ip ospf disable all
no ip ospf disable all

Function: Stops OSPF packet processing on the interface.

Command Mode: Interface Mode.

Usage Guidelines: This command overrides the **network area** command and stops OSPF packet processing on the interface.

Example:

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf disable all
```

5.4.32 ip ospf hello-interval

Command: ip ospf [<ip-address>] hello-interval <time>
no ip ospf [<ip-address>] hello-interval

Function: Specifies the hello interval of the interface. The **no ip ospf [<ip-address>] hello-interval** command restores the default.

Parameters: <ip-address> is the interface IP address in dotted decimal notation.

<time> is the interval at which Hello packets are sent, in seconds, ranging from 1 to 65535.

Default: 10 seconds.

Command Mode: Interface Mode.

Usage Guidelines: Hello packets are the most common OSPF packets; they are sent periodically to adjacent Layer 3 switches to discover and maintain adjacencies and to elect the DR and BDR. The configured hello interval is carried in Hello packets. The smaller the hello interval, the faster topology changes are detected, but the greater the overhead. For OSPF to operate normally, the hello interval must be the same on adjacent Layer 3 switches.

Example:

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf hello-interval 20
```

Related Commands: ip ospf dead-interval

5.4.33 ip ospf message-digest-key

Command: ip ospf [<ip-address>] message-digest-key <key_id> MD5 <0 LINE | 7 WORD | LINE>
no ip ospf [<ip-address>] message-digest-key <key_id>

Function: Specifies the key ID and key for MD5 authentication on the interface. The **no** form of this command restores the default.

Parameters: <ip-address> is the interface IP address in dotted decimal notation.

<key_id> ranges from 1 to 255.

<LINE> is the OSPF key. Key option 0 specifies a plaintext key, and key option 7 specifies an encrypted string. If no option is given, the key is plaintext.

Default: No MD5 key is configured.

Command Mode: Interface Mode.

Usage Guidelines: MD5 authentication secures communication between OSPF routers on the network. Neighbors must be configured with the same key ID and key; otherwise, no adjacency is established.

Example:

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf message-digest-key 2 MD5 0 yourpassword
```

5.4.34 ip ospf mtu

Command: ip ospf mtu <mtu>
no ip ospf mtu

Function: Specifies the MTU that OSPF uses for the interface when building packets. The **no ip ospf mtu** command restores the default.

Parameters: <mtu> is the interface MTU, ranging from 576 to 65535.

Default: The interface MTU obtained from the kernel is used.

Command Mode: Interface Mode.

Usage Guidelines: The MTU configured with this command is used only by OSPF; it is not applied to the kernel.

Example:

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf mtu 1480
```

5.4.35 ip ospf mtu-ignore

Command: ip ospf <ip-address> mtu-ignore
no ip ospf <ip-address> mtu-ignore

Function: Disables the MTU check during DD packet exchange. The **no ip ospf <ip-address> mtu-ignore** command re-enables the MTU check.

Parameters: <ip-address> is the interface IP address in dotted decimal notation.

Default: The MTU is checked during DD exchange.

Command Mode: Interface Mode.

Example:

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf mtu-ignore
```

5.4.36 ip ospf network

Command: ip ospf network {broadcast | non-broadcast | point-to-point | point-to-multipoint}
no ip ospf network

Function: Configures the OSPF network type of the interface. The **no ip ospf network** command restores the default.

Parameters: broadcast: Sets the OSPF network type to broadcast.

non-broadcast: Sets the OSPF network type to NBMA.

point-to-point: Sets the OSPF network type to point-to-point.

point-to-multipoint: Sets the OSPF network type to point-to-multipoint.

Default: Broadcast.

Command Mode: Interface Mode.

Example: Set the OSPF network type of interface VLAN 1 to point-to-point.

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf network point-to-point
```

5.4.37 ip ospf priority

Command: ip ospf [<ip-address>] priority <priority>
no ip ospf [<ip-address>] priority

Function: Configures the interface priority for designated router (DR) election. The **no ip ospf [<ip-address>] priority** command restores the default.

Parameters: <ip-address> is the interface IP address in dotted decimal notation.

<priority> is the priority, ranging from 0 to 255.

Default: 1.

Command Mode: Interface Mode.

Usage Guidelines: When two Layer 3 switches on the same segment both want to become the DR, the priority decides which one is elected. Normally the switch with the higher priority is elected; if the priorities are equal, the switch with the higher router ID is elected. A Layer 3 switch with priority 0 is never elected DR or BDR.

Example: Set the DR election priority of interface VLAN 1 to 0, so that it does not take part in the election.

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf priority 0
```

5.4.38 ip ospf retransmit-interval

Command: ip ospf [<ip-address>] retransmit-interval <time>
no ip ospf [<ip-address>] retransmit-interval

Function: Specifies the interval at which LSAs are retransmitted to adjacent Layer 3 switches. The **no ip ospf [<ip-address>] retransmit-interval** command restores the default.

Parameters: <ip-address> is the interface IP address in dotted decimal notation.

<time> is the LSA retransmit interval, in seconds, ranging from 1 to 65535.

Default: 5 seconds.

Command Mode: Interface Mode.

Usage Guidelines: When a Layer 3 switch sends an LSA to a neighbor, it keeps the LSA until it receives an acknowledgment. If no acknowledgment arrives within the interval, the LSA is retransmitted. The retransmit interval must be longer than the round-trip time between the two Layer 3 switches.

Example: Set the LSA retransmit interval of interface VLAN 1 to 10 seconds.

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf retransmit-interval 10
```

5.4.39 ip ospf transmit-delay

Command: ip ospf [<ip-address>] transmit-delay <time>
no ip ospf [<ip-address>] transmit-delay

Function: Sets the LSA transmit delay. The **no ip ospf [<ip-address>] transmit-delay** command restores the default.

Parameters: <ip-address> is the interface IP address in dotted decimal notation.

<time> is the LSA transmit delay, in seconds, ranging from 1 to 3600.

Default: 1 second.

Command Mode: Interface Mode.

Usage Guidelines: LSAs age while stored on a Layer 3 switch but not while in transit on the network. Adding the transmit delay to the LSA age before sending accounts for the time spent in transit.

Example: Set the LSA transmit delay of interface VLAN 1 to 3 seconds.

```
Switch#config terminal
Switch(config)#interface vlan 1
```

```
Switch(Config-if-Vlan1)#ip ospf transmit-delay 3
```

5.4.40 key

Command: key <keyid>
no key <keyid>

Function: Adds and manages keys in the key chain. The **no key <keyid>** command deletes a key.

Parameters: <keyid> is the key ID, ranging from 0 to 2147483647.

Command Mode: Keychain Mode and Keychain-Key Mode.

Usage Guidelines: This command enters Keychain-key Mode, where you can set the password for the key.

Example:

```
Switch#config terminal
Switch(config)#key chain mychain
Switch(config-keychain)#key 1
Switch(config-keychain-key)#
```

Related Commands: key chain, key-string, accept-lifetime, send-lifetime

5.4.41 key chain

Command: key chain <name-of-chain>
no key chain < name-of-chain >

Function: Enters Keychain Mode and configures a key chain. The **no key chain <name-of-chain>** command deletes a key chain.

Parameters: <name-of-chain> is the name of the key chain. Its length has no specific limit.

Command Mode: Global Mode and Keychain Mode.

Example:

```
Switch#config terminal
Switch(config)#key chain mychain
Switch(config-keychain)#
```

5.4.42 log-adjacency-changes detail

Command: log-adjacency-changes detail
no log-adjacency-changes detail

Function: Enables or disables logging of OSPF adjacency changes.

Parameters: None.

Default: OSPF adjacency changes are not logged.

Command Mode: OSPF Router Mode.

Usage Guidelines: When this command is configured, OSPF adjacency changes are recorded in the log.

Example:

```
Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#log-adjacency-changes detail
```

5.4.43 max-concurrent-dd

Command: `max-concurrent-dd <value>`
`no max-concurrent-dd`

Function: Sets the maximum number of concurrent DD exchanges in the OSPF process. The **no max-concurrent-dd** command restores the default.

Parameters: <value> is the maximum number of DD packets processed concurrently, ranging from 1 to 65535.

Default: Not set; the number of concurrent DD exchanges is not limited.

Command Mode: OSPF Router Mode.

Usage Guidelines: Specifies the maximum number of concurrent DD exchanges in the OSPF process.

Example: Set the maximum number of concurrent DD exchanges to 20.

```
Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#max-concurrent-dd 20
```

5.4.44 neighbor

Command: `neighbor A.B.C.D [<cost>| priority <value> | poll-interval <value>]`
`no neighbor A.B.C.D [<cost>| priority <value> | poll-interval <value>]`

Function: Configures an OSPF neighbor on an NBMA network. The **no neighbor A.B.C.D** command removes this configuration.

Parameters: <cost>: The OSPF neighbor cost, ranging from 1 to 65535.

priority <value>: The neighbor priority, ranging from 0 to 255. The default is 0.

poll-interval <value>: The polling interval before the neighbor relationship is established, ranging from 1 to 65535 seconds. The default is 120 seconds.

Default: None.

Command Mode: OSPF Router Mode.

Usage Guidelines: Use this command to configure neighbors manually on an NBMA network. Configure a neighbor entry for every known non-broadcast neighbor router. The configured neighbor address must be the primary address of the neighbor's interface. The poll interval should be much longer than the hello interval.

Example:

```
Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#neighbor 1.2.3.4 priority 1 poll-interval 90
Switch(config-router)#neighbor 1.2.3.4 cost 15
```

5.4.45 network area

Command: `network NETWORKADDRESS area <area-id>`
`no network NETWORKADDRESS area <area-id>`

Function: Enables OSPF on interfaces whose IP addresses match the specified network. The **no network NETWORKADDRESS area <area-id>** command removes the configuration and stops OSPF on the corresponding interfaces.

Parameters: NETWORKADDRESS = A.B.C.D/M | A.B.C.D X.Y.Z.W: The network address with a prefix length, or with a wildcard mask.

<area-id>: The area ID, in dotted decimal notation or as a decimal integer from 0 to 4294967295.

Default: None.

Command Mode: OSPF Router Mode.

Usage Guidelines: When a network segment is assigned to an area, the interfaces on that segment join the area and start exchanging Hello packets and database information with connected neighbors.

Example:

```
Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#network 10.1.1.0/24 area 1
```

5.4.46 ospf abr-type

Command: ospf abr-type {cisco|ibm|shortcut|standard}
no ospf abr-type

Function: Configures the OSPF ABR type. The **no ospf abr-type** command restores the default.

Parameters: cisco: Cisco ABR implementation.

ibm: IBM ABR implementation.

shortcut: Shortcut ABR.

standard: Standard (RFC 2328) ABR.

Default: cisco.

Command Mode: OSPF Router Mode.

Usage Guidelines: Specifies the ABR implementation type. This command improves interoperability between different OSPF implementations and is especially useful in multi-vendor environments.

Example: Set the ABR type to standard.

```
Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#ospf abr-type standard
```

5.4.47 ospf router-id

Command: ospf router-id <address>
no ospf router-id

Function: Specifies the router ID of the OSPF process. The **no ospf router-id** command removes the router ID.

Parameters: <address>: The router ID in IPv4 address format.

Default: None.

Command Mode: OSPF Router Mode.

Usage Guidelines: The new router ID takes effect immediately.

Example: Set the router ID of OSPF process 100 to 2.3.4.5.

```
Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#ospf router-id 2.3.4.5
```

5.4.48 overflow database

Command: `overflow database <maxdbsize > [{hard|soft}]`
`no overflow database`

Function: Configures the maximum number of LSAs. The **no overflow database** command removes the limit.

Default: Not configured.

Parameters: <maxdbsize>: The maximum number of LSAs, ranging from 0 to 4294967294.

soft: Soft limit; a warning is issued when the limit is exceeded.

hard: Hard limit; the OSPF instance is shut down when the limit is exceeded.

If neither **soft** nor **hard** is specified, a hard limit is applied.

Command Mode: OSPF Router Mode.

Example:

```
Switch#config terminal
Switch(config)#router ospf
Switch(config-router)#overflow database 10000 soft
```

5.4.49 overflow database external

Command: `overflow database external [<maxdbsize > <maxtime>]`
`no overflow database external [<maxdbsize > <maxtime>]`

Function: Configures the size of the external link-state database and the time to wait before the router exits the overflow state. The **no overflow database external** command restores the defaults.

Parameters: <maxdbsize>: The size of the external link-state database, ranging from 0 to 4294967294. The default is 4294967294.

<maxtime>: The time in seconds the router waits before exiting the overflow state, ranging from 0 to 65535.

Command Mode: OSPF Router Mode.

Example:

```
Switch#config terminal
Switch(config)#router ospf
Switch(config-router)#overflow database external 5 3
```

5.4.50 passive-interface

Command: `passive-interface <ifname> [<ip-address>]`
`no passive-interface <ifname>[<ip-address>]`

Function: Stops sending Hello packets on the specified interface. The **no passive-interface <ifname> [<ip-address>]** command cancels this function.

Parameters: <ifname> is the interface name.

<ip-address> is the interface IP address in dotted decimal notation.

Default: Not configured.

Command Mode: OSPF Router Mode.

Example:

```
Switch#config terminal
Switch(config)#router ospf
Switch(config-router)#passive-interface vlan1
```

5.4.51 redistribute

Command: redistribute {kernel |connected| static| rip| isis| bgp} [NAME] [metric<value>] [metric-type {1|2}][route-map<word>][tag<tag-value>]
no redistribute {kernel |connected| static| rip| isis| bgp} [metric<value>] [metric-type {1|2}][route-map<word>][tag<tag-value>]

Function: Redistributes routes learned from other routing protocols into OSPF.

Parameters: kernel: Redistributes kernel routes.

connected: Redistributes direct routes.

static: Redistributes static routes.

rip: Redistributes RIP routes.

isis: Redistributes IS-IS routes.

bgp: Redistributes BGP routes.

metric <value>: The metric of redistributed routes, ranging from 0 to 16777214.

metric-type {1|2}: The metric type of the redistributed external routes, 1 or 2. The default is 2.

route-map <word>: The route map applied to redistributed routes.

tag <tag-value>: The tag of the external routes, ranging from 0 to 4294967295. The default is 0.

NAME: The IS-IS area tag.

Command Mode: OSPF Router Mode.

Usage Guidelines: Redistributes routes from other routing protocols into the OSPF area to generate AS-external LSAs.

Example:

```
Switch#config terminal
Switch(config)#router ospf
Switch(config-router)#redistribute bgp metric 12
```

5.4.52 redistribute ospf

Command: redistribute ospf [<process-id>] [metric<value>] [metric-type {1|2}][route-map<word>]
no redistribute ospf [<process-id>] [metric<value>] [metric-type {1|2}][route-map<word>]

Function: Redistributes routes of the specified OSPF process into this process. The **no** form of this command deletes the redistribution; if the optional metric, metric-type, or route-map parameters are entered, only those settings are restored to their defaults.

Parameters: <process-id>: The OSPF process ID. The default is 0.

metric <value>: The metric of redistributed routes, ranging from 0 to 16777214.

metric-type {1|2}: The metric type of redistributed routes, 1 or 2. The default is 2.

route-map <word>: The route map applied to redistributed routes.

Default: No OSPF routes are redistributed.

Command Mode: OSPF Router Mode.

Usage Guidelines: If no process ID is entered, routes of the default OSPF process (process ID 0) are redistributed.

Example:

```
Switch(config-router)#redistribute ospf
```

5.4.53 router ospf

Command: `router ospf <process_id> <vrf-name>`
`no router ospf <process_id> <vrf-name>`

Function: Associates an OSPF process with a VPN. After the configuration succeeds, all configuration commands of this OSPF process apply to the VPN. The **no** form of this command deletes the OSPF instance associated with the VRF.

Parameters: <process_id> specifies the ID of the OSPF process to create, ranging from 1 to 65535.

<vrf-name> specifies the name of the VPN routing and forwarding instance.

Command Mode: Global Mode.

Usage Guidelines: Before using this command, create a VRF with the **ip vrf** command. This command then associates the VRF with the OSPF instance.

Example:

```
Switch#config terminal
Switch(config)#router ospf 100 VRF1
Switch(config-router)#network 10.1.1.0/24 area 0
```

5.4.54 show ip ospf

Command: `show ip ospf [<process-id>]`

Function: Displays general OSPF information.

Parameters: <process-id> is the process ID, ranging from 0 to 65535.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch#show ip ospf
Routing Process "ospf 0" with ID 192.168.1.1
 Process uptime is 2 days 0 hour 30 minutes
 Conforms to RFC2328, and RFC1583Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Refresh timer 10 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 0
 Number of LSA received 0
 Number of areas attached to this router: 1
 Area 0 (BACKBONE) (Inactive)
 Number of interfaces in this area is 0(0)
 Number of fully adjacent neighbors in this area is 0
 Area has message digest authentication
SPF algorithm executed 0 times
 Number of LSA 0. Checksum Sum 0x000000

 Routing Process "ospf 10" with ID 0.0.0.0
 Process bound to VRF test
 Process uptime is 4 days 23 hours 51 minutes
 Conforms to RFC2328, and RFC1583Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Refresh timer 10 secs
```

```
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 0
 Number of LSA received 0
 Number of areas attached to this router: 1
 Area 0 (BACKBONE) (Inactive)
Number of interfaces in this area is 0(0)
Number of fully adjacent neighbors in this area is 0
Area has no authentication
 SPF algorithm executed 0 times
Number of LSA 0. Checksum Sum 0x000000
```

5.4.55 show ip ospf border-routers

Command: show ip ospf [<process-id>] border-routers

Function: Displays the intra-domain route entries used to reach the ABRs and ASBRs of all instances.

Parameters: <process-id> is the process ID, ranging from 0 to 65535.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch#show ip ospf border-routers
OSPF process 0 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 10.15.0.1 [10] via 10.10.0.1, Vlan1, ASBR, Area 0.0.0.0
i 172.16.10.1 [10] via 10.10.11.50, Vlan2, ABR, ASBR, Area 0.0.0.0
```

5.4.56 show ip ospf database

Command: show ip ospf [<process-id>] database[{
adv-router [{<linkstate_id>| self-originate |adv-router <advertiser_router>}]
| asbr-summary[{<linkstate_id>| self-originate |adv-router <advertiser_router>}] | externel [{<linkstate_id>| self-originate |adv-router <advertiser_router>}]
| network [{<linkstate_id>| self-originate |adv-router <advertiser_router>}]
| nssa-external [{<linkstate_id>| self-originate |adv-router <advertiser_router>}] | opaque-area [{<linkstate_id>| self-originate |adv-router <advertiser_router>}]
| opaque-as [{<linkstate_id>| self-originate |adv-router <advertiser_router>}]
|opaque-link [{<linkstate_id>| self-originate |adv-router <advertiser_router>}]
| router [{<linkstate_id>| self-originate |adv-router <advertiser_router>}]
| summary [{<linkstate_id>| self-originate |adv-router <advertiser_router>}] |self-originate | max-age }]

Function: Displays OSPF link-state database information.

Parameters: <process-id> is the process ID, ranging from 0 to 65535.

<linkstate_id>: The link-state ID, in dotted decimal notation.

<advertiser_router>: The ID of the advertising router, in dotted decimal IP address format.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Use this command to view the OSPF link-state database.

Example:

```
Switch#show ip ospf database
                Router Link States (Area 0.0.0.2)
Link ID         ADV Router      Age Seq#       CkSum Link count
192.168.1.2     192.168.1.2      254 0x80000031 0xec21 1
192.168.1.3     192.168.1.3      236 0x80000033 0x0521 2
                Net Link States (Area 0.0.0.2)
Link ID         ADV Router      Age Seq#       CkSum
20.1.1.2        192.168.1.2      254 0x8000002b 0xece4
                Summary Link States (Area 0.0.0.2)
Link ID         ADV Router      Age Seq#        CkSum  Route
6.1.0.0         192.168.1.2       68 0x8000002b  0x5757  6.1.0.0/22
6.1.1.0         192.168.1.2      879 0x8000002a  0xf8bc   6.1.1.0/24
22.1.1.0        192.168.1.2      308 0x8000000c  0xc8f0   22.1.1.0/24
                ASBR-Summary Link States (Area 0.0.0.2)
Link ID         ADV Router      Age Seq#       CkSum
192.168.1.1     192.168.1.2     1702 0x8000002a 0x89c7
                AS External Link States
Link ID         ADV Router      Age Seq#       CkSum  Route
2.2.2.0         192.168.1.1     1499 0x80000056 0x3a63  E2 2.2.2.0/24 [0x0]
2.2.3.0         192.168.1.1     1103 0x8000002b 0x0ec3  E2 2.2.3.0/24 [0x0]
```

5.4.57 show ip ospf interface

Command: `show ip ospf interface <interface>`

Function: Displays OSPF interface information.

Parameters: <interface> is the interface name.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch#show ip ospf interface
Loopback is up, line protocol is up
  OSPF not enabled on this interface
Vlan1 is up, line protocol is up
  Internet Address 10.10.10.50/24, Area 0.0.0.0
    Process ID 0, Router ID 10.10.11.50, Network Type BROADCAST, Cost: 10
    Transmit Delay is 5 sec, State Waiting, Priority 1
    No designated router on this network
    No backup designated router on this network
    Timer intervals configured, Hello 35, Dead 35, Wait 35, Retransmit 5
      Hello due in 00:00:16
Neighbor Count is 0, Adjacent neighbor count is 0
```

5.4.58 show ip ospf neighbor

Command: `show ip ospf [<process-id>] neighbor [{<neighbor_id> |all | detail [all] |interface <ifaddress>}]`

Function: Displays OSPF neighbor information.

Parameters: <process-id> is the process ID, ranging from 0 to 65535.

<neighbor_id>: The neighbor ID in dotted decimal notation.

all: Displays information about all neighbors.

detail: Displays detailed information about all neighbors.

<ifaddress>: The interface IP address.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Use this command to check the state of OSPF neighbors.

Example:

```
Switch#show ip ospf neighbor
OSPF process 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.1.1       1   Full/Backup     00:00:32    6.1.1.1           Vlan1
192.168.1.3       1   Full/DR         00:00:36    20.1.1.3          Vlan2
192.168.1.3       1   Full/ -          00:00:30     20.1.1.3        VLINK2
```

Output	Description
Neighbor ID	Neighbor ID
Priority	Priority
State	Neighbor state
Dead time	Neighbor dead time
Address	Interface address
Interface	Interface name

5.4.59 show ip ospf redistribute

Command: `show ip ospf [<process-id>] redistribute`

Function: Displays the routing information that OSPF has redistributed from external processes.

Parameters: <process-id> is the process ID, ranging from 0 to 65535.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: None.

Example:

```
Switch#show ip ospf redistribute
ospf process 1 redistribute information:
ospf process 2
ospf process 3
bgp
ospf process 2 redistribute information:
ospf process 1
bgp
ospf process 3 redistribute information:
ospf process 1
bgp
Switch#show ip ospf 2 redistribute
ospf process 2 redistribute information:
ospf process 1
bgp
```

5.4.60 show ip ospf route

Command: `show ip ospf [<process-id>] route`

Function: Displays the OSPF routing table.

Parameters: <process-id> is the process ID, ranging from 0 to 65535.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch#show ip ospf route
O  10.1.1.0/24 [10] is directly connected, Vlan1, Area 0.0.0.0
O  10.1.1.4/32 [10] via 10.1.1.4, Vlan1, Area 0.0.0.0
IA 11.1.1.0/24 [20] via 10.1.1.1, Vlan1, Area 0.0.0.0
IA 11.1.1.2/32 [20] via 10.1.1.1, Vlan1, Area 0.0.0.0
IA 12.1.1.0/24 [20] via 10.1.1.2, Vlan1, Area 0.0.0.0
IA 12.1.1.2/32 [20] via 10.1.1.2, Vlan1, Area 0.0.0.0
O  13.1.1.0/24 [10] is directly connected, Vlan4, Area 0.0.0.3
O  14.1.1.0/24 [10] is directly connected, Vlan5, Area 0.0.0.4
IA 15.1.1.0/24 [20] via 13.1.1.2, Vlan4, Area 0.0.0.3
IA 15.1.1.2/32 [20] via 13.1.1.2, Vlan4, Area 0.0.0.3
E1 100.1.0.0/16 [21] via 10.1.1.1, Vlan1
E1 100.2.0.0/16 [21] via 10.1.1.1, Vlan1
```

5.4.61 show ip ospf virtual-links

Command: show ip ospf [<process-id>] virtual-links

Function: Displays OSPF virtual link information.

Parameters: <process-id> is the process ID, ranging from 0 to 65535.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch#show ip ospf virtual-links
Virtual Link VLINK0 to router 10.10.0.9 is up
  Transit area 0.0.0.1 via interface Vlan1
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
    Adjacency state Full
Virtual Link VLINK1 to router 10.10.0.123 is down
  Transit area 0.0.0.1 via interface Vlan1
  Transmit Delay is 1 sec, State Down,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in inactive
    Adjacency state Down
```

5.4.62 show ip route process-detail

Command: show ip route [database] process-detail

Function: Displays the IP routing table with the process ID or tag of each route.

Parameters: database displays all routes; without this parameter, only active routes are displayed.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: None.

Example:

```
Switch#show ip route database process-detail
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       > - selected route, * - FIB route, p - stale info
C      *> 127.0.0.0/8 is directly connected, Loopback
```

```
O         192.168.2.0/24 [110/10] is directly connected, Vlan2, 00:06:13,
process 12
C      *> 192.168.2.0/24 is directly connected, Vlan2
```

5.4.63 show ip protocols

Command: `show ip protocols`

Function: Displays information about the running routing protocols.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch#show ip protocols
```

This command displays information about the routing protocols running on the Layer 3 switch.

Sample output:

```
Routing Protocol is "ospf 0"
  Invalid after 0 seconds, hold down 0, flushed after 0
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Redistributing:
  Routing for Networks:
    10.1.1.0/24
    12.1.1.0/24
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 110)
    Address         Mask            Distance List

Routing Protocol is "bgp 0"
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  IGP synchronization is disabled
  Automatic route summarization is disabled
  Neighbor(s):
  Address          FiltIn FiltOut DistIn DistOut Weight RouteMap
Incoming Route Filter:
```

5.4.64 summary-address

Command: `summary-address <A.B.C.D/M> [{not-advertise|tag<tag-value>}]`

Function: Summarizes or suppresses external routes within the specified address range.

Parameters: <A.B.C.D/M>: The address range, as an IPv4 address in dotted decimal notation plus a mask length.

not-advertise: Suppresses the external routes in the range.

tag <tag-value>: The tag of the external routes, ranging from 0 to 4294967295. The default is 0.

Command Mode: OSPF Router Mode.

Usage Guidelines: When routes from other routing protocols are redistributed into OSPF, each route is advertised in a separate external LSA. This command advertises one summary route for all redistributed routes within the specified network address and mask, which can greatly reduce the size of the link-state database.

Example:

```
Switch#config terminal
Switch(config)#router ospf
Switch(config-router)#summary-address 172.16.0.0/16 tag 3
```

5.4.65 timers spf

Command: `timers spf <spf-delay> <spf-holdtime>`
`no timers spf`

Function: Adjusts the SPF calculation timers. The **no timers spf** command restores the defaults.

Parameters: <spf-delay>: The default is 5 seconds.

<spf-holdtime>: The default is 10 seconds.

Command Mode: OSPF Router Mode.

Usage Guidelines: This command sets the delay between receiving a topology change and starting the SPF calculation, and the hold time between two consecutive SPF calculations.

Example:

```
Switch#config terminal
Switch(config)#router ospf
Switch(config-router)#timers spf 5 10
```

5.5 BGP

5.5.1 address-family

Command: `address-family <AFI> <SAFI>`

Function: Enters Address-family Mode.

Parameters: <AFI>: The address family, such as IPv4 or IPv6.

<SAFI>: The subsequent address family, such as unicast, multicast, or VRF.

Default: None.

Command Mode: BGP Mode.

Usage Guidelines: Because BGP-4 supports multiple protocols, each address family can be configured separately. Configuration made outside Address-family Mode applies to the default address family (normally IPv4 unicast). To configure another address family, enter its Address-family Mode.

For MCE, VRFs must be enabled and associated with the corresponding address family. Configuration made with this command for a specific VRF is independent of the IPv4 unicast address family. Create the VRF with the **ip vrf <NAME>** command in Global Mode; the address family can be configured only after the VRF is created.

For MPLS VPN, VRFs must be enabled on the border (PE) routers. To implement a VPN, create BGP neighbors in the VRF address family on the private network and in the VPNv4 address family on the public network. When the VPNv4 address family is configured with this command, the IPv4 unicast address connection is used. The neighbor configuration can be the same as for IPv4 unicast; use **neighbor A.B.C.D activate** on the neighbor to enable this address family.

Example:

Example 1: Enter IPv4 unicast Address-family Mode.

```
Switch(config-router)# address-family ipv4 unicast
```

Example 2: Create a VRF named test and enter its BGP address family for configuration.

```
Switch(config)#ip vrf test
Switch(config-vrf)#exit
Switch(config)#router bgp 100
Switch(config-router)#address-family ipv4 vrf test
Switch(config-bgp-vrf)#
```

Related Commands: exit-address-family

5.5.2 aggregate-address

Command: `aggregate-address <ip-address/M> [summary-only] [as-set]`
`no aggregate-address <ip-address/M> [summary-only] [as-set]`

Function: Configures an aggregate address. The **no aggregate-address <ip-address/M> [summary-only] [as-set]** command deletes the aggregate address.

Parameters: <ip-address/M>: The IP address and mask length.

summary-only: Advertises only the summary route and suppresses the more specific routes.

as-set: Lists the ASs in the path as a set, with each AS appearing once.

Default: No aggregate address is configured.

Command Mode: Address Family Mode.

Usage Guidelines: Address aggregation reduces the amount of routing information advertised. With **summary-only**, the aggregate route is advertised to neighbors without the specific routes. With **as-set**, the ASs of each route covered by the aggregate are listed only once.

Example:

```
Switch(config-bgp-ipv4)# aggregate-address 100.1.0.0/16 summary-only
Switch(config-bgp-ipv4)# aggregate-address 100.2.0.0/16 summary-only as-set
Switch(config-bgp-ipv4)# aggregate-address 100.3.0.0/16 as-set
```

Related Commands: bgp aggregate-nexthop-check, no bgp aggregate-nexthop-check

5.5.3 bgp aggregate-nexthop-check

Command: `bgp aggregate-nexthop-check`
`no bgp aggregate-nexthop-check`

Function: Configures whether BGP checks the next hops of all routes during aggregation. The **no bgp aggregate-nexthop-check** command cancels this configuration, so that next-hop consistency is not checked for aggregate routes.

Parameters: None.

Default: Next hops are not checked during aggregation.

Command Mode: Global Mode.

Usage Guidelines: When checking is enabled, aggregation is not performed if the covered routes have different next hops. When checking is disabled, all covered routes are aggregated into the aggregate route.

Example:

```
Switch(config)#bgp aggregate-nexthop-check
```

Related Commands: aggregate-address, no aggregate-address

5.5.4 bgp always-compare-med

Command: `bgp always-compare-med`
`no bgp always-compare-med`

Function: Configures BGP to always compare MED values. The **no bgp always-compare-med** command cancels this configuration.

Parameters: None.

Default: Not configured.

Command Mode: BGP Mode.

Usage Guidelines: Normally BGP compares MED values only between routes from the same AS. With this configuration, MED values of routes from different ASs are also compared.

Example: AS 200 receives the same route prefix from AS 100 and AS 300 with different MED values. Configure MED values to always be compared.

```
Switch(config-router)#bgp always-compare-med
```

5.5.5 bgp asnotation asdot

Command: **bgp asnotation asdot**
no bgp asnotation asdot

Function: Displays AS numbers and matches regular expressions in ASDOT notation. The **no** form of this command cancels this notation.

Parameters: None.

Default: ASPLAIN notation.

Command Mode: BGP Route Mode.

Usage Guidelines: After changing the notation used to display AS numbers and match regular expressions, run **clear ip bgp *** to rebuild all BGP neighbor relationships.

Example: Display AS numbers and match regular expressions in ASDOT notation.

```
Switch(config)#router bgp 200
Switch(config-router)#bgp asnotation asdot
```

Related Commands: None.

5.5.6 bgp bestpath as-path ignore

Command: **bgp bestpath as-path ignore**
no bgp bestpath as-path ignore

Function: Ignores the AS_PATH length in best-path selection. The **no bgp bestpath as-path ignore** command cancels this configuration.

Parameters: None.

Default: Not set.

Command Mode: BGP Mode.

Usage Guidelines: BGP compares the AS_PATH length during best-path selection; use this configuration to ignore it.

Example:

Ignore the AS_PATH length:

```
Switch(config)#router bgp 200
Switch(config-router)#bgp bestpath as-path ignore
```

Related Commands: bgp bestpath compare-confed-aspath, bgp bestpath compare-routerid, bgp bestpath med, no bgp bestpath compare-confed-aspath, no bgp bestpath compare-routerid, no bgp bestpath med

5.5.7 bgp bestpath compare-confed-aspath

Command: **bgp bestpath compare-confed-aspath**
no bgp bestpath compare-confed-aspath

Function: Includes the confederation AS_PATH length in best-path selection. The **no bgp bestpath compare-confed-aspath** command cancels this configuration.

Parameters: None.

Default: Not configured.

Command Mode: BGP Mode.

Usage Guidelines: Normally only the external AS_PATH length is compared during best-path selection. With this configuration, the AS_PATH length within the confederation is also compared.

Example: Include the confederation AS_PATH length in best-path selection.

```
Switch(config-router)#bgp bestpath compare-confed-aspath
```

5.5.8 bgp bestpath compare-routerid

Command: bgp bestpath compare-routerid
no bgp bestpath compare-routerid

Function: Compares router IDs in best-path selection. The **no bgp bestpath compare-routerid** command cancels this configuration.

Parameters: None.

Default: Not configured.

Command Mode: BGP Mode.

Usage Guidelines: Normally, when other conditions are equal, the route that arrived first from the same AS is selected as the best route. With this command, the router IDs of the sources are also compared.

Example: A device (10.1.1.66, AS 200) receives the same route prefix from two devices (10.1.1.64 and 10.1.1.68) in AS 100. Configure the device to compare router IDs.

```
Switch(config-router)#bgp bestpath compare-routerid
```

Related Commands: bgp bestpath as-path ignore, bgp bestpath compare-confed-aspath, bgp bestpath med

5.5.9 bgp bestpath med

Command: bgp bestpath med {[confed] [missing-as-worst]}
no bgp bestpath med {[confed] [missing-as-worst]}

Function: Configures comparison of MED attributes within the confederation path and treats a missing MED as the largest value. The **no bgp bestpath med** command cancels this configuration.

Parameters: confed: Compares MED values within the confederation path.

missing-as-worst: Treats a missing MED as the maximum value.

Default: Not configured.

Command Mode: BGP Mode.

Usage Guidelines: Use this command to choose whether MED values are compared among confederations. A missing MED is treated as the maximum value when **missing-as-worst** is configured; otherwise it is treated as 0.

Example: Compare MED attributes within the confederation path and treat a missing MED as the largest value.

```
Switch(config-router)#bgp bestpath med confed missing-as-worst
```

Related Commands: bgp bestpath as-path ignore, bgp bestpath compare-confed-aspath, bgp bestpath compare-routerid

5.5.10 bgp client-to-client reflection

Command: bgp client-to-client reflection
no bgp client-to-client reflection

Function: Configures whether route reflection between clients is performed. The **no bgp client-to-client reflection** command cancels this configuration.

Parameters: None.

Default: Route reflection is performed once clients are configured.

Command Mode: BGP Mode.

Usage Guidelines: After route reflector clients are configured with **neighbor {<ip-address>|<TAG>} route-reflector-client**, the router performs route reflection by default. The **no** form of this command cancels route reflection between clients; reflection between clients and non-clients is not affected.

Example: Cancel route reflection between clients.

```
Switch(config-router)#no bgp client-to-client reflection
```

Related Commands: neighbor route-reflector-client

5.5.11 bgp cluster-id

Command: bgp cluster-id {<ip-address>|<01-4294967295>}
no bgp cluster-id {[<ip-address>]|<0-4294967295>}

Function: Configures the cluster ID used for route reflection. The **no bgp cluster-id** command cancels this configuration.

Parameters: <ip-address>|<1-4294967295>: The cluster ID, in dotted decimal notation or as a 32-bit number.

Default: Not configured.

Command Mode: BGP Mode.

Usage Guidelines: A cluster consists of one route reflector and its clients. To increase redundancy, more than one route reflector may be deployed in a cluster. The router ID uniquely identifies a router, and the cluster ID is required to identify a cluster that has two or more reflectors.

Example: Set the route reflection cluster ID to 1.1.1.1.

```
Switch(config-router)#bgp cluster-id 1.1.1.1
```

Related Commands: neighbor route-reflector-client

5.5.12 bgp confederation identifier

Command: bgp confederation identifier <as-id>
no bgp confederation identifier [<as-id>]

Function: Creates a confederation. The **no bgp confederation identifier [<as-id>]** command deletes the confederation.

Parameters: <as-id>: The confederation AS number, ranging from 1 to 4294967295. It can be entered in decimal notation (such as 6553700) or dotted notation (such as 100.100).

Default: No confederation is configured.

Command Mode: BGP Mode.

Usage Guidelines: A confederation divides a large AS into several smaller ASs while it is still identified externally as the large AS. Use this command to specify the AS number of the confederation.

Example:

```
Switch(config-router)# bgp confederation identifier 600
```

Related Commands: bgp confederation peers

5.5.13 bgp confederation peers

Command: bgp confederation peers <as-id> [<as-id>..]
no bgp confederation peers <as-id> [<as-id>..]

Function: Adds one or more ASs to, or deletes them from, a confederation.

Parameters: <as-id>: The numbers of the ASs in the confederation, ranging from 1 to 4294967295. They can be entered in decimal notation (such as 6553700) or dotted notation (such as 100.100). Multiple AS numbers can be specified.

Default: No members.

Command Mode: BGP Mode.

Usage Guidelines: A confederation divides a large AS into several smaller ASs while it is still identified externally as the large AS. Use this command to add or delete confederation members.

Example: Create confederation 600 and add members 100, 200, and 100.300.

```
Switch(config-router)# bgp confederation identifier 600
Switch(config-router)#bgp confederation peers 100 200 100.300
```

5.5.14 bgp dampening

Command: bgp dampening [<1-45>] [<1-20000> <1-20000> <1-255>] [<1-45>]
no bgp dampening

Function: Configures route dampening. The **no bgp dampening** command disables route dampening.

Parameters: <1-45>: The penalty half-lives, in minutes, of reachable and unreachable routes, that is, the time after which the penalty is reduced to half of its previous value.

<1-20000>: The reuse threshold and the suppress threshold.

<1-255>: The maximum suppress time, in minutes.

Default: The half-life is 15 minutes for both reachable and unreachable routes. The suppress threshold is 2000, the reuse threshold is 750, and the maximum suppress time is 60 minutes.

Command Mode: Address Family Mode.

Usage Guidelines: Route dampening reduces the large number of route updates caused by unstable routes. Each time a route flaps, a penalty is added to it; when the penalty exceeds the suppress threshold, the route is no longer advertised. If the route remains stable, the penalty decays according to the half-life, and the route is advertised again when the penalty falls below the reuse threshold or the suppress time exceeds the maximum suppress time. Use this command to enable or disable route dampening and configure its parameters.

Example: Enable route dampening with the default parameters.

```
Switch(config-bgp-ipv4)# bgp dampening
```

5.5.15 bgp default

Command: bgp default {ipv4-unicast|local-preference <0-4294967295>}
no bgp default {ipv4-unicast|local-preference [<0-4294967295>]}

Function: Sets BGP defaults. The **no bgp default** command cancels this configuration.

Parameters: ipv4-unicast: Uses IPv4 unicast by default to establish neighbor connections.

local-preference <0-4294967295>: Sets the default local preference.

Default: IPv4 unicast is enabled by default when BGP is enabled. The default local preference is 100.

Command Mode: BGP Mode.

Usage Guidelines: The IPv4 unicast address family is enabled by default in BGP. Use **no bgp default ipv4-unicast** to stop enabling this address family by default. Use **bgp default local-preference** to configure the default local preference.

Example: Set the default local preference to 500 on device 10.1.1.66.

```
Switch(config)#router bgp 200
Switch(config-router)# bgp default local-preference 500
```

5.5.16 bgp deterministic-med

Command: bgp deterministic-med
no bgp deterministic-med

Function: Compares the best MED among paths for the same prefix within an AS before comparing with paths from other ASs. The **no bgp deterministic-med** command cancels this configuration.

Parameters: None.

Default: Not configured.

Command Mode: BGP Mode.

Usage Guidelines: Normally, when routes for the same prefix are received over several paths, each path is compared. With this configuration, the system first selects, within each AS, the path with the lowest MED (when other main attributes are equal), and compares only that path with paths from other ASs. After the best path in each AS is selected, paths from different ASs are compared without regard to MED.

Example: Configure BGP to use the best MED within each AS for the same prefix when comparing with other ASs.

```
Switch(config-router)#bgp deterministic-med
```

5.5.17 bgp enforce-first-as

Command: bgp enforce-first-as
no bgp enforce-first-as

Function: When BGP receives external routes, requires the first AS in the AS_PATH to be the neighbor's AS number; otherwise, the peer connection is torn down. The **no bgp enforce-first-as** command cancels this configuration.

Parameters: None.

Default: Not configured.

Command Mode: BGP Mode.

Usage Guidelines: This command is usually used to reject insecure or unauthenticated routes.

Example:

```
Switch(config-router)#bgp enforce-first-as
```

5.5.18 bgp fast-external-failover

Command: bgp fast-external-failover
no bgp fast-external-failover

Function: Resets the BGP neighbor connection immediately when the connected interface changes, instead of waiting for the TCP timeout. The **no bgp fast-external-failover** command cancels this configuration.

Parameters: None.

Default: Enabled.

Command Mode: BGP Mode.

Usage Guidelines: This command immediately tears down the neighbor connection when the interface goes down.

Example:

```
Switch(config-router)# bgp fast-external-failover
```

5.5.19 bgp inbound-route-filter

Command: **bgp inbound-route-filter**
no bgp inbound-route-filter

Function: Prevents BGP from installing routes whose RD does not exist locally. The **no** form of this command installs the routes regardless of whether the RD exists locally.

Parameters: None.

Command Mode: BGP Route Mode.

Usage Guidelines: Normally, when the switch acts as a PE, whether a VPN route learned by BGP is stored in BGP depends on whether a VRF configured on the PE matches it. With the **no** form, BGP stores the route whether or not a match exists.

Example:

```
Switch(config)#router bgp 100
Switch(config-router)#no bgp inbound-route-filter
```

5.5.20 bgp inbound-max-route-num

Command: **bgp inbound-max-route-num <0-500000>**
no bgp inbound-max-route-num

Function: Sets the maximum number of routes that the BGP process learns from its neighbors.

Parameters: The maximum number of routes, ranging from 0 to 500000.

Default: 50000.

Command Mode: BGP Route Mode.

Usage Guidelines: Use this command to limit the number of routes that the BGP process learns from its neighbors.

Example: Limit the number of routes that the BGP process receives from its neighbors to 20000.

```
Switch(config-router)# bgp inbound-max-route-num 20000
```

5.5.21 bgp log-neighbor-changes

Command: **bgp log-neighbor-changes**
no bgp log-neighbor-changes

Function: Logs a message when a BGP neighbor changes state. The **no bgp log-neighbor-changes** command cancels this configuration.

Parameters: None.

Default: Enabled.

Command Mode: BGP Mode.

Usage Guidelines: Neighbor change messages can be displayed on the console.

Example:

```
Switch(config-router)# bgp log-neighbor-changes
```

5.5.22 bgp network import-check

Command: `bgp network import-check`
`no bgp network import-check`

Function: Sets whether BGP checks the IGP reachability of network routes. The **no bgp network import-check** command disables the IGP reachability check.

Parameters: None.

Default: Enabled.

Command Mode: BGP Mode.

Usage Guidelines: Checking the IGP reachability of a route advertised by BGP means checking that its next hop exists and is reachable through the IGP.

Example: Enable the IGP reachability check for BGP network routes.

```
Switch(config-router)# bgp network import-check
```

5.5.23 bgp rfc1771-path-select

Command: `bgp rfc1771-path-select`
`no bgp rfc1771-path-select`

Function: When this attribute is set, path selection follows RFC 1771; that is, the internal metric within the AS is not checked or compared.

Parameters: None.

Default: Enabled.

Command Mode: Global Mode.

Usage Guidelines: When this attribute is set, path selection follows RFC 1771 and does not check the internal metric within the AS. When paths from different ASs exist, the internal metric is compared only if this attribute is not set.

Example: Configure path selection to follow RFC 1771.

```
Switch(config)# bgp rfc1771-path-select
```

5.5.24 bgp rfc1771-strict

Command: `bgp rfc1771-strict`
`no bgp rfc1771-strict`

Function: Sets whether BGP strictly follows the RFC 1771 restrictions. The **no bgp rfc1771-strict** command disables strict compliance.

Parameters: None.

Default: RFC 1771 restrictions are not strictly followed.

Command Mode: Global Mode.

Usage Guidelines: With this attribute set, the origin of routes from protocols such as RIP, OSPF, and IS-IS is set to IGP; otherwise, it is set to INCOMPLETE.

Example: Configure BGP to strictly follow the RFC 1771 restrictions.

```
Switch(config)#bgp rfc1771-strict
```

5.5.25 bgp router-id

Command: `bgp router-id <A.B.C.D>`
`no bgp router-id [<A.B.C.D>]`

Function: Configures the router ID manually. The **no** form of this command cancels this configuration.

Parameters: <A.B.C.D>: The router ID.

Default: The router ID is obtained automatically.

Command Mode: BGP Mode.

Usage Guidelines: Use this command to set the router ID manually.

Example: Set the router ID to 1.1.1.1.

```
Switch(config-router)# bgp router-id 1.1.1.1
```

5.5.26 bgp scan-time

Command: bgp scan-time <0-60>
no bgp scan-time [<0-60>]

Function: Sets the interval for periodic next-hop validation. The **no bgp scan-time [<0-60>]** command restores the default.

Parameters: <0-60>: The validation interval, in seconds.

Default: 60 seconds.

Command Mode: BGP Mode.

Usage Guidelines: BGP periodically validates the next hops of BGP routes; this command sets the interval of this check. Set the value to 0 to disable the check.

Example: Set the next-hop validation interval to 30 seconds.

```
Switch(config-router)# bgp scan-time 30
```

5.5.27 clear ip bgp

Command: clear ip bgp * [vrf <vrf-name>] [in | out | soft [in | out]]

Function: Resets the BGP connections between the specified VRF and all peers.

Parameters: <vrf-name>: The VPN instance name, 1 to 64 characters long.

in: Triggers an inbound soft update.

out: Triggers an outbound soft update.

soft: Performs a soft reset.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: clear ip bgp * resets BGP. With **in**, a route refresh request is sent to the neighbor; with **out**, routes are re-sent to the neighbor. With **soft**, the BGP session is not reset.

Example:

```
Switch#clear ip bgp * vrf VRF-A
Switch#
```

5.5.28 clear ip bgp dampening

Command: clear ip bgp [<address-family>] dampening [<ip-address>|<ip-address/M>]

Function: Resets BGP route dampening.

Parameters: <address-family>: The address family, such as "ipv4 unicast".

<ip-address>: The IP address.

<ip-address/M>: The IP address and mask length.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: BGP route dampening information and state can be cleared by different parameters (such as address family or IPv4 address).

Example: Clear BGP route dampening information and state for the IPv4 unicast address family.

```
Switch#clear ip bgp ipv4 unicast dampening
```

Related Commands: bgp dampening

5.5.29 clear ip bgp flap-statistics

Command: clear ip bgp [<address-family>] flap-statistics [<ip-address>| <ip-address/M>]

Function: Resets BGP route dampening (flap) statistics.

Parameters: <address-family>: The address family, such as "ipv4 unicast".

<ip-address>: The IP address.

<ip-address/M>: The IP address and mask length.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: BGP route flap statistics and state can be cleared by different parameters (such as address family or IPv4 address).

Example: Clear the BGP flap statistics for the IPv4 unicast address family.

```
Switch#clear ip bgp ipv4 unicast flap-statistics
```

5.5.30 debug bgp

Command: debug bgp [<MODULE>|all]
no debug bgp [<MODULE>|all]

Function: Enables BGP debugging. The **no debug bgp [<MODULE>|all]** command disables BGP debugging.

Parameters: <MODULE>: The BGP module name, such as dampening, events, filters, fsm, keepalives, nsm, or updates.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Use this command to monitor BGP events, errors, and warnings.

Example: Display debugging messages for all BGP modules.

```
Switch#debug bgp all
```

5.5.31 debug bgp redistribute message send

Command: debug bgp redistribute message send
no debug bgp redistribute message send

Function: Enables debugging of the messages sent when routing information from external processes, such as OSPF and RIP, is redistributed into BGP. The **no** form of this command disables this debugging.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example:

```
Switch# debug bgp redistribute message send
Switch# no debug bgp redistribute message send
```

5.5.32 debug bgp redistribute route receive

Command: debug bgp redistribute route receive
no debug bgp redistribute route receive

Function: Enables debugging of messages that BGP receives from the NSM. The **no** form of this command disables this debugging.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example:

```
Switch#debug bgp redistribute route receive
Switch#no debug bgp redistribute route receive
```

5.5.33 distance

Command: distance <1-255> <ip-address/M> [<WORD>]
no distance <1-255> <ip-address/M> [<WORD>]

Function: Sets the administrative distance for a route prefix. The **no distance <1-255> <ip-address/M> [<WORD>]** command restores the default.

Parameters: <1-255>: The administrative distance.

<ip-address/M>: The route prefix.

<WORD>: The access list name.

Default: Not set.

Command Mode: BGP Mode.

Usage Guidelines: Sets the administrative distance used as the basis for path selection for the specified BGP routes.

Example: Set the administrative distance of route 10.1.1.64/32 to 90.

```
Switch(config-router)# distance 90 10.1.1.64/32
```

5.5.34 distance bgp

Command: distance bgp <1-255> <1-255> <1-255>
no distance bgp [<1-255> <1-255> <1-255>]

Function: Sets the BGP administrative distances. The **no distance bgp [<1-255> <1-255> <1-255>]** command restores the defaults.

Parameters: <1-255>: The EBGP, IBGP, and local administrative distances, in that order.

Default: 20 for EBGP and 200 for IBGP and local routes.

Command Mode: BGP Mode.

Usage Guidelines: Sets the administrative distances of BGP routes, which the NSM uses as the basis for path selection.

Example: Set the administrative distance of EBGP routes to 15 and that of IBGP and local routes to 150.

```
Switch(config-router)# distance bgp 15 150 150
```

5.5.35 exit-address-family

Command: `exit-address-family`

Function: Exits BGP Address-family Mode.

Parameters: None.

Default: None.

Command Mode: Address-family Mode.

Usage Guidelines: Use this command to exit Address-family Mode and end the address family configuration.

Example:

```
Switch(config)#router bgp 100
Switch(config-router)#address-family ipv4 unicast
Switch(config-bgp-ipv4)# exit-address-family
Switch(config-router)#
```

Related Commands: address-family

5.5.36 import map

Command: `import map <map-name>`
`no import map <map-name>`

Function: Configures the route map rules applied when routes are imported into the VRF.

Parameters: <map-name> is the name of the route map.

Default: None.

Command Mode: VRF Mode.

Usage Guidelines: Create the route map and its rules with **route-map NAME permit|deny <1-65535>**. This command applies the rules to routes imported into this VRF.

Example: Configure route map map1, and then configure VRF test to use it.

```
Switch(config)#route-map map1 permit 15
Switch(config-map)#match interface Vlan1
Switch(config-map)#set weight 655
```

Configure VRF test to use this route map:

```
Switch(config-map)#exit
Switch(config)#ip vrf test
Switch(config-af)#rd 100:10
Switch(config-af)#route-target both 100:10
Switch(config-af)#import map map1
Switch#show ip bgp vpn all
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:10 (Default for VRF test)
*> 11.1.1.0/24      11.1.1.64                0             0 200 ?
*>i15.1.1.0/24      10.1.1.68                0    100    655 300 ?
*> 20.1.1.0/24      11.1.1.64                0             0 200 ?
*>i100.1.1.0/24     10.1.1.68                0    100    655 300 ?
Route Distinguisher: 100:10
*>i15.1.1.0/24      10.1.1.68                0    100      0 300 ?
*>i100.1.1.0/24     10.1.1.68                0    100      0 300 ?
```

The output shows that the weight of the routes from the VPN changes to 655 after they are imported into VRF test.

5.5.37 ip as-path access-list

Command: ip as-path access-list <.LINE> {<permit>|<deny>} <LINE>
no ip as-path access-list <.LINE> {<permit>|<deny>} <LINE>

Function: Configures an AS_PATH access list. The **no ip as-path access-list** command deletes the access list.

Parameters: <.LINE>: The access list name.

<LINE>: The string to match in the AS_PATH.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: Use this command to configure an AS_PATH access list that provides permit or deny conditions.

Example: Configure access list ASPF to filter routes whose AS_PATH is 100.

```
Switch(config)#ip as-path access-list ASPF deny ^100$
```

5.5.38 ip community-list

Command: ip community-list {<LISTNAME> | <1-199> | [expanded <WORD>] | [standard <WORD>]} {deny | permit} <.COMMUNITY>
no ip community-list {<LISTNAME> | <1-199> | [expanded <WORD>] | [standard <WORD>]} [{deny | permit} <.COMMUNITY>]

Function: Configures a community list. The **no ip community-list** command deletes the community list.

Parameters: <LISTNAME>: The community list name.

<1-199>: The standard or expanded community list number.

<WORD>: The standard or expanded community list name.

<.COMMUNITY>: The members of the community list, which can be a combination of aa:nn, internet, local-AS, no-advertise, and no-export. Expanded lists accept regular expressions.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: Use this command to configure a community list that provides permit, deny, or search conditions.

Example: Configure community list LN to permit the community attribute 100:10.

```
Switch(config)# ip community-list LN permit 100:10
```

5.5.39 ip extcommunity-list

Command: ip extcommunity-list {<1-199>|[expanded <WORD>]|[standard <WORD>]} {deny|permit} <.COMMUNITY>
no ip extcommunity-list {<1-199>|[expanded <WORD>]|[standard <WORD>]} {deny|permit} <.COMMUNITY>

Function: Configures an extended community list. The **no ip extcommunity-list** command deletes the extended community list.

Parameters:

<1-199>: The standard or expanded extended community list number.

<WORD>: The standard or expanded extended community list name.

<.COMMUNITY>: The members of the extended community list. Expanded lists accept regular expressions.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: Use this command to configure an extended community list that provides permit, deny, or search conditions.

Example: Configure extended community list LN to permit the attribute 100:10.

```
Switch(config)# ip extcommunity-list expanded LN permit 100:10
```

5.5.40 neighbor activate

Command: neighbor {<ip-address>|<TAG>} activate
no neighbor {<ip-address>|<TAG>} activate

Function: Enables or disables the exchange of routes of the specified address family with a BGP neighbor. The **no neighbor {<ip-address>|<TAG>} activate** command disables the exchange of routes of that address family.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

Default: Route exchange is enabled for the IPv4 unicast address family and disabled for other address families.

Command Mode: Address Family Mode.

Usage Guidelines: IPv4 unicast is configured in BGP Route Mode; whether other address families are exchanged is configured in Address-family Mode. If this option is not enabled on either the local side or the peer, routes of that address family are not exchanged, and routes of the address family learned earlier are withdrawn when this option is disabled.

Example: Configure exchange of unicast routes with neighbor 2002::2.

```
Switch(config-bgp-ipv4)#neighbor 2002::2 activate
Switch(config-bgp-ipv4)#no neighbor 2002::2 activate
Switch(config-router-af)#
```

5.5.41 neighbor advertisement-interval

Command: neighbor {<ip-address>|<TAG>} advertisement-interval <0-600>
no neighbor {<ip-address>|<TAG>} advertisement-interval [<0-600>]

Function: Configures the route advertisement interval for the specified neighbor. The **no neighbor {<ip-address>|<TAG>} advertisement-interval [<0-600>]** command restores the default.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

<0-600>: The advertisement interval, in seconds.

Default: 5 seconds for IBGP and 30 seconds for EBGP.

Command Mode: BGP Mode.

Usage Guidelines: Reducing this value speeds up route updates but consumes more bandwidth.

Example: Set the route advertisement interval for neighbor 10.1.1.64 to 20 seconds.

```
Switch(config-router)#neighbor 10.1.1.64 advertisement-interval 20
```

5.5.42 neighbor allowas-in

Command: neighbor {<ip-address>|<TAG>} allowas-in [<1-10>]
no neighbor {<ip-address>|<TAG>} allowas-in

Function: Configures how many times the local AS number may appear in the AS_PATH of routes from the neighbor. The **no neighbor {<ip-address>|<TAG>} allowas-in** command restores the default, which allows no repetition.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

<1-10>: The number of times the AS number may appear.

Default: The AS number may not be repeated in a route. If this command is configured without the <1-10> parameter, the count is 3.

Command Mode: Address-family Mode.

Usage Guidelines: Normally BGP rejects a route whose AS_PATH already contains the local AS number. To support special requirements, especially VPNs, BGP can be configured to allow the AS number to appear a specified number of times. Use this command to configure that count.

Example: Allow the AS number to appear three times in routes from neighbor 10.1.1.66.

```
Switch(config-bgp-ipv4)#neighbor 10.1.1.66 allowas-in
```

5.5.43 neighbor as-override

Command: neighbor {<ip-address> | <TAG>} as-override
no neighbor {<ip-address> | <TAG>} as-override

Function: Overrides the AS number in the AS_PATH. Configure this command after the neighbor is created. The **no** form of this command deletes the configuration.

Parameters: <ip-address>: The neighbor address.

<TAG>: The peer group name.

Default: None.

Command Mode: VRF Address-family Mode.

Usage Guidelines: After this command is configured, the existing AS number in routes from the neighbor is overridden.

Example:

```
Switch (config)#router bgp 100
Switch (config-router)#address-family ipv4 vrf VRF-A
Switch(config-bgp-vrf)#neighbor 3.0.0.1 remote-as 65001
Switch(config-bgp-vrf)# neighbor 3.0.0.1 as-override
Switch(config-bgp-vrf)#
```

5.5.44 neighbor attribute-unchanged

Command: neighbor {<ip-address>|<TAG>} attribute-unchanged [as-path] [med] [next-hop]
no neighbor {<ip-address>|<TAG>} attribute-unchanged [as-path] [med] [next-hop]

Function: Configures route attributes that are passed to the neighbor unchanged (attribute transparent transmission). The **no neighbor {<ip-address>|<TAG>} attribute-unchanged** command cancels transparent transmission.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

Default: No attributes are transmitted transparently.

Command Mode: Address Family Mode.

Usage Guidelines: With this configuration, the specified route attributes do not change when routes are sent to the specified neighbor. In BGP Route Mode, the configuration applies to the IPv4 unicast address family. If no parameter is specified, all three attributes are kept unchanged.

Example: Keep the as-path, med, and next-hop attributes of routes unchanged for neighbor 10.1.1.64.

```
Switch(config-bgp-ipv4)#neighbor 10.1.1.64 attribute-unchanged
```

5.5.45 neighbor capability

Command: neighbor {<ip-address>|<TAG>} capability {dynamic | route-refresh}
no neighbor {<ip-address>|<TAG>} capability {dynamic | route-refresh}

Function: Configures negotiation of the dynamic update and route refresh capabilities with neighbors. The **no neighbor {<ip-address>|<TAG>} capability {dynamic | route-refresh}** command disables negotiation of the specified capability.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

Default: The route refresh capability is configured; the dynamic update capability is not.

Command Mode: BGP Mode.

Usage Guidelines: These are BGP extended capabilities. With this configuration, the capabilities supported by both sides are negotiated in OPEN messages. If the peer supports a capability, it responds accordingly; if not, it sends a NOTIFICATION message, and the originating side then sends an OPEN message without that capability to re-establish the connection. The dynamic capability allows address family changes without restarting the connection. Route refresh allows a router, after changing soft-reconfigurable attributes, to request the peer to resend its existing routes; with this capability, the connection does not need to be restarted and can be refreshed with **clear ip bgp * soft in**.

Example:

```
Switch(config-router)#neighbor 10.1.1.64 capability dynamic
Switch(config-router)# no neighbor 10.1.1.64 capability route-refresh
```

5.5.46 neighbor capability orf prefix-list

Command: neighbor {<ip-address>|<TAG>} capability orf prefix-list {<both>|<send>|<receive>}
no neighbor {<ip-address>|<TAG>} capability orf prefix-list {<both>|<send>|<receive>}

Function: Configures negotiation of the outbound route filtering (ORF) capability with neighbors. The **no neighbor {<ip-address>|<TAG>} capability orf prefix-list** command disables this negotiation.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

Default: The ORF capability is not configured.

Command Mode: Address Family Mode.

Usage Guidelines: This is a BGP extended capability. With this configuration, the capabilities supported by both sides are negotiated in OPEN messages. If the peer supports the capability, it responds accordingly; if not, it sends a NOTIFICATION message, and the originating side then sends an OPEN message without that capability to re-establish the connection. With this capability, the side configured with inbound prefix-list filter rules sends its rules to the peer, which applies them as its outbound rules; this avoids sending routes that the receiver will deny.

Example: Enable ORF capability negotiation with neighbor 10.1.1.66.

```
Switch(config-bgp-ipv4)#neighbor 10.1.1.66 capability orf prefix-list both
```

Related Commands: neighbor capability

5.5.47 neighbor collide-established

Command: neighbor {<ip-address>|<TAG>} collide-established
no neighbor {<ip-address>|<TAG>} collide-established

Function: Enables collision detection and resolution for TCP connections. The **no neighbor {<ip-address>|<TAG>} collide-established** command disables TCP connection collision resolution.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

Default: Disabled.

Command Mode: BGP Mode.

Usage Guidelines: This command resolves duplicate connections between peers caused by TCP connection collisions. With this option enabled, connections are checked even in the Established state. When a collision occurs, the switch checks whether the local IP address is higher than the peer's; if so, the existing connection is deleted. Without this option, collisions are checked only for locally originated connections in the OpenSent and OpenConfirm states.

Example: Enable TCP connection collision detection and resolution with neighbor 10.1.1.64.

```
Switch(config-router)#neighbor 10.1.1.64 collide-established
```

5.5.48 neighbor default-originate

Command: neighbor {<ip-address>|<TAG>} default-originate [route-map <WORD>]
no neighbor {<ip-address>|<TAG>} default-originate [route-map <WORD>]

Function: Configures whether the default route is sent to the specified neighbor. The **no neighbor {<ip-address>|<TAG>} default-originate [route-map <WORD>]** command stops sending the default route to the neighbor.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

<WORD>: The route map name.

Default: The default route is not sent.

Command Mode: Address Family Mode.

Usage Guidelines: With this option, the local default route is sent to the peer; without it, it is not. This lets you choose which router supplies the default route. If several neighbors of the peer supply a default route, the best one is selected according to the path selection rules. With a route map, you can control when the default route is sent.

Example: Send the local default route to neighbor 10.1.1.64.

```
Switch(config-router)#neighbor 10.1.1.64 default-originate
Switch(config-router)#
```

The default route from BGP then appears in the peer's routing table.

Related Commands: route-map

5.5.49 neighbor description

Command: neighbor {<ip-address>|<TAG>} description <.LINE>
no neighbor {<ip-address>|<TAG>} description

Function: Configures a description string for the peer or peer group. The **no neighbor {<ip-address>|<TAG>} description** command deletes the description.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

<.LINE>: The description, fewer than 80 printable characters.

Default: No description.

Command Mode: BGP Mode.

Usage Guidelines: Configures a description of the peer or peer group.

Example: Set the description of neighbor 10.1.1.64 to tester.

```
Switch(config-router)#neighbor 10.1.1.64 description tester
Switch(config-router)#
```

5.5.50 neighbor distribute-list

Command: neighbor {<ip-address>|<TAG>} distribute-list {<1-199>|<1300-2699>|<WORD>} {in|out}
no neighbor {<ip-address>|<TAG>} distribute-list {<1-199>|<1300-2699>|<WORD>} {in|out}

Function: Configures the policy applied to route updates exchanged with the neighbor. The **no neighbor {<ip-address>|<TAG>} distribute-list** command cancels the policy.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

<1-199>|<1300-2699>|<WORD>: The number or name of the access list.

Default: No policy is applied.

Command Mode: Address Family Mode.

Usage Guidelines: Configure the policy with the **access-list** command, and then apply it to routes sent or received with this command. In the **in** direction, route updates from the peer are filtered; in the **out** direction, routes sent from the local side to the peer are filtered.

Example: Filter routes destined for 100.1.0.0 received from neighbor 10.1.1.66.

```
Switch(config)#access-list 101 deny ip 100.1.0.0 0.0.1.255 any
Switch(config)#access-list 101 permit ip any any
Switch(config)#router bgp 100
Switch(config-router)#address-family ipv4 unicast
Switch(config-bgp-ipv4)# neighbor 10.1.1.66 distribute-list 101 in
```

Related Commands: ip access-list

5.5.51 neighbor dont-capability-negotiate

Command: neighbor {<ip-address>|<TAG>} dont-capability-negotiate
no neighbor {<ip-address>|<TAG>} dont-capability-negotiate

Function: Disables capability negotiation when establishing connections. The **no neighbor {<ip-address>|<TAG>} dont-capability-negotiate** command cancels this configuration.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

Default: Capability negotiation is performed.

Command Mode: BGP Mode.

Usage Guidelines: Capability negotiation is performed by default. Use this configuration to disable it when the peer runs an older BGP version that does not support capability negotiation.

Example: Disable capability negotiation on the connection with neighbor 10.1.1.64.

```
Switch(config-router)#neighbor 10.1.1.64 dont-capability-negotiate
```

5.5.52 neighbor ebgp-multihop

Command: neighbor {<ip-address>|<TAG>} ebgp-multihop [<1-255>]
no neighbor {<ip-address>|<TAG>} ebgp-multihop [<1-255>]

Function: Allows EBGP neighbors to be on different network segments and sets the maximum hop count (TTL). The **no neighbor {<ip-address>|<TAG>} ebgp-multihop [<1-255>]** command requires EBGP neighbors to be on the same segment.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

<1-255>: The maximum hop count.

Default: EBGP neighbors must be on the same segment.

Command Mode: BGP Mode.

Usage Guidelines: Without this command, EBGP peers must be on the same segment; with it, peer addresses can be on different segments. If no hop count is specified, it is 255.

Example:

Devices 10.1.1.64 (AS 100) and 11.1.1.120 (AS 300) are connected to interfaces 10.1.1.66 and 10.1.1.100 of a third device. Reachability between 10.1.1.64 and 11.1.1.120 is provided by static routes. The neighbor relationship is established only after both sides are configured as follows:

On 10.1.1.64:

```
Switch(config-router)#neighbor 11.1.1.120 ebgp-multihop
```

On 11.1.1.120:

```
Switch(config-router)#neighbor 10.1.1.64 ebgp-multihop
```

The switches on different segments can then establish a BGP neighbor relationship.

5.5.53 neighbor enforce-multihop

Command: neighbor {<ip-address>|<TAG>} enforce-multihop
no neighbor {<ip-address>|<TAG>} enforce-multihop

Function: Forces a multihop connection to the neighbor. The **no neighbor {<ip-address>|<TAG>} enforce-multihop** command cancels this configuration.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

Default: Not enforced.

Command Mode: BGP Mode.

Usage Guidelines: A directly connected neighbor is not actually multihop, but with this configuration it is treated as a multihop connection; that is, the checks normally performed only for IBGP and for EBGP over non-direct routes are performed for all connections. With multihop enforced, the directly connected next-hop check is not performed on outgoing routes.

Example: Force neighbor 10.1.1.66 to be treated as a multihop connection.

```
Switch(config-router)#neighbor 10.1.1.66 enforce-multihop
```

5.5.54 neighbor filter-list

Command: neighbor {<ip-address>|<TAG>} filter-list <.LINE> {<in>|<out>}
no neighbor {<ip-address>|<TAG>} filter-list <.LINE> {<in>|<out>}

Function: Applies AS_PATH access list control to the neighbor. The **no neighbor {<ip-address>|<TAG>} filter-list** command cancels the AS_PATH access list control.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

<.LINE>: The name of the AS_PATH access list configured with **ip as-path access-list <.LINE> <permit|deny> <LINE>**.

Default: Not configured.

Command Mode: Address Family Mode.

Usage Guidelines: First configure the IP AS_PATH access list, and then apply it to the specified neighbor to control sending and receiving of routes with the specified AS numbers. Whether routes are permitted or denied depends on the access list; the direction (in or out) is configured with this command.

Example:

Configure AS_PATH access list ASPF. Because of the filter, routes with AS number 100 are not sent to the peer.

```
Switch(config)#ip as-path access-list ASPF deny 100
Switch(config)#router bgp 100
Switch(config-router)# address-family ipv4 unicast
Switch(config-bgp-ipv4)# redistribute static
Switch(config-bgp-ipv4)# neighbor 10.1.1.66 filter-list aspf out
```

Related Commands: ip as-path access-list

5.5.55 neighbor interface

Command: neighbor <ip-address> interface <IFNAM>
no neighbor <ip-address> interface <IFNAM>

Function: Specifies the interface used to reach the neighbor. The **no neighbor <ip-address> interface <IFNAM>** command cancels this configuration.

Parameters: <ip-address>: The IP address of the neighbor.

<IFNAME>: The interface name, for example, Vlan2.

Default: Not configured.

Command Mode: BGP Mode.

Usage Guidelines: Use this command to specify the egress interface to the neighbor. Ensure that the destination is reachable through the interface.

Example: Set the interface to neighbor 10.1.1.64 to VLAN 2.

```
Switch(config-router)# neighbor 10.1.1.64 interface Vlan2
```

5.5.56 neighbor maximum-prefix

Command: neighbor {<ip-address>|<TAG>} maximum-prefix <1-4294967295> [<1-100> <warning-only>]
no neighbor {<ip-address>|<TAG>} maximum-prefix <1-4294967295> [<1-100> <warning-only>]

Function: Limits the number of route prefixes received from the neighbor. The **no neighbor {<ip-address>|<TAG>} maximum-prefix** command cancels this configuration.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

<1-4294967295>: The maximum number of prefixes allowed.

<1-100>: The percentage of the maximum at which a warning is generated.

<warning-only>: Only generates a warning when the limit is exceeded.

Default: No limit.

Command Mode: Address Family Mode.

Usage Guidelines: To guard against excessive route updates from neighbors (for example, attacks), the number of prefixes received from a neighbor is limited, and a warning is generated when the number reaches the configured percentage. If **warning-only** is set, only a warning is generated; otherwise, the connection to the neighbor is torn down until it is reset with the **clear ip bgp** command.

Example: Set the maximum number of prefixes from neighbor 10.1.1.64 to 12. A warning is generated when the number reaches 6, and the connection is torn down when it reaches 13.

```
Switch(config-bgp-ipv4)#neighbor 10.1.1.64 maximum-prefix 12 50
```

5.5.57 neighbor next-hop-self

Command: neighbor {<ip-address>|<TAG>} next-hop-self
no neighbor {<ip-address>|<TAG>} next-hop-self

Function: Sets the next hop of routes sent to the neighbor to the local router. The **no neighbor {<ip-address>|<TAG>} next-hop-self** command cancels this configuration.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

Default: Not configured.

Command Mode: Address Family Mode.

Usage Guidelines: In EBGP, the next hop automatically points to the advertising neighbor. In IBGP, the next hop of routes on the same segment is not changed, which causes errors on non-broadcast networks. Use this command to force the local router to be the next hop for IBGP neighbors.

Example:

```
Switch(config-bgp-ipv4)#neighbor 10.1.1.66 next-hop-self
```

5.5.58 neighbor override-capability

Command: neighbor {<ip-address>|<TAG>} override-capability
no neighbor {<ip-address>|<TAG>} override-capability

Function: Enables or disables overriding of capability negotiation. The **no neighbor {<ip-address>|<TAG>} override-capability** command restores capability negotiation.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

Default: Disabled.

Command Mode: BGP Mode.

Usage Guidelines: With this attribute, no error notification is sent when a capability requested by the neighbor is not supported.

Example:

```
Switch(config-router)#neighbor 10.1.1.64 override-capability
```

Related Commands: neighbor capability

5.5.59 neighbor passive

Command: neighbor {<ip-address>|<TAG>} passive
no neighbor {<ip-address>|<TAG>} passive

Function: Configures whether the local side actively initiates the connection to the specified neighbor. The **no neighbor {<ip-address>|<TAG>} passive** command restores active connection initiation.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

Default: The connection is initiated actively.

Command Mode: BGP Mode.

Usage Guidelines: With this attribute, the local side does not actively send a TCP connection request after the neighbor is configured; instead, it listens for a connection request from the peer.

Example:

```
Switch(config-router)#neighbor 10.1.1.64 passive
```

After this attribute is configured and the connection is re-established, the local side does not attempt to connect but stays in the Active state, waiting for a TCP connection request from the peer.

5.5.60 neighbor peer-group (Creating)

Command: neighbor < TAG> peer-group
no neighbor < TAG> peer-group

Function: Creates a peer group. The **no neighbor <TAG> peer-group** command deletes the peer group.

Parameters: <TAG>: The peer group name, up to 256 characters long.

Default: No peer group.

Command Mode: BGP Mode.

Usage Guidelines: A peer group lets you configure a set of peers with the same attributes at once, reducing configuration effort. Assign members to the peer group with the **neighbor <ip-address> peer-group <TAG>** command.

Example:

```
Switch(config-router)#neighbor pg peer-group
Switch(config-router)#neighbor 10.1.1.64 peer-group pg
Switch(config-router)#neighbor pg remote-as 100
```

Related Commands: neighbor peer-group (Configuring group members)

5.5.61 neighbor peer-group (Configuring group members)

Command: neighbor <ip-address> peer-group <TAG>
no neighbor <ip-address> peer-group <TAG>

Function: Assigns a peer to a peer group. The **no neighbor <ip-address> peer-group <TAG>** command removes the peer from the peer group.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

Default: No peer group.

Command Mode: BGP Mode.

Usage Guidelines: A peer group lets you configure a set of peers with the same attributes at once, reducing configuration effort. Create the peer group with the preceding command, and then assign members to it with this command.

Example: See the example for **neighbor peer-group (Creating)**.

Related Commands: neighbor peer-group (Creating)

5.5.62 neighbor port

Command: `neighbor <ip-address> port <0-65535>`
`no neighbor <ip-address> port [<0-65535>]`

Function: Specifies the TCP port number used to communicate with the peer. The **no neighbor <ip-address> port [<0-65535>]** command restores the default port number.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

<0-65535>: The TCP port number.

Default: 179.

Command Mode: BGP Mode.

Usage Guidelines: Use this configuration when the peer connects through a port other than the standard BGP port.

Example:

```
Switch(config-router)#neighbor 10.1.1.64 port 1023
```

5.5.63 neighbor prefix-list

Command: `neighbor {<ip-address>|<TAG>} prefix-list <LISTNAME|number> {<in|out>}`
`no neighbor {<ip-address>|<TAG>} prefix-list <LISTNAME|number> {<in>|<out>}`

Function: Configures prefix restrictions applied to routes sent to or received from the specified neighbor. The **no neighbor {<ip-address>|<TAG>} prefix-list** command cancels this configuration.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

<LISTNAME|number>: The name or number of the prefix list.

<in|out>: The direction in which the restrictions are applied.

Default: No prefix restrictions are applied.

Command Mode: Address Family Mode.

Usage Guidelines: Specify prefixes and their ranges with **ip prefix-list** and define whether each range is permitted or denied. Only routes with permitted prefixes are sent or received.

Example:

```
Switch(config)#ip prefix-list prw permit 100.1.0.0/22 ge 23 le 25
Switch(config)#router bgp 200
Switch(config-router)#address-family ipv4 unicast
Switch(config-bgp-ipv4)#redistribute static
Switch(config-bgp-ipv4)neighbor 10.1.1.66 prefix-list prw out
```

5.5.64 neighbor remote-as

Command: `neighbor {<ip-address>|<TAG>} remote-as <as-id>`
`no neighbor {<ip-address>|<TAG>} [remote-as <as-id>]`

Function: Configures a BGP neighbor. The **no** form of this command deletes the BGP neighbor.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

<as-id>: The neighbor AS number, ranging from 1 to 4294967295. It can be entered in decimal notation (such as 6553700) or dotted notation (such as 100.100).

Default: No neighbors are configured.

Command Mode: BGP Mode.

Usage Guidelines: BGP neighbors are created only by configuration, and a neighbor relationship is established only when both sides are configured. The peer's AS number must be specified; if it is incorrect, the neighbor relationship cannot be established. Within an AS, the peer AS number is the same as the local AS number.

Example: Configure two neighbors in AS 100 and AS 100.200.

```
Switch(config)#router bgp 200
Switch(config-router)# neighbor 10.1.1.64 remote-as 100
Switch(config-router)# neighbor 10.2.1.64 remote-as 100.200
```

5.5.65 neighbor remove-private-AS

Command: `neighbor {<ip-address>|<TAG>} remove-private-AS`
`no neighbor {<ip-address>|<TAG>} remove-private-AS`

Function: Configures whether private AS numbers are removed from routes sent to the neighbor. The **no neighbor {<ip-address>|<TAG>} remove-private-AS** command cancels this configuration.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

Default: Not configured.

Command Mode: Address Family Mode.

Usage Guidelines: Configure this attribute to avoid advertising private AS numbers to external ASs. Private AS numbers range from 64512 to 65535; they are not valid on the Internet and must not be advertised there. Only routes whose AS_PATH contains private AS numbers exclusively are processed; routes that contain both private and public AS numbers are not.

Example:

```
Switch(config-bgp-ipv4)#neighbor 10.1.1.64 remove-private-AS
```

5.5.66 neighbor route-map

Command: `neighbor {<ip-address>|<TAG>} route-map <NAME> {<in|out>}`
`no neighbor {<ip-address>|<TAG>} route-map <NAME> {<in|out>}`

Function: Configures the route map policy applied when routes are sent or received. The **no neighbor {<ip-address>|<TAG>} route-map <NAME> {<in|out>}** command cancels this configuration.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

<NAME>: The route map name.

<in|out>: The direction in which the route map is applied.

Default: Not set.

Command Mode: Address Family Mode.

Usage Guidelines: First create a route map in Global Mode with the **route-map** command and configure its match conditions and actions; then apply it with this command.

Example:

```
Switch(config)#route-map test permit 5
Switch(config-route-map)#match interface Vlan1
Switch(config-route-map)#set as-path prepend 65532
Switch(config-route-map)#exit
Switch(config)#router bgp 200
Switch(config-router)#address-family ipv4 unicast
Switch(config-bgp-ipv4)#neighbor 10.1.1.64 route-map test out
```

5.5.67 neighbor route-reflector-client

Command: neighbor {<ip-address>|<TAG>} route-reflector-client
no neighbor {<ip-address>|<TAG>} route-reflector-client

Function: Configures a route reflector client. The **no neighbor {<ip-address>|<TAG>} route-reflector-client** command cancels this configuration.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

Default: Not configured.

Command Mode: Address Family Mode.

Usage Guidelines: Route reflection reduces the number of peer sessions when there are many IBGP routers in an AS. Clients exchange routing information only with the route reflector, which handles the exchange between clients and other IBGP and EBGP routers. This command makes the local router a route reflector and the specified peer or peer group its client. Note: This configuration applies only within an AS.

Example:

```
Switch(config)#router bgp 100
Switch(config-router)#neighbor 10.1.1.66 remote-as 100
Switch(config-router)#neighbor 10.1.1.68 remote-as 100
Switch(config-router)#address-family ipv4 unicast
Switch(config-bgp-ipv4)#neighbor 10.1.1.66 route-reflector-client
Switch(config-bgp-ipv4)#neighbor 10.1.1.68 route-reflector-client
```

Related Commands: bgp client-to-client reflection, bgp cluster-id

5.5.68 neighbor route-server-client

Command: neighbor {<ip-address>|<TAG>} route-server-client
no neighbor {<ip-address>|<TAG>} route-server-client

Function: Configures a route server client. The **no neighbor {<ip-address>|<TAG>} route-server-client** command cancels this configuration.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

Default: Not configured.

Command Mode: Address Family Mode.

Usage Guidelines: A route server reduces the number of peer sessions when there are many routers between ASs in an EBGP environment. Clients exchange routing information through the route server, which passes the information transparently to the other clients.

Example:

Three routers: 10.1.1.64 (AS 100) and 10.1.1.68 (AS 300) each establish a neighbor relationship with the connected router 10.1.1.66 (AS 200). The configuration on 10.1.1.66 is as follows:

```
Switch(config)#router bgp 200
Switch(config-router)#neighbor 10.1.1.64 remote-as 100
Switch(config-router)# neighbor 10.1.1.68 remote-as 300
Switch(config-router)# address-family ipv4 unicast
Switch(config-bgp-ipv4)#neighbor 10.1.1.64 route-server-client
Switch(config-bgp-ipv4)# neighbor 10.1.1.68 route-server-client
```

5.5.69 neighbor send-community

Command: neighbor {<ip-address>|<TAG>} send-community [both|extended| standard]
no neighbor {<ip-address>|<TAG>} send-community [both|extended| standard]

Function: Configures whether community attributes are sent to the neighbor. The **no neighbor {<ip-address>|<TAG>} send-community** command stops sending them.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

both|extended|standard: Sends both standard and extended communities, extended communities only, or standard communities only.

Default: Community attributes are sent.

Command Mode: Address Family Mode.

Usage Guidelines: Configures whether community attributes are sent. On this switch, they are sent by default, whereas the standard protocol default is not to send them. With this attribute configured, community attributes are carried in routing information sent to the neighbor; otherwise, they are not. If no option is specified, **standard** is used.

Example:

```
Switch(config-bgp-ipv4)#no neighbor 10.1.1.66 send-community
Switch(config-bgp-ipv4)#neighbor 10.1.1.66 send-community
```

5.5.70 neighbor shutdown

Command: neighbor {<ip-address>|<TAG>} shutdown
no neighbor {<ip-address>|<TAG>} shutdown

Function: Shuts down the connection to the neighbor. The **no neighbor {<ip-address>|<TAG>} shutdown** command cancels this configuration.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

Default: The connection is not shut down.

Command Mode: BGP Mode.

Usage Guidelines: Disconnects from or reconnects to a peer or peer group without deleting the neighbor configuration.

Example:

```
Switch(config-router)#neighbor 10.1.1.64 shutdown
```

5.5.71 neighbor soft-reconfiguration inbound

Command: neighbor {<ip-address>|<TAG>} soft-reconfiguration inbound
no neighbor {<ip-address>|<TAG>} soft-reconfiguration inbound

Function: Configures whether inbound soft reconfiguration is performed. The **no neighbor {<ip-address>|<TAG>} soft-reconfiguration inbound** command disables inbound soft reconfiguration.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

Default: Inbound soft reconfiguration is not performed.

Command Mode: Address Family Mode.

Usage Guidelines: After soft reconfiguration is configured, the system stores inbound updates in a buffer and reapplies them when the session is reset, reducing route exchange with other routers. This command is needed only when the route refresh capability is not enabled.

Example:

```
Switch(config-bgp-ipv4)#neighbor 11.1.1.120 soft-reconfiguration inbound
```

5.5.72 neighbor soo

Command: neighbor <ip-addr> soo <soo-val>
no neighbor <ip-addr> soo <soo-val>

Function: Configures the site of origin (SoO) for routes from the neighbor. The **no** form of this command deletes the configuration.

Parameters: <ip-addr> is the neighbor IP address in dotted decimal notation.

<soo-val> is the site of origin in the format AA:NN. AA is the AS number, ranging from 1 to 4294967295, which can be entered in decimal notation (such as 6553700) or dotted notation (such as 100.100); NN is an arbitrary 2-byte number.

Default: None.

Command Mode: VRF Address-family Mode.

Usage Guidelines: If a customer AS connects to several ISP devices, set this attribute to prevent customer routes from returning to the customer through the provider network. Once set, the attribute is carried with the route, and routes carrying the SoO attribute are not advertised to a neighbor configured with the same attribute.

Example:

```
Switch (config)#router bgp 100
Switch(config-router)#address-family ipv4 vrf test
Switch(config-bgp-vrf)# neighbor 11.1.1.64 remote 200
Switch(config-bgp-vrf)# neighbor 11.1.1.64 soo 100.100:10
```

After this attribute is set, the switch no longer advertises routes with the 100.100:10 attribute to 11.1.1.64. Note that the SoO attribute is evaluated together with route target (RT) attributes: if an RT has the same value, the neighbor is regarded as the origin even if it is not. In practice, an SoO value should be configured separately, differ from the RT and RD values, and be unique within its scope, so that it correctly identifies the origin.

5.5.73 neighbor strict-capability-match

Command: neighbor {<ip-address>|<TAG>} strict-capability-match
no neighbor {<ip-address>|<TAG>} strict-capability-match

Function: Configures whether a strict capability match is required to establish the connection. The **no neighbor {<ip-address>|<TAG>} strict-capability-match** command removes this requirement.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

Default: Strict capability match is not configured.

Command Mode: BGP Mode.

Usage Guidelines: This command applies only to MP-BGP. With this command, the neighbor relationship is established only if the MP-BGP capabilities of both sides match. Whether other capabilities match does not affect neighbor establishment.

Example:

```
Switch(config-router)#neighbor 10.1.1.64 strict-capability-match
```

5.5.74 neighbor timers

Command: neighbor {<ip-address>|<TAG>} timers <0-65535> <0-65535>
no neighbor {<ip-address>|<TAG>} timers <0-65535> <0-65535>

Function: Configures the keepalive interval and hold time. The **no neighbor {<ip-address>|<TAG>} timers** command restores the defaults.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

<0-65535>: The keepalive interval and the hold time, in seconds, in that order.

Default: The keepalive interval is 60 seconds and the hold time is 240 seconds.

Command Mode: BGP Mode.

Usage Guidelines: Sets the keepalive interval and hold time used on the peer connection. The hold time is how long the connection is maintained when no message (such as a keepalive) is received from the peer; after the hold time expires, the connection is closed.

Example:

```
Switch(config-router)#neighbor 10.1.1.64 timers 50 200
```

Related Commands: neighbor timers connect, timers bgp

5.5.75 neighbor timers connect

Command: neighbor {<ip-address>|<TAG>} timers connect <0-65535>
no neighbor {<ip-address>|<TAG>} timers connect [<0-65535>]

Function: Configures the connection retry interval. The **no neighbor {<ip-address>|<TAG>} timers connect [<0-65535>]** command restores the default.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

<0-65535>: The retry interval, in seconds.

Default: 120 seconds.

Command Mode: BGP Mode.

Usage Guidelines: Configures the interval between attempts to connect to a peer.

Example:

```
Switch(config-router)#neighbor 10.1.1.64 timers connect 100
```

Related Commands: neighbor timers

5.5.76 neighbor unsuppress-map

Command: neighbor {<ip-address>|<TAG>} unsuppress-map <WORD>
no neighbor {<ip-address>|<TAG>} unsuppress-map <WORD>

Function: Configures or cancels the unsuppression of routes that match the specified route map. The **no neighbor {<ip-address>|<TAG>} unsuppress-map <WORD>** command cancels this configuration.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

<WORD>: The route map name.

Default: Not set.

Command Mode: Address Family Mode.

Usage Guidelines: This command is generally used for routes suppressed by aggregation with **summary-only**. Routes that match the route map are still advertised individually instead of being suppressed.

Example:

```
Switch(config-bgp-ipv4)#neighbor 10.1.1.66 unsuppress-map rmp
Switch(config)#access-list 10 permit 10.1.1.100 0.0.0.255
Switch(config)#route-map rmp permit 5
Switch(config-route-map)#match ip next-hop 10
```

Routes with next hop 10.1.1.100 are not suppressed.

5.5.77 neighbor update-source

Command: neighbor {<ip-address>|<TAG>} update-source <IFNAME>
no neighbor {<ip-address>|<TAG>} update-source <IFNAME>

Function: Configures the update source. The **no neighbor {<ip-address>|<TAG>} update-source <IFNAME>** command cancels this configuration.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

<IFNAME>: The name or IP address of the interface.

Default: Not configured; the nearest interface is used.

Command Mode: BGP Mode.

Usage Guidelines: The update source can be any available interface; normally a loopback interface is used. The **no** form restores the nearest interface as the update source. An improper update source can make the neighbor connection unavailable, and an interface that goes down causes problems, which is why loopback interfaces are used. Note: When a loopback interface is the update source, its address must be reachable for the connection to be established.

Example:

```
Switch(config-router)#neighbor 10.1.1.66 update-source 192.168.0.1
```

5.5.78 neighbor version 4

Command: neighbor {<ip-address>|<TAG>} version 4

Function: Configures the BGP version of the peer.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

4: The BGP version. Only version 4 is allowed.

Default: 4.

Command Mode: BGP Mode.

Usage Guidelines: Only version 4 is currently supported, so the version is always 4.

Example:

```
Switch(config-router)#neighbor 10.1.1.66 version 4
Switch(config-router)#
```

5.5.79 neighbor weight

Command: neighbor {<ip-address>|<TAG>} weight <0-65535>
no neighbor {<ip-address>|<TAG>} weight [<0-65535>]

Function: Configures the weight of routes received from the peer. The **no neighbor {<ip-address>|<TAG>} weight [<0-65535>]** command restores the default.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The peer group name.

<0-65535>: The weight.

Default: Routes learned from other routers have a weight of 0. Locally configured static routes have a weight of 32768.

Command Mode: BGP Mode.

Usage Guidelines: The weight affects path selection. The weight is local to the router and is not an attribute advertised to other routers.

Example:

```
Switch(config-router)#neighbor 10.1.1.66 weight 500
```

5.5.80 network (BGP)

Command: network <ip-address/M> [route-map <WORD>] [backdoor]
no network <ip-address/M> [route-map <WORD>] [backdoor]

Function: Configures a network to be advertised by BGP, optionally with a route map applied or as a backdoor route. The **no network <ip-address/M> [route-map <WORD>] [backdoor]** command cancels this configuration.

Parameters: <ip-address/M>: The network prefix.

<WORD>: The route map name.

Default: None.

Command Mode: Address Family Mode.

Usage Guidelines: Specifies the routes to be advertised by BGP. A network defined with this command is advertised to neighbors even if no matching local route exists. A route map can set the attributes applied to the network. With **backdoor**, the internal route is preferred even if the external (EBGP) route has a shorter distance.

Example:

```
Switch(config-bgp-ipv4)# network 172.16.0.0/16
```

5.5.81 redistribute (BGP)

Command: redistribute <ROUTES> [route-map <WORD>]
no redistribute <ROUTES> [route-map <WORD>]

Function: Redistributes routes from other sources into BGP. The **no redistribute <ROUTES> [route-map <WORD>]** command cancels this configuration.

Parameters: <ROUTES>: The route source or protocol, such as connected, isis, kernel, ospf, rip, or static.

<WORD>: The route map name.

Default: None.

Command Mode: Address Family Mode.

Usage Guidelines: Routes from other sources are redistributed into the BGP routing table and advertised to neighbors.

Example: Redistribute static routes into BGP and advertise them to neighbors.

```
Switch(config-bgp-ipv4)# redistribute static
```

5.5.82 redistribute ospf

Command: `redistribute ospf [<process-id>] [route-map<word>]`
`no redistribute ospf [<process-id>]`

Function: Redistributes routing information from OSPF into BGP. The **no** form of this command removes the configuration.

Parameters: <process-id> is the OSPF process ID, ranging from 1 to 65535. If no process ID is specified, the default process is used.

route-map <word> is the route map applied to redistributed routes.

Default: Not redistributed.

Command Mode: Address Family Mode.

Usage Guidelines: None.

Example: Redistribute routes of OSPFv2 process 2 into BGP (AS 1).

```
Switch(config)#router bgp 1
Switch(config-router)#address-family ipv4 unicast
Switch(config-bgp-ipv4)#redistribute ospf 2
```

5.5.83 router bgp

Command: `router bgp <as-id>`
`no router bgp <as-id>`

Function: Enables a BGP instance. The **no router bgp <as-id>** command deletes the BGP instance.

Parameters: <as-id>: The AS number, ranging from 1 to 4294967295. It can be entered in decimal notation (such as 6553700) or dotted notation (such as 100.100).

Default: BGP is not enabled.

Command Mode: Global Mode.

Usage Guidelines: Enables BGP for the specified AS and enters Router Mode (config-router), where the protocol can be configured.

Example: Enable BGP with AS number 4294967295 in decimal notation.

```
Switch(config)#router bgp 4294967295
Switch(config-router)#exit
```

Enable BGP with AS number 4294967295 in dotted notation.

```
Switch(config)#router bgp 65535.65535
Switch(config-router)#exit
```

5.5.84 show ip bgp

Command: show ip bgp [<ADDRESS-FAMILY>] [<ip-address>|<ip-address/M> [longer-prefixes]| cidr-only]

Function: Displays the BGP routing table.

Parameters: <ADDRESS-FAMILY>: The address family, such as "ipv4 unicast".

<ip-address>: The IP address.

<ip-address/M>: The IP address and mask length.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: BGP routing information can be displayed by different parameters (such as address family or IPv4 address), for routes covered by a prefix (**longer-prefixes**), or only for routes that do not match classful network boundaries (**cidr-only**; that is, routes whose masks are not class A, B, or C).

Example:

```
Switch#show ip bgp
BGP table version is 147, local router ID is 10.1.1.64
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 12.0.0.0         10.1.1.121               0         32768 ?
*> 100.1.1.0/24     10.1.1.200               0         32768 ?
*> 100.1.2.0/24     10.1.1.200               0         32768 ?
*> 172.0.0.0/8      0.0.0.0                            32768 i
Total number of prefixes 4
```

5.5.85 show ip bgp attribute-info

Command: show ip bgp attribute-info

Function: Displays BGP attribute information.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the attribute entries stored by BGP.

Example:

```
Switch#sh ip bgp attribute-info
attr[1] nexthop 0.0.0.0
attr[1] nexthop 10.1.1.64
attr[3] nexthop 10.1.1.64
attr[1] nexthop 10.1.1.121
attr[2] nexthop 10.1.1.200
```

5.5.86 show ip bgp community

Command: show ip bgp [<ADDRESS-FAMILY>] community <TYPE> [exact-match]

Function: Displays BGP routes with the specified community attributes.

Parameters: <ADDRESS-FAMILY>: The address family, such as "ipv4 unicast".

<TYPE>: The community, in AA:NN format, or a combination of local-AS, no-advertise, and no-export.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Several communities can be specified at once. With **exact-match**, only entries that match exactly are displayed.

Example:

```
Switch#show ip bgp community
BGP table version is 10, local router ID is 10.1.1.64
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*  100.1.1.0/24     0.0.0.0                              32768 700 800 i
*> 172.0.0.0/8      0.0.0.0                              32768 700 800 i
Total number of prefixes 2
```

5.5.87 show ip bgp community-info

Command: show ip bgp community-info

Function: Displays BGP community information.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the community entries stored by BGP; routes in the same community share one entry.

Example:

```
Switch#show ip bgp community-info
Address Refcnt Community
[0x3312558] (3) 100:50
```

5.5.88 show ip bgp community-list

Command: show ip bgp [<ADDRESS-FAMILY>] community-list <NAME> [exact-match]

Function: Displays BGP routes that match the specified community list.

Parameters: <ADDRESS-FAMILY>: The address family, such as "ipv4 unicast".

<NAME>: The community list name.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Configure the community list and its communities with the **ip community-list** command. When the list is specified by name, routes matching any community in the list are displayed.

Example:

```
Switch(config)#ip community-list commu per 100:50
Switch#sh ip bgp community-list commu
BGP table version is 25, local router ID is 10.1.1.64
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*  100.1.1.0/24     0.0.0.0                              32768 700 800 i
*> 172.0.0.0/8      0.0.0.0                              32768 700 800 i
```

Related Commands: ip community-list

5.5.89 show ip bgp dampening

Command: show ip bgp [<ADDRESS-FAMILY>] dampening {<dampened-paths>| <flap-statistics>|<parameters>}

Function: Displays BGP routes related to route dampening.

Parameters: <ADDRESS-FAMILY>: The address family, such as "ipv4 unicast". **dampened-paths**: Displays suppressed routes. **flap-statistics**: Displays route flap statistics. **parameters**: Displays the dampening parameters.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Only flapping routes are displayed. **parameters** displays the dampening configuration rather than specific routes. The other two options display the suppressed routes and the flap statistics (routes recently recovered from the unreachable state), respectively.

Example:

```
Switch#sh ip bgp dampening dampened-paths
BGP table version is 12, local router ID is 10.1.1.66
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            From                Reuse   Path
*d 100.1.3.0/24     10.1.1.64            00:27:40 100 ?

Total number of prefixes 1

Switch#sh ip bgp dampening flap-statistics
BGP table version is 13, local router ID is 10.1.1.66
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            From               Flaps  Duration  Reuse   Path
*d 100.1.3.0/24     10.1.1.64              3  00:06:05  00:27:00  100 ?
Switch#sh ip bgp dampening parameters
 dampening 15 750 2000 60 15 (route-map rmp)
  Reach ability Half-Life time    : 15 min
  Reuse penalty                  : 750
  Suppress penalty               : 2000
  Max suppress time              : 60 min
  Un-reach ability Half-Life time : 15 min
  Max penalty (ceil)             : 11999
  Min penalty (floor)            : 375
Total number of prefixes 1
```

Related Commands: bgp dampening

5.5.90 show ip bgp filter-list

Command: show ip bgp [<ADDRESS-FAMILY>] filter-list [<WORD >]

Function: Displays BGP routes that match the specified AS_PATH access list.

Parameters: <ADDRESS-FAMILY>: The address family, such as "ipv4 unicast".

<WORD>: The AS_PATH access list name.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Configure the AS_PATH access list with the **ip as-path access-list** command. This command displays the routes that pass the access list.

Example:

```
Switch#SH IP BGP filter-list FL
BGP table version is 2, local router ID is 11.1.1.100
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 100.1.1.0/24     10.1.1.64                0             0 100 ?
Total number of prefixes 1
```

Related Commands: neighbor filter-list, ip as-path access-list

5.5.91 show ip bgp inconsistent-as

Command: show ip bgp [<ADDRESS-FAMILY>] inconsistent-as

Function: Displays routes with inconsistent origin ASs.

Parameters: <ADDRESS-FAMILY>: The address family, such as "ipv4 unicast".

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: If the same prefix is received from different origin ASs, the origin AS is considered inconsistent. This command displays such routes.

Example:

```
Switch#sh ip bgp inconsistent-as
BGP table version is 2, local router ID is 11.1.1.100
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*  100.1.1.0/24     10.1.1.68                0             0 300 ?
*>                  10.1.1.64                0             0 100 ?
Total number of prefixes 1
```

5.5.92 show ip bgp neighbors

Command: show ip bgp [<ADDRESS-FAMILY>] neighbors [IP-ADDRESS] [advertised-routes|received {prefix-filter|routes}|routes]

Function: Displays information about BGP neighbors.

Parameters: <ADDRESS-FAMILY>: The address family, such as "ipv4 unicast".

<ip-address>: The IP address of the neighbor.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Without parameters, this command displays detailed information about all neighbors; with an IP address, it displays detailed information about that neighbor. The **advertised-routes**, **received prefix-filter**, **received routes**, and **routes** parameters display, respectively, the routes advertised by the local side, the received prefix filter, the received routes (soft reconfiguration must be enabled), and the routes from the specified neighbor.

Example:

```
Switch#sh ip bgp neighbor
BGP neighbor is 10.1.1.66, remote AS 200, local AS 100, external link
```

```
 BGP version 4, remote router ID 11.1.1.100
 BGP state = Established, up for 00:13:43
 Last read 00:13:43, hold time is 240, keep alive interval is 60 seconds
 Neighbor capabilities:
   Route refresh: advertised and received (old and new)
   Address family IPv4 Unicast: advertised and received
 Received 17 messages, 0 notifications, 0 in queue
 Sent 17 messages, 0 notifications, 0 in queue
 Route refresh request: received 0, sent 0
 Minimum time between advertisement runs is 30 seconds

For address family: IPv4 Unicast
 BGP table version 2, neighbor version 2
 Index 1, Offset 0, Mask 0x2
 Community attribute sent to this neighbor (both)
 0 accepted prefixes
 1 announced prefixes
Connections established 7; dropped 6
```

5.5.93 show ip bgp paths

Command: show ip bgp [<ADDRESS-FAMILY>] paths

Function: Displays BGP path information.

Parameters: <ADDRESS-FAMILY>: The address family, such as "ipv4 unicast".

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays BGP path information, including reference counts.

Example:

```
Switch#sh ip bgp paths
Address       Refcnt Path
[0x331dad0:0] (1)
[0x331d850:93] (1) 600
[0x331d8d8:249] (2) 200 300
```

5.5.94 show ip bgp prefix-list

Command: show ip bgp [<ADDRESS-FAMILY>] prefix-list [<NAME>]

Function: Displays BGP routes that match the specified prefix list.

Parameters: <ADDRESS-FAMILY>: The address family, such as "ipv4 unicast".

<NAME>: The prefix list name.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Use this command to select BGP routes by prefix list.

Example:

```
Switch(config)#ip prefix-list PL permit any
Switch(config)#
Switch#sh ip bgp prefix-list PL
BGP table version is 1, local router ID is 10.1.1.64
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*  100.1.1.0/24     10.1.1.66                              0 200 300 ?
```

```
*>                  10.1.1.100               0         32768 ?
Total number of prefixes 1
```

5.5.95 show ip bgp quote-regexp

Command: show ip bgp [<ADDRESS-FAMILY>] quote-regexp [<WORD>]

Function: Displays BGP routes whose AS_PATH matches the specified quoted regular expression.

Parameters: <ADDRESS-FAMILY>: The address family, such as "ipv4 unicast".

<WORD>: The regular expression.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Use a regular expression to select the required routes.

Example:

```
Switch#sh ip bgp quote-regexp ^300$
BGP table version is 2, local router ID is 11.1.1.100
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 100.1.1.0/24     10.1.1.68                0             0 300 ?
Total number of prefixes 1
Switch#sh ip bgp quote-regexp 100
BGP table version is 2, local router ID is 11.1.1.100
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*  100.1.1.0/24     10.1.1.64                0             0 500 100 600 ?
Total number of prefixes 1
```

5.5.96 show ip bgp regexp

Command: show ip bgp [<ADDRESS-FAMILY>] regexp [<LINE>]

Function: Displays BGP routes whose AS_PATH matches the specified regular expression.

Parameters: <ADDRESS-FAMILY>: The address family, such as "ipv4 unicast".

<LINE>: The regular expression.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Use a regular expression to select BGP routes of the required ASs.

Example:

```
Switch#sh ip bgp regexp 100
BGP table version is 2, local router ID is 11.1.1.100
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*  100.1.1.0/24     10.1.1.64                0             0 500 100 600 ?
Total number of prefixes 1
```

5.5.97 show ip bgp route-map

Command: show ip bgp [<ADDRESS-FAMILY>] route-map [<NAME>]

Function: Displays BGP routes that match the specified route map.

Parameters: <ADDRESS-FAMILY>: The address family, such as "ipv4 unicast".

<NAME>: The route map name.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Configure the route map with the **route-map** command. This command displays the routes that match the specified route map.

Example:

```
Switch#sh ip bgp route-map rmp
BGP table version is 2, local router ID is 11.1.1.100
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*  100.1.1.0/24     10.1.1.64                0             0 500 100 600 ?
*>                  10.1.1.68                0             0 300 ?
Total number of prefixes 1
```

5.5.98 show ip bgp scan

Command: show ip bgp scan

Function: Displays BGP scan information.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: BGP periodically scans next-hop information. This command displays the current scan interval and related routes.

Example:

```
Switch#show ip bgp scan
BGP Instance: (Default) AS 200, router-id 11.1.1.100
BGP scan interval is 60
Current BGP nexthop cache:
```

Related Commands: bgp scan-time

5.5.99 show ip bgp summary

Command: show ip bgp [<ADDRESS-FAMILY>] summary

Function: Displays BGP summary information.

Parameters: <ADDRESS-FAMILY>: The address family, such as "ipv4 unicast".

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays basic BGP summary information.

Example:

```
Switch#show ip bgp summary
BGP router identifier 10.1.1.66, local AS number 200
BGP table version is 1
```

```
1 BGP AS-PATH entries
0 BGP community entries
Neighbor    V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.1.1.68    4   300    0       0         0      0    0    never      Active
Total number of neighbors 1
```

Output	Description
identifier	Local router identifier
local AS number	Local AS number
table version	Version number of the BGP internal database
AS-PATH entries	Number of AS_PATH entries
community entries	Number of community entries
Neighbor	Neighbor address
V	BGP version run by the neighbor
AS	AS number to which the neighbor belongs
MsgRcvd	Number of messages received from the neighbor
MsgSent	Number of messages sent to the neighbor
TblVer	Routing table version
Up/Down	If the session with the neighbor is established, the duration of the session; otherwise, the current state.
State/PfxRcd	If the session is established, the number of prefixes received from the neighbor; otherwise, the current state of the neighbor.

5.5.100 show ip bgp view

Command: show ip bgp view [<NAME>] [<ip-address> | <ip-address/M> | [<ADDRESS-FAMILY>] summary]

Function: Displays information about the specified BGP instance.

Parameters: <NAME>: The BGP instance name.

<ip-address>: The IP address.

<ip-address/M>: The IP address and mask length.

<ADDRESS-FAMILY>: The address family, such as "ipv4 unicast".

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays information about the specified BGP instance.

Example:

```
Switch#show ip bgp view as300 100.1.1.0/24
```

Related Commands: router bgp

5.5.101 show ip bgp view neighbors

Command: show ip bgp view [<NAME>] neighbors [<ip-address>]

Function: Displays neighbor information for the specified BGP instance.

Parameters: <NAME>: The BGP instance name.

<ip-address>: The IP address of the neighbor.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays neighbor information for the specified BGP instance.

Example:

```
Switch#show ip bgp view as300 neighbors
```

5.5.102 show ip bgp vrf

Command: show ip bgp vrf [NAME] {summary | A.B.C.D | A.B.C.D/M}

Function: Displays the BGP routes and neighbors of a VRF.

Parameters: <NAME>: The VRF instance name.

summary: Displays summary information about BGP neighbors.

A.B.C.D: The IP address.

A.B.C.D/M: The IP address and mask length.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: BGP routing information can be displayed by different parameters (such as IPv4 address or IPv4 address and mask).

Example:

Example 1: Display BGP neighbor information.

```
S2#show ip bgp vrf 1 summary
BGP router identifier 30.1.1.2, local AS number 200
BGP table version is 8
1 BGP AS-PATH entries
0 BGP community entries
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
30.1.1.1        4   100      57      51        8    0    0 00:41:44       31
Total number of neighbors 1
```

For a description of the output fields, see **show ip bgp summary**.

Example 2: Display BGP route information.

```
S2#show ip bgp vrf 1
BGP routing table entry for 44.1.1.0/24
Paths: (1 available, best #1, table vrf 1 ipv4 unicast)
  Not advertised to any peer
  100
    30.1.1.1 from 30.1.1.1 (30.1.1.1)
      Origin incomplete, metric 6, localpref 100, valid, external, best
      Last update: 00:41:47
BGP routing table entry for 44.1.2.0/24
Paths: (1 available, best #1, table vrf 1 ipv4 unicast)
  Not advertised to any peer
  100
    30.1.1.1 from 30.1.1.1 (30.1.1.1)
      Origin incomplete, metric 6, localpref 100, valid, external, best
      Last update: 00:41:47
BGP routing table entry for 44.1.3.0/24
Paths: (1 available, best #1, table vrf 1 ipv4 unicast)
  Not advertised to any peer
  100
    30.1.1.1 from 30.1.1.1 (30.1.1.1)
      Origin incomplete, metric 6, localpref 100, valid, external, best
      Last update: 00:41:47
BGP routing table entry for 44.1.4.0/24
Paths: (1 available, best #1, table vrf 1 ipv4 unicast)
  Not advertised to any peer
  100
    30.1.1.1 from 30.1.1.1 (30.1.1.1)
```

```
      Origin incomplete, metric 6, localpref 100, valid, external, best
      Last update: 00:41:47
```

5.5.103 show ip bgp vpnv4

Command: show ip bgp vpnv4 {all | rd <rd-val> }

Function: Displays detailed information about all VPNv4 peers, or about BGP neighbor connections for the specified route distinguisher.

Parameters: all: All VPNv4 peers.

rd <rd-val>: The route distinguisher, usually in the form ASN:nn or IP-address:nn, such as 100:10.

Default: None.

Command Mode: All Modes.

Usage Guidelines: Information can be displayed for a specified RD.

Example:

```
switch(config)#show ip bgp vpnv4 all neighbors
BGP neighbor is 11.1.1.2, remote AS 200, local AS 100, external link
  BGP version 4, remote router ID 0.0.0.0
  Neighbor under common administration
  BGP state = Active
  Last read         , hold time is 240, keepalive interval is 60 seconds
  Received 0 messages, 0 notifications, 0 in queue
  Sent 0 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 0
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes
 Connections established 0; dropped 0
Next connect timer due in 83 seconds
```

5.5.104 timers bgp

Command: timers bgp <0-65535> <0-65535>
no timers bgp [<0-65535> <0-65535>]

Function: Configures the timers for all BGP neighbors. The **no timers bgp [<0-65535> <0-65535>]** command restores the defaults.

Parameters: <0-65535>: The keepalive interval and the hold time, in seconds, in that order.

Default: The keepalive interval is 60 seconds and the hold time is 240 seconds.

Command Mode: BGP Route Mode.

Usage Guidelines: Similar to the **neighbor timers** command, but applies to all neighbors.

Example:

```
Switch(config-router)# timers bgp 50 200
```

Related Commands: neighbor timers

5.6 IPv4 Black Hole Routing

5.6.1 ip route null0

Command: ip route {<ip-prefix> <mask>|<ip-prefix>|<prefix-length>} null0 [<distance>]
no ip route {<ip-prefix> <mask>|<ip-prefix>|<prefix-length>} null0

Function: Routes traffic destined for the specified network to the null0 interface.

Parameters: <ip-prefix> and **<mask>** are the destination IP address and mask in dotted decimal notation. **<ip-prefix>/<prefix-length>** are the destination IP address and prefix length. **null0** is the egress interface for black hole routing. **<distance>** is the administrative distance of the route, ranging from 1 to 255.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: Use null0 as the egress interface for IPv4 black hole routes.

Example: Configure the route to 192.168.188.0/24 as a black hole route.

```
Switch (config)# ip route 192.168.188.0/24 null0 20
```

5.7 GRE

5.7.1 debug gre

Command: debug gre {packet | events | all}
no debug gre {packet | events | all}

Function: Enables debugging for GRE tunnels.

Parameters: all: Displays all GRE tunnel debugging information.

packet: Displays information about packets sent and received on GRE tunnels.

events: Displays GRE tunnel event information.

Command Mode: Admin Mode.

Default: None.

Example: Enable all GRE tunnel debugging. Information about processing, encapsulation, and forwarding on the GRE tunnel is displayed.

```
Switch# debug gre all
GRE Tunnel PACKET: sent, src <1.1.1.1>, dst <1.1.1.2>, size <140>, proto
<0x0800>, to <tunnel1>
GRE Tunnel PACKET: recv, src <1.1.1.2>, dst <1.1.1.1>, size <140>, proto
<0x0800>, from <tunnel1>
```

5.7.2 ip address

Command: ip address <ipv4-address> <mask>
no ip address <ipv4-address> <mask>

Function: Configures the IPv4 address of a GRE tunnel interface.

Parameters: <ipv4-address> is the IPv4 address, and **<mask>** is the subnet mask.

Command Mode: Tunnel Mode.

Default: None.

Usage Guidelines: Only one primary IPv4 address can be configured on a GRE tunnel interface; secondary addresses are not supported. This limitation also applies to other tunnel types, such as configured, 6to4, and ISATAP tunnels.

Note: The tunnel must be active when an IPv4 address is configured; this differs from IPv6 addresses.

Example: Configure an IPv4 address on a GRE tunnel interface.

```
Switch(config)# interface tunnel 1
Switch(config-if-tunnel1)#ip address 11.0.0.1 255.255.255.0
```

5.7.3 ip route

Command: `ip route <ipv4-address/mask> tunnel <ID>`
`no ip route <ipv4-address/mask> tunnel <ID>`

Function: Configures a GRE tunnel as the egress interface of an IPv4 static route.

Parameters: <ipv4-address/mask> is the IPv4 address and mask length. **<ID>** is the GRE tunnel ID.

Command Mode: Global Mode.

Default: None.

Usage Guidelines: Configures a GRE tunnel as the egress interface of an IPv4 static route.

Example: Configure GRE tunnel 1 as the egress interface of an IPv4 static route.

```
Switch(config)# interface tunnel 1
Switch(config)#ip route 101.0.0.0/24 tunnel 1
```

5.7.4 ipv6 address

Command: `ipv6 address <ipv6-address/prefix>`
`no ipv6 address <ipv6-address/prefix>`

Function: Configures the IPv6 address of a GRE tunnel interface.

Parameters: <ipv6-address/prefix> is the IPv6 address and prefix length.

Command Mode: Tunnel Mode.

Default: None.

Usage Guidelines: Only one IPv6 address can be configured on a GRE tunnel interface. This limitation also applies to other tunnel types, such as configured, 6to4, and ISATAP tunnels.

Note: A 6to4 tunnel generates an IPv6 address automatically. An IPv6 address can be configured while the tunnel is active; this differs from IPv4 addresses.

Example: Configure an IPv6 address on a GRE tunnel interface.

```
Switch(config)# interface tunnel 1
Switch(config-if-tunnel1)#ipv6 address 2011::1/64
```

5.7.5 ipv6 route

Command: `ipv6 route <ipv6-address/prefix> tunnel <ID>`
`no ipv6 route <ipv6-address/prefix> tunnel <ID>`

Function: Configures a GRE tunnel as the egress interface of an IPv6 static route.

Parameters: <ipv6-address/prefix> is the IPv6 address and prefix length. **<ID>** is the GRE tunnel ID.

Command Mode: Global Mode.

Default: None.

Usage Guidelines: Configures a GRE tunnel as the egress interface of an IPv6 static route.

Example: Configure GRE tunnel 1 as the egress interface of an IPv6 static route.

```
Switch(config)# interface tunnel 1
```

```
Switch(config)# ipv6 route 2080::/64 tunnel 1
```

5.7.6 loopback-group (Global)

Command: `loopback-group <id>`
`no loopback-group <id>`

Function: Creates a loopback group. The **no** form of this command deletes it.

Parameters: <id> is the loopback group ID, ranging from 1 to 128.

Command Mode: Global Mode.

Default: None.

Usage Guidelines: Creates a loopback group.

Example: Create loopback group 1.

```
Switch(config)#loopback-group 1
```

5.7.7 loopback-group (Port)

Command: `loopback-group <id>`
`no loopback-group <id>`

Function: Adds a Layer 2 Ethernet port to the specified loopback group.

Parameters: <id> is the loopback group ID, ranging from 1 to 128.

Command Mode: Port Mode.

Default: None.

Usage Guidelines: The port must have no other configuration before it is added to a loopback group.

Example: Add port 1/1/1 to loopback group 1.

```
Switch (config-if-ethernet1/1/1)#loopback-group 1
```

5.7.8 loopback-group (Tunnel Interface)

Command: `loopback-group <id>`
`no loopback-group <id>`

Function: Binds the tunnel to the specified loopback group.

Parameters: <id> is the loopback group ID, ranging from 1 to 128.

Command Mode: Tunnel Mode.

Default: None.

Usage Guidelines: Binds the tunnel to a loopback group. Currently only GRE and ISATAP tunnels support this function; on an ISATAP tunnel, binding a loopback group is mutually exclusive with the next-hop configuration.

Example: Bind tunnel 1 to loopback group 1.

```
Switch (config-if-tunnel1)#loopback-group 1
```

5.7.9 show gre tunnel

Command: `show gre tunnel {<1-50 |>}`

Function: Displays GRE tunnel configuration information.

Parameters: <1-50>: The tunnel ID.

Command Mode: Admin Mode and Configuration Mode.

Default: None.

Example: Display GRE tunnel configuration information.

```
Switch# show gre tunnel
name          mode            source              destination
Tunnel1       gre ip          192.168.1.1         192.168.1.2
Tunnel2       gre ipv6        2001::1             2001::2
```

Output	Description
name	Tunnel name
mode	Tunnel type
source	Tunnel source address (IPv4 or IPv6)
destination	Tunnel destination address (IPv4 or IPv6)

5.7.10 show interface tunnel

Command: `show interface tunnel <1-50>`

Function: Displays information about a tunnel interface.

Parameters: <1-50>: The tunnel ID.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Example: Display information about the specified tunnel interface. If the tunnel is a GRE tunnel, GRE tunnel interface information is displayed.

```
Switch# show interface tunnel 1
Tunnel1 is up, line protocol is up, dev index is 8001
  Device flag 0x81(UP NOARP)
  IPv4 address is:
    (NULL)
  VRF Bind: Not Bind
```

5.7.11 tunnel destination

Command: `tunnel destination <ipv4-address>`
`no tunnel destination`

Function: Configures the IPv4 destination address of a GRE tunnel.

Parameters: <ipv4-address> is the IPv4 address.

Command Mode: Tunnel Mode.

Default: None.

Usage Guidelines: Configures the IPv4 destination address of a GRE tunnel.

Example: Configure the IPv4 destination address of a GRE tunnel.

```
Switch(config)# interface tunnel 1
Switch(config-if-tunnel1)#tunnel destination 60.0.0.3
```

5.7.12 tunnel mode gre ip

Command: `tunnel mode gre ip`
`no tunnel mode`

Function: Sets the tunnel mode to GREv4. Packets encapsulated with GREv4 carry an IPv4 header and traverse an IPv4 network.

Parameters: None.

Command Mode: Tunnel Mode.

Default: None.

Usage Guidelines: In GREv4 tunnel mode, packets are encapsulated with GREv4 before they are forwarded.

Example: Configure GREv4 encapsulation for forwarded packets.

```
Switch(config)# interface tunnel 1
Switch(config-if-tunnel1)# tunnel mode gre ip
```

5.7.13 tunnel source

Command: `tunnel source <ipv4-address>`
`no tunnel source`

Function: Configures the IPv4 source address of a GRE tunnel.

Parameters: <ipv4-address> is the IPv4 address.

Command Mode: Tunnel Mode.

Default: None.

Usage Guidelines: Configures the IPv4 source address of a GRE tunnel.

Example: Configure the IPv4 source address of a GRE tunnel.

```
Switch(config)# interface tunnel 1
Switch(config-if-tunnel1)#tunnel source 10.1.1.3
```

5.8 ECMP

5.8.1 load-balance

Command: `load-balance {dst-src-mac | dst-src-ip | dst-src-mac-ip}`

Function: Sets the load-balancing mode of the switch. The mode applies to both port channels and ECMP.

Parameters: dst-src-mac: Load balancing based on source and destination MAC addresses.

dst-src-ip: Load balancing based on destination and source IP addresses.

dst-src-mac-ip: Load balancing based on destination and source MAC addresses and destination and source IP addresses.

Command Mode: Global Mode.

Default: Load balancing based on source and destination MAC addresses.

Usage Guidelines: Port channels and ECMP both perform load balancing; configure the mode as required. If the specified mode differs from the current mode, the mode is changed; otherwise, a message indicates that the mode is already configured.

Example: Set the load-balancing mode.

```
Switch(config)#load-balance src-mac-ip
```

5.8.2 maximum-paths

Command: `maximum-paths <1-8>`
`no maximum-paths`

Function: Configures the maximum number of equal-cost multipaths (ECMP). The **no** form of this command restores the default.

Parameters: <1-8>: The number of paths, ranging from 1 to 8. A value of 1 disables ECMP.

Command Mode: Global Mode.

Default: 4.

Usage Guidelines: None.

Example: Set the maximum number of equal-cost paths to 8.

```
Switch(config)# maximum-paths 8
```

5.8.3 load-balance hash-shift

Command: **load-balance hash-shift { dstmac| srcmac | srcport | vlan | dstip | srcip | l4-srcport | l4-dstport | flow-label | proto} value < num >**

Function: Sets the hash shift of the specified field used in the load-balancing algorithm.

Parameters: **dstmac**: Applies the shift to the destination MAC address.

srcmac: Applies the shift to the source MAC address.

srcport: Applies the shift to the source port.

vlan: Applies the shift to the VLAN.

dstip: Applies the shift to the destination IP address.

srcip: Applies the shift to the source IP address.

l4-srcport: Applies the shift to the Layer 4 source port.

l4-dstport: Applies the shift to the Layer 4 destination port.

flow-label: Applies the shift to the flow label.

proto: Applies the shift to the protocol.

<num>: The shift value, ranging from 0 to 5.

Command Mode: Global Mode.

Default: Not set.

Usage Guidelines: Set the field shift to distribute traffic evenly across aggregated port members. This command is intended to help in troubleshooting unbalanced loads.

Example: Set the destination IP shift to 5.

```
Switch(config)# load-balance hash-shift dstip value 5
```

5.9 BFD

5.9.1 bfd authentication key

Command: **bfd authentication key <1-255>**
no bfd authentication key

Function: Enables BFD authentication and configures the key for the interface. The **no** form of this command disables BFD authentication.

Parameters: **<1-255>**: The key ID.

Default: BFD authentication is disabled on the interface.

Command Mode: Interface Mode.

Usage Guidelines: Configures the key ID of the BFD interface; different interfaces can use different authentication methods. As a result, the specified BFD interface uses authentication.

Example: Enable BFD authentication on the interface with key ID 1.

```
s5(config-if-vlan50)#bfd authentication key 1
```

5.9.2 bfd authentication key md5|sm3

Command: `bfd authentication key <1-255> md5|sm3 <WORD>`
`no bfd authentication key <1-255>`

Function: Configures the key and authentication string for BFD with MD5 (or SM3). The **no** form of this command deletes the key.

Parameters: <1-255>: The key ID. **<WORD>**: The key string, 1 to 16 bytes long.

Default: No key or string is configured.

Command Mode: Global Mode.

Usage Guidelines: Configures MD5 mode and the authentication string for BFD authentication. After this command is configured, BFD authentication is carried in the optional fields of packets. BFD establishes a neighbor only if the keys on both peers are the same.

Example: Use MD5 authentication with key ID 1 and authentication string 123456.

```
s5(config)#in vlan 50
s5(config)#bfd authentication key 1 md5 123456
```

5.9.3 bfd authentication key text

Command: `bfd authentication key <1-255> text <WORD>`
`no bfd authentication key <1-255>`

Function: Configures the key and authentication string for BFD with simple text authentication. The **no** form of this command deletes the key.

Parameters: <1-255>: The key ID. **<WORD>**: The key string, 1 to 16 bytes long.

Default: No key or string is configured.

Command Mode: Global Mode.

Usage Guidelines: Configures the mode and authentication string for BFD authentication. After this command is configured, BFD authentication is carried in the optional fields of packets. BFD establishes a neighbor only if the keys on both peers are the same.

Example: Use text authentication with key ID 1 and authentication string 123456.

```
s5(config)#bfd authentication key 1 text 123456
```

5.9.4 bfd echo

Command: `bfd echo`
`no bfd echo`

Function: Enables BFD echo. The **no** form of this command disables BFD echo.

Parameters: None.

Default: Echo is disabled on the interface.

Command Mode: Interface Mode.

Usage Guidelines: With BFD echo enabled, a session in the Up state sends echo packets, reducing the frequency of control packets.

Example: Enable echo on the interface.

```
s5(config)#in vlan 50
s5(config-if-vlan50)#bfd echo
```

5.9.5 bfd echo-source-ip

Command: **`bfd echo-source-ip <ipv4-address>`**
`no bfd echo-source-ip`

Function: Configures the source address of echo packets used to detect link faults. The **no** form of this command deletes the configured source address.

Parameters: <ipv4-address> is the IPv4 address. The switch does not check the validity of the address; ensure that it is valid.

Default: No echo source address is configured.

Command Mode: Global Mode.

Usage Guidelines: Configure the source address of echo packets when BFD echo is used to detect IPv4 link faults. The source address is optional; it only prevents ICMP redirect packets from being sent. The destination address of the packets is an interface address, which ensures that packets return along the original path. There are no special requirements for the UDP data.

Example: Set the source address of BFD echo packets to 192.168.1.1.

```
s5(config)#bfd echo-source-ip 192.168.1.1
```

5.9.6 bfd echo-source-ipv6

Command: **`bfd echo-source-ipv6 <ipv6-address>`**
`no bfd echo-source-ipv6`

Function: Configures the source address of IPv6 echo packets used to detect link faults. The **no** form of this command deletes the configured source address.

Parameters: <ipv6-address> is the IPv6 address. The switch does not check the validity of the address; ensure that it is valid.

Default: No echo source address is configured.

Command Mode: Global Mode.

Usage Guidelines: Configure the source address of echo packets when BFD echo is used to detect IPv6 link faults. The source address is optional; it only prevents ICMPv6 redirect packets from being sent. The destination address of the packets is an interface address, which ensures that packets return along the original path. There are no special requirements for the UDP data.

Example: Set the source address of BFD echo packets to 2000::1.

```
s5(config)#bfd echo-source-ipv6 2000::1
```

5.9.7 bfd enable

Command: **`bfd enable`**
`no bfd enable`

Function: Enables BFD for VRRP (or VRRPv3) and enables BFD detection on the group. The **no** form of this command disables BFD for VRRP (or VRRPv3).

Parameters: None.

Default: BFD is not enabled for VRRP or VRRPv3.

Command Mode: VRRP (VRRPv3) Group Mode.

Usage Guidelines: After BFD detection is enabled on the group, if the group receives Hello packets while in the Backup state, it notifies BFD to establish the corresponding session. The local and remote IP addresses are the interface addresses of the two peers.

Example: Enable BFD on VRRP group 1.

```
s5(config)#router vrrp 1
s5(config-router)#virtual-ip 50.1.1.10
```

```
s5(config-router)#interface vlan 50
s5(config-router)#bfd enable
s5(config-router)#enable
```

Enable BFD on VRRPv3 group 1.

```
s5(config)#router ipv6 vrrp 1
s5(config-router)#virtual-ipv6 fe80::1 interface vlan 50
s5(config-router)#bfd enable
s5(config-router)#enable
```

5.9.8 bfd interval

Command: `bfd interval <value1> min_rx <value2> multiplier <value3>`
`no bfd interval`

Function: Configures the minimum transmit interval, minimum receive interval, and detection multiplier of BFD control packets. The **no** form of this command restores the defaults.

Parameters: <value1>: The minimum transmit interval in milliseconds, ranging from 200 to 1000. The range may differ between devices.

<value2>: The minimum receive interval in milliseconds, ranging from 200 to 1000. The range may differ between devices.

<value3>: The detection multiplier, ranging from 3 to 50.

Default: The minimum transmit interval is 400 ms, the minimum receive interval is 400 ms, and the detection multiplier is 5.

Command Mode: Interface Mode.

Usage Guidelines: Configures the minimum transmit interval and detection multiplier of BFD control packets. The default minimum interval is 400 ms and the default detection multiplier is 5.

Example: Set the minimum transmit and receive intervals to 800 ms and the detection multiplier to 50 on the interface.

```
s5(config)#in vlan 50
s5(config-if-vlan50)#bfd interval 800 min-rx 800 multiplier 50
s5(config-if-vlan50)#
```

5.9.9 bfd min-echo-recv-interval

Command: `bfd min-echo-receive-interval <value>`
`no bfd min-echo-receive-interval`

Function: Configures the minimum receive interval of BFD echo packets. The **no** form of this command restores the default.

Parameters: <value>: The minimum receive interval in milliseconds, ranging from 200 to 1000. The range may differ between devices.

Default: 400 ms.

Command Mode: Interface Mode.

Usage Guidelines: The default minimum receive interval is 400 ms.

Example: Set the minimum receive interval of BFD echo packets to 800 ms.

```
s5(config)#in vlan 50
s5(config-if-vlan50)#bfd min-echo-recv-interval 800
```

5.9.10 bfd mode

Command: `bfd mode {active | passive}`
`no bfd mode`

Function: Configures the BFD operating mode used before the session is established. The default mode is active. The **no** form of this command restores active mode.

Parameters: active: Active mode. **passive**: Passive mode.

Default: Active mode.

Command Mode: Global Mode.

Usage Guidelines: Configures the BFD operating mode used before the session is established. In active mode, BFD control packets are sent whether or not any are received.

Example: Set the BFD operating mode to passive globally.

```
s1(config)#bfd mode passive
```

5.9.11 debug bfd

Command: `debug bfd {packet | event | all | fsm | error | timer | notify}`
Function: Enables BFD debugging.

Parameters: all: Enables all BFD debugging.

packet: Enables debugging of BFD packets sent and received.

event: Enables debugging of BFD events.

fsm: Displays the BFD state machine.

error: Displays BFD error events.

timer: Displays BFD timeout events.

notify: Displays BFD notification information.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Enables BFD debugging.

Example: Enable all BFD debugging.

```
s5#debug bfd all
```

5.9.12 ip ospf bfd enable

Command: `ip ospf bfd enable`
`no ip ospf bfd enable`

Function: Enables BFD for OSPF on the interface. The **no** form of this command disables BFD for OSPF.

Parameters: None.

Default: BFD is not enabled for OSPF.

Command Mode: Interface Mode.

Usage Guidelines: Enables BFD for OSPF on the interface. When BFD detects a link fault, it notifies OSPF, which then reacts promptly.

Example: Enable BFD for OSPF on the interface.

```
s5(config-if-vlan50)#ip ospf bfd enable
```

5.9.13 ip route bfd

Command: ip route {vrf <name> <ipv4-address> | <ipv4-address>} mask <nexthop> bfd
no ip route {vrf <name> <ipv4-address> | <ipv4-address>} mask <nexthop> bfd

Function: Configures BFD for a static route. The **no** form of this command cancels the configuration.

Parameters: <name> is the VRF name, **<ipv4-address>** is the destination address, **mask** is the subnet mask, and **<nexthop>** is the next-hop address.

Command Mode: Global Mode.

Default: BFD is not configured for static routes.

Usage Guidelines: Configures BFD detection for the route.

Example: Configure BFD for a static route.

```
s3(config)#ip route 10.1.1.0/24 20.1.1.2 bfd
```

5.9.14 ipv6 ospf bfd enable

Command: ipv6 ospf bfd enable
no ipv6 ospf bfd enable

Function: Enables BFD for OSPFv3 on the interface. The **no** form of this command cancels the configuration.

Parameters: None.

Default: BFD is not enabled for OSPFv3.

Command Mode: Interface Mode.

Usage Guidelines: Enables BFD for OSPFv3 on the interface. When BFD detects a link fault, it notifies OSPFv3, which then reacts promptly.

Example: Enable BFD for OSPFv3 on the interface.

```
s5(config-if-vlan50)#ipv ospf bfd enable
```

5.9.15 ipv6 ospf bfd enable instance-id

Command: ipv6 ospf bfd enable instance-id <0-255>
no ipv6 ospf bfd enable

Function: Enables BFD for an OSPFv3 instance on the interface. The **no** form of this command cancels the configuration.

Parameters: <0-255>: The OSPFv3 instance ID.

Default: BFD is not enabled for OSPFv3 instances.

Command Mode: Interface Mode.

Usage Guidelines: Enables BFD for the OSPFv3 instance on an interface running OSPFv3. When BFD detects a link fault, it notifies OSPFv3, which then reacts promptly.

Example: Enable BFD for OSPFv3 instance 254 on the interface.

```
s5(config-if-vlan50)#ipv ospf bfd enable instance-id 254
```

5.9.16 ipv6 rip bfd enable

Command: ipv6 rip bfd enable
no ipv6 rip bfd enable

Function: Enables BFD for RIPng on the interface. The **no** form of this command cancels the configuration.

Parameters: None.

Default: BFD is not enabled for RIPng.

Command Mode: Interface Mode.

Usage Guidelines: After BFD is enabled for RIPng, when the interface receives RIPng packets, RIPng asks BFD to establish a session with the remote IP address and monitor its state so that RIPng is notified promptly.

Example: Enable BFD for RIPng.

```
s5(config-if-vlan50)#ipv6 rip bfd enable
```

5.9.17 ipv6 route bfd

Command: ipv6 route {vrf <name> <ipv6-address> | <ipv6-address>} prefix <nexthop> bfd
no ipv6 route {vrf <name> <ipv6-address>|<ipv6-address>} prefix <nexthop> bfd

Function: Configures BFD for a static IPv6 route. The **no** form of this command cancels the configuration.

Parameters: <name> is the VRF name, **<ipv6-address>** is the destination address, **prefix** is the prefix length, and **<nexthop>** is the next-hop address.

Default: BFD is not configured for static IPv6 routes.

Command Mode: Global Mode.

Usage Guidelines: Configures BFD detection for the route.

Example: Configure BFD for a static IPv6 route.

```
s3(config)#ipv6 route 3000::/64 2010::1 bfd
```

5.9.18 neighbor

Command: neighbor {<ipv6-address> | <ipv4-address>} bfd
no neighbor {<ipv6-address> | <ipv4-address>}bfd

Function: Enables BFD link detection for a BGP or BGP4+ neighbor. The **no** form of this command cancels the configuration.

Parameters: <ipv4-address> is the IPv4 address.

<ipv6-address> is the IPv6 address.

The switch does not check the validity of the address; ensure that it is valid.

Default: BFD is not enabled for BGP or BGP4+.

Command Mode: BGP Route Mode.

Usage Guidelines: Enables BFD link detection for a BGP or BGP4+ neighbor. When BFD detects a fault on the link to the neighbor, it notifies BGP or BGP4+.

Example:

Enable BFD link detection for a BGP neighbor.

```
s5(config)#router bgp 1
s5(config-router)#neighbor 1.1.1.1 bfd
```

Enable BFD link detection for a BGP4+ neighbor.

```
s5(config-router)#router bgp 1
s5(config-router)#neighbor 2001::2 remote-as 200
s5(config-router)#neighbor 2001::2 bfd
```

5.9.19 rip bfd enable

Command: `rip bfd enable`
`no rip bfd enable`

Function: Enables BFD for RIP on the interface. The **no** form of this command disables BFD for RIP.

Parameters: None.

Default: BFD is not enabled for RIP.

Command Mode: Interface Mode.

Usage Guidelines: After BFD is enabled for RIP, when the interface receives RIP packets, RIP asks BFD to establish a session with the remote IP address and monitor its state so that RIP is notified.

Example: Enable BFD for RIP on the interface.

```
s5(config-if-vlan50)#rip bfd enable
```

5.9.20 show bfd neighbor

Command: `show bfd neighbor [[<ipv6-address>|<ipv4-address] [details]]`

Function: Displays BFD neighbors on the switch.

Parameters: <ipv6-address> specifies the IPv6 address of the neighbor and **<ipv4-address>** specifies the IPv4 address of the neighbor (the remote IP address). **details** displays detailed neighbor information.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays BFD neighbors on the switch.

Example: Display BFD neighbor information.

```
s5#show bfd neighbor 50.1.1.1 details
OurAddr     NeighAddr     LD/RD     Detec Int(ms)    State     Interface
50.1.1.5      50.1.1.1        1/1         2000           Up        3050
Local Diag: 0, Poll bit: 0
MinTx Int: 400(ms), MinRx Int: 400(ms), Multiplier: 5
Received MinRxInt: 400(ms), Received MinTxInt: 400(ms), Received Multiplier:
5
Local Act Trans Int: 400(ms), Remote Act Trans Int: 400(ms)
Local Act Detec Int: 2000(ms)
Registered protocols: RIP
Echo state: Disable, Echo Detec Int(ms): 2000
Multi Hop: No, Vrf Id: 0
Recv Ctl Pkt Num: 631, Send Ctl Pkt Num: 630
Recv Echo Pkt Num: 0, Send Echo Pkt Num: 0
Last packet:  Version: 1 - Diagnostic: 0
Poll bit: 0 - Final bit: 0
Multiplier: 5 - Length: 24
My Discr: 1 - Your Discr: 1
Min tx interval: 400(ms) - Min rx interval: 400(ms)
Min Echo interval: 400(ms)
```

5.10 BGP GR

5.10.1 bgp graceful-restart

Command: bgp graceful-restart
no bgp graceful-restart

Function: Enables graceful restart (GR) support for BGP and sets the restart time and stale path time to their default values. The **no** form of this command disables GR.

Parameters: None.

Command Mode: BGP Route Mode.

Default: GR is not enabled for BGP.

Usage Guidelines: None.

Example: Configure GR.

```
Switch(config-router)# bgp graceful-restart
```

5.10.2 bgp graceful-restart restart-time

Command: bgp graceful-restart restart-time <1-3600>
no bgp graceful-restart restart-time <1-3600>

Function: Configures the BGP GR restart time. The receiving speaker starts a timeout timer for the restarting neighbor using this value: the restart time is the maximum time the receiving speaker waits, after detecting the restart, to receive an OPEN message. If no OPEN message is received within this time, the receiving speaker deletes the stale routes saved for the neighbor. The **no** form of this command restores the default of 120 seconds.

Parameters: <1-3600>: The time in seconds.

Command Mode: BGP Route Mode.

Default: 120 seconds.

Usage Guidelines: None.

Example: Set the BGP GR restart time to 60 seconds.

```
Switch(config-router)# bgp graceful-restart restart-time 60
```

5.10.3 bgp graceful-restart stale-path-time

Command: bgp graceful-restart stale-path-time <1-3600>
no bgp graceful-restart stale-path-time <1-3600>

Function: Configures the BGP GR stale path time: the maximum time the receiving speaker waits, after receiving the OPEN message, to receive an End-of-RIB (EOR) marker before deleting stale routes. The **no** form of this command restores the default of 360 seconds.

Parameters: <1-3600>: The time in seconds.

Command Mode: BGP Route Mode.

Default: 360 seconds.

Usage Guidelines: None.

Example: Set the BGP GR stale path time to 460 seconds.

```
Switch(config-router)# bgp graceful-restart stale-path-time 460
```

5.10.4 bgp selection-deferral-time

Command: `bgp selection-deferral-time <1-3600>`
`no bgp selection-deferral-time <1-3600>`

Function: Configures the BGP GR selection deferral time: the maximum time the restarting speaker waits, after receiving the OPEN message, to receive an EOR marker before starting route selection. If no EOR is received within this time, the restarting speaker starts route selection. The **no** form of this command restores the default of 120 seconds.

Parameters: <1-3600>: The time in seconds.

Command Mode: BGP Route Mode.

Default: 120 seconds.

Usage Guidelines: None.

Example: Set the BGP GR selection deferral time to 240 seconds.

```
Switch(config-router)# bgp selection-deferral-time 240
```

5.10.5 neighbor capability graceful-restart

Command: `neighbor (A.B.C.D | X:X::X:X | WORD) capability graceful-restart`
`no neighbor (A.B.C.D | X:X::X:X | WORD) capability graceful-restart`

Function: Configures whether GR capability is advertised to the neighbor. The **no** form of this command disables GR capability for the neighbor.

Parameters: A.B.C.D | X:X::X:X | WORD: The BGP neighbor address or peer group name.

Command Mode: BGP Unicast Address-family Mode and VRF Address-family Mode.

Default: GR is not configured.

Usage Guidelines: None.

Example: Advertise GR capability to neighbor 1.1.1.1.

```
Switch(config-router)#neighbor 1.1.1.1 capability graceful-restart
```

5.11 OSPF GR

5.11.1 capability restart graceful

Command: `capability restart graceful`
`no capability restart`

Function: Enables GR for the specified OSPF process. The **no** form of this command disables this function.

Parameters: None.

Command Mode: OSPF Router Mode.

Default: OSPF GR is enabled.

Usage Guidelines: If GR is disabled while the switch is performing OSPF GR, the switch exits GR immediately.

Example: Enable OSPF GR.

```
Switch(config)#router ospf
Switch(config-router)#capability restart graceful
```

5.11.2 debug ospf events gr

Command: `debug ospf events gr`
`no debug ospf events gr`

Function: Enables debugging of OSPF GR events. The **no** form of this command disables this debugging.

Parameters: None.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: None.

Example: Enable debugging of OSPF GR events.

```
Switch#debug ospf events gr
```

5.11.3 ospf graceful-restart grace-period

Command: `ospf graceful-restart grace-period <integer>`
`no ospf restart grace-period`

Function: Configures the grace period of the GR restarter. The **no** form of this command restores the default.

Parameters: <integer>: The grace period in seconds, ranging from 1 to 1800.

Command Mode: Global Mode.

Default: 60 seconds.

Usage Guidelines: Configures the grace period of the GR restarter (the switch performing a switchover or protocol restart). The GR process must be completed within the grace period; if it is not, the switch exits GR and restarts OSPF normally.

Example: Set the grace period of the GR restarter to 100 seconds.

```
Switch(config)#ospf graceful-restart grace-period 100
```

5.11.4 ospf graceful-restart helper max-grace-period

Command: `ospf graceful-restart helper max-grace-period <integer>`
`no ospf graceful-restart helper`

Function: Configures one of the GR helper policies: the maximum grace period supported by the helper. The **no** form of this command deletes all configured helper policies.

Parameters: <integer>: The grace period in seconds, ranging from 1 to 1800.

Command Mode: Global Mode.

Default: The grace period supported by the helper is not limited.

Usage Guidelines: If the grace period set by the GR restarter is greater than the maximum grace period configured on the helper, the helper does not help the restarter complete GR. The **no** form deletes all helper policies.

Example: Set the maximum grace period supported by the GR helper to 100 seconds.

```
Switch(config)#ospf graceful-restart helper max-grace-period 100
```

5.11.5 ospf graceful-restart helper never

Command: `ospf graceful-restart helper never`
`no ospf graceful-restart helper`

Function: Configures one of the GR helper policies: the switch cannot act as an OSPF GR helper. The **no** form of this command deletes all configured helper policies.

Parameters: None.

Command Mode: Global Mode.

Default: The switch can act as a GR helper.

Usage Guidelines: With this policy configured, the switch can act only as a GR restarter (the switch performing a switchover or protocol restart), not as a GR helper (the switch that helps the restarter complete GR).

Example: Configure the switch so that it cannot act as an OSPF GR helper.

```
Switch(config)#ospf graceful-restart helper never
```

5.11.6 show ip ospf

Command: `show ip ospf [<process-id>]`

Function: Displays general OSPF information, including whether GR and GR helper mode are supported and the configured grace period.

Parameters: <process-id>: The process ID, ranging from 0 to 65535. If it is omitted, information about all processes is displayed.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: None.

Example: Display general OSPF information for all processes.

```
Switch#show ip ospf
Routing Process "ospf 0" with ID 192.168.40.69
 Process bound to VRF default
 Process uptime is 52 minutes
Conforms to RFC2328, and RFC1583Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Graceful Restart
 Supports helper mode for Graceful Restart
 Grace period for Graceful Restart 100 secs
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Refresh timer 10 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 0
 Number of LSA received 0
Number of areas attached to this router: 0
```

Output	Description
Supports Graceful Restart	The switch supports OSPF GR.
Supports helper mode for Graceful Restart	The switch supports OSPF GR helper mode.
Grace period for Graceful Restart 100 secs	The OSPF GR grace period configured on the switch is 100 seconds.

5.11.7 show ip ospf graceful-restart

Command: `show ip ospf [<process-id>] graceful-restart`

Function: Displays the OSPF GR state, including whether the switch is performing GR in helper mode and the remaining GR time.

Parameters: <process-id>: The process ID, ranging from 0 to 65535. If it is omitted, the GR state of all processes is displayed.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: None.

Example: Display the GR state of all processes on the GR restarter.

```
Switch#show ip ospf graceful-restart
OSPF process 0 graceful-restart information :
GR status        :GR in progress
GR remaining time : 50
```

Output	Description
OSPF process 0 graceful-restart information	OSPF GR state of process 0
GR status	GR state; "GR in progress" means that the switch is performing GR.
GR remaining time	Remaining GR time

Display the GR state of all processes on the GR helper:

```
Switch#show ip ospf graceful-restart
OSPF process 0 graceful-restart information:
GR status :Helper
Neighbor ID    Interface    Remaining time
1.1.1.1         Vlan1       100
2.2.2.2         Vlan1       200
```

Output	Description
OSPF process 0 graceful-restart information	OSPF GR state of process 0
GR status	GR state; "Helper" means that the switch is in helper mode.
Neighbor ID	Router ID of the restarter being helped
Interface	Layer 3 interface connected to the restarter
Remaining time	Remaining GR time

Chapter 6 Commands for Multicast Protocol

6.1 Multicast

6.1.1 show ip mroute

Command: show ip mroute [<GroupAddr> [<SourceAddr>]]

Function: Displays the IPv4 software multicast routing table.

Parameters: <GroupAddr>: Displays the multicast route entries for this group address.

<SourceAddr>: Displays the multicast route entries for this source address.

Default: None.

Command Mode: Admin Mode and Global Mode.

Usage Guidelines: None.

Example: Display all entries of the multicast routing table.

```
Switch(config)#show ip mroute
Name: Loopback, Index: 2002, State:49
Name: null0, Index: 2003, State:49
Name: sit0, Index: 2004, State:80
Name: Vlan1, Index: 2005, State:1043
Name: Vlan2, Index: 2006, State:1002
Name: pimreg, Index: 2007, State:c1
The total matched ipmr active mfc entries is 1, unresolved ipmr entries is 0
Group           Origin          Iif              Wrong     Oif:TTL
225.1.1.1       192.168.1.136   vlan1              0       2006:1
```

Output	Description
Name	Interface name
Index	Interface index
State	Interface state
The total matched ipmr active mfc entries	Total number of matched active IP multicast forwarding cache (MFC) entries
unresolved ipmr entries	Number of unresolved IP multicast route entries
Group	Destination (group) address of the entry
Origin	Source address of the entry
Iif	Ingress interface of the entry
Wrong	Number of packets received on the wrong interface
Oif	Egress interface of the entry
TTL	TTL value

6.2 PIM-DM

6.2.1 debug pim timer sat

Command: debug pim timer sat
no debug pim timer sat

Function: Enables detailed debugging of the PIM-DM source active timer (SAT). The **no debug pim timer sat** command disables this debugging.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Displays detailed source active timer information.

Example:

```
Switch # debug ip pim timer sat
```

Note: The other PIM-DM debugging commands are shared with PIM-SM, including **debug pim event**, **debug pim packet**, **debug pim nexthop**, **debug pim nsm**, **debug pim mfc**, **debug pim timer**, and **debug pim state**. See the PIM-SM section.

6.2.2 debug pim timer srt

Command: debug pim timer srt
no debug pim timer srt

Function: Enables detailed debugging of the PIM-DM state refresh timer (SRT). The **no debug pim timer srt** command disables this debugging.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Displays detailed PIM-DM state refresh timer information.

Example:

```
Switch #debug ip pim timer srt
```

Note: The other PIM-DM debugging commands are shared with PIM-SM, including **debug pim event**, **debug pim packet**, **debug pim nexthop**, **debug pim nsm**, **debug pim mfc**, **debug pim timer**, and **debug pim state**. See the PIM-SM section.

6.2.3 ip mroute

Command: ip mroute <A.B.C.D> <A.B.C.D> <ifname> <.ifname>
no ip mroute <A.B.C.D> <A.B.C.D> [<ifname> <.ifname>]

Function: Configures a static multicast entry. The **no** form of this command deletes static multicast entries or egress interfaces.

Parameters: <A.B.C.D> <A.B.C.D> are the multicast source address and group address.

<ifname> <.ifname>: The first interface is the ingress interface; the following interfaces are egress interfaces.

Default: None. If the **no** form is entered without interface parameters, the static multicast entry is deleted.

Command Mode: Global Mode.

Usage Guidelines: Each **<ifname>** must be a valid VLAN interface. Multicast traffic is forwarded only if PIM is configured on the egress interface and the interface is up; if the interface is not up, PIM is not configured, or the RPF check fails, the traffic is not forwarded. With the **no** form, if all egress interfaces or no interfaces are specified, the multicast routing entry is removed; otherwise, only the specified interfaces are removed from the entry.

Example:

```
Switch(config)#ip mroute 10.1.1.1 225.1.1.1 v10 v20 v30
```

6.2.4 ip pim bsr-border

Command: ip pim bsr-border
no ip pim bsr-border

Function: Configures or deletes a PIM BSR border interface.

Parameters: None.

Default: The interface is not a BSR border.

Command Mode: Interface Mode.

Usage Guidelines: Configures the interface as a BSR border. BSR messages are then neither received on nor sent from the interface, and all networks connected to the interface are treated as directly connected.

Example:

```
Switch(Config-if-Vlan1)#no ip pim bsr-border
```

6.2.5 ip pim dense-mode

Command: `ip pim dense-mode`
`no ip pim dense-mode`

Function: Enables PIM-DM on the interface. The **no ip pim dense-mode** command disables PIM-DM on the interface.

Parameters: None.

Default: PIM-DM is disabled.

Command Mode: Interface Mode.

Usage Guidelines: This command takes effect only after multicast routing is enabled in Global Mode. Multicast protocol interoperation is not supported; dense mode and sparse mode cannot be enabled on the same switch at the same time.

Example: Enable PIM-DM on interface VLAN 1.

```
Switch (config)#ip pim multicast-routing
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ip pim dense-mode
```

6.2.6 ip pim dr-priority

Command: `ip pim dr-priority <priority>`
`no ip pim dr-priority`

Function: Configures the DR priority of the interface. Neighbors on the same network segment elect the DR of the segment based on Hello packets. The **no ip pim dr-priority** command restores the default.

Parameters: <priority> is the priority, ranging from 0 to 4294967294. A higher value means a higher priority.

Default: 1

Command Mode: Interface Mode.

Usage Guidelines: The priority ranges from 0 to 4294967294; a higher value has higher priority.

Example: Set the DR priority of VLAN 1 to 100.

```
Switch (config)# interface vlan 1
Switch(Config-if-Vlan1)ip pim dr-priority 100
Switch (Config -if-Vlan1)#
```

6.2.7 ip pim exclude-genid

Command: `ip pim exclude-genid`
`no ip pim exclude-genid`

Function: Excludes the GenID option from Hello packets sent by PIM-SM. The **no ip pim exclude-genid** command restores the default.

Parameters: None.

Default: Hello packets include the GenID option.

Command Mode: Interface Mode.

Usage Guidelines: Use this command to interoperate with older Cisco IOS versions.

Example: Exclude the GenID option from Hello packets sent by the switch.

```
Switch (Config-if-Vlan1)#ip pim exclude-genid
Switch (Config-if-Vlan1)#
```

6.2.8 ip pim hello-holdtime

Command: `ip pim hello-holdtime <value>`
`no ip pim hello-holdtime`

Function: Configures the Holdtime option in Hello packets. This value is the neighbor hold time: if no Hello packet is received from a neighbor within this time, the neighbor is deleted. The **no ip pim hello-holdtime** command cancels the configured value and restores the default.

Parameters: <value> is the hold time.

Default: 3.5 × the Hello interval. The default Hello interval is 30 seconds, so the default hold time is 105 seconds.

Command Mode: Interface Mode.

Usage Guidelines: If this value is not configured, the hold time is 3.5 × the Hello interval. A configured hold time that is less than the current Hello interval is rejected. Whenever the Hello interval is changed, the hold time is updated as follows: if the hold time is not configured, or is configured but less than the current Hello interval, it is changed to 3.5 × the Hello interval; otherwise, the configured value is kept.

Example: Configure the Hello hold time of VLAN 1.

```
Switch (config)# interface vlan1
Switch (Config -if-Vlan1)#ip pim hello-holdtime 10
Switch (Config -if-Vlan1)#
```

6.2.9 ip pim hello-interval

Command: `ip pim hello-interval < interval>`
`no ip pim hello-interval`

Function: Configures the PIM-DM Hello interval of the interface. The **no ip pim hello-interval** command restores the default.

Parameters: <interval> is the interval at which PIM-DM Hello messages are sent periodically, ranging from 1 to 18724 seconds.

Default: 30 seconds.

Command Mode: Interface Mode.

Usage Guidelines: Hello messages allow PIM-DM switches to discover each other and maintain neighbor relationships. A PIM-DM switch announces its presence by periodically sending Hello messages to its neighbors; if it receives no Hello messages from a neighbor within the specified time, it considers the neighbor lost. The configured interval must not exceed the neighbor timeout.

Example: Configure the PIM-DM Hello interval on interface VLAN 1.

```
Switch (config)#interface vlan1
Switch(Config-if-Vlan1)#ip pim hello-interval 20
```

6.2.10 ip pim multicast-routing

Command: ip pim multicast-routing
no ip pim multicast-routing

Function: Enables PIM multicast routing globally. The **no ip pim multicast-routing** command disables it globally.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Enables PIM globally. PIM must also be enabled on interfaces for it to work.

Example: Enable PIM multicast routing globally.

```
Switch (config)#ip pim multicast-routing
```

6.2.11 ip pim neighbor-filter

Command: ip pim neighbor-filter <list-number>
no ip pim neighbor-filter <list-number>

Function: Configures a neighbor access list. If an existing neighbor is filtered by the list, its connection is torn down immediately; if no connection exists, it cannot be established.

Parameters: <list-number> is the standard access list number, ranging from 1 to 99.

Default: No neighbor filter is configured.

Command Mode: Interface Mode.

Usage Guidelines: The default action of an ACL is deny. For example, if access list 1 is configured, its default action is deny. In the following example, if **permit any-source** is not configured, **deny 10.1.4.10 0.0.0.255** has the same effect as **deny any-source**.

Example: Configure PIM neighbor filtering rules on a VLAN interface.

```
Switch #show ip pim neighbor
Neighbor          Interface          Uptime/Expires    Ver   DR
Address                                                    Priority/Mode
10.1.4.10         Vlan1              02:30:30/00:01:41 v2    4294967294 / DR
Switch (Config-if-Vlan1)#ip pim neighbor-filter 2
Switch (config)#access-list 2 deny 10.1.4.10 0.0.0.255
Switch (config)#access-list 2 permit any-source
Switch (config)#show ip pim neighbor
Switch (config)#
```

6.2.12 ip pim scope-border

Command: ip pim scope-border [<1-99 >|<acl_name>]
no ip pim scope-border

Function: Configures or deletes a PIM administrative scope border.

Parameters: <1-99>: The number of the ACL for the administrative scope border.

<acl_name>: The name of the ACL for the administrative scope border.

Default: No administrative scope border is configured. If no ACL is specified, the default administrative scope border is used.

Command Mode: Interface Mode.

Usage Guidelines: Configures the administrative scope border and its ACL for PIM. Multicast traffic is not forwarded across the scope border.

Example:

```
Switch(Config-if-Vlan2)#ip pim scope-border 3
```

6.2.13 ip pim state-refresh origination-interval

Command: `ip pim state-refresh origination-interval <interval>`
`no ip pim state-refresh origination-interval`

Function: Configures the interval at which state refresh messages are sent. The **no ip pim state-refresh origination-interval** command restores the default.

Parameters: <interval>: The transmission interval, ranging from 4 to 100 seconds.

Default: 60 seconds.

Command Mode: Global Mode.

Usage Guidelines: The first-hop router periodically sends state refresh messages to maintain the PIM-DM entries of all downstream routers. Use this command to change the origination interval of state refresh messages. Normally this timer does not need to be changed.

Example: Set the state refresh message interval to 90 seconds.

```
Switch (config)#ip pim state-refresh origination-interval 90
```

6.2.14 show ip pim interface

Command: `show ip pim interface`

Function: Displays PIM interface information.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Global Mode.

Usage Guidelines: Displays PIM interface information.

Example:

```
Switch(config)#show ip pim interface
Address          Interface VIFindex Ver/   Nbr    DR    DR
                                    Mode  Count  Prior
10.1.4.3         Vlan1     0        v2/S   1      1     10.1.4.3
10.1.7.1         Vlan2     2        v2/S   0      1     10.1.7.1
```

Output	Description
Address	Interface address
Interface	Interface name
VIF index	Interface index
Ver/Mode	PIM version and mode. The version is usually v2; S indicates sparse mode and D indicates dense mode.
Nbr Count	Number of neighbors on the interface
DR Prior	DR priority
DR	DR address of the interface

6.2.15 show ip pim mroute dense-mode

Command: `show ip pim mroute dense-mode [group <A.B.C.D>] [source <A.B.C.D>]`

Function: Displays PIM-DM multicast forwarding entries.

Parameters: group <A.B.C.D>: Displays forwarding entries for this multicast group address.

source <A.B.C.D>: Displays forwarding entries for this source.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays PIM-DM multicast forwarding entries, that is, the entries used to forward multicast packets in the system FIB.

Example: Display all PIM-DM multicast forwarding entries.

```
Switch(config)#show ip pim mroute dense-mode
IP Multicast Routing Table
(*,G) Entries: 1
(S,G) Entries: 1
(*, 226.0.0.1)
 Local     ..l.............................
(192.168.1.12, 226.0.0.1)
RPF nbr: 0.0.0.0
RPF idx: Vlan2
Upstream State: FORWARDING
Origin State: ORIGINATOR
 Local     ..............................
 Pruned    ..............................
 Asserted  ..............................
 Outgoing  ..o...........................
Switch#
```

Output	Description
(*,226.0.0.1)	(*,G) forwarding entry
(192.168.1.12, 226.0.0.1)	(S,G) forwarding entry
RPF nbr	RPF neighbor: the upstream neighbor toward the source in DM. 0.0.0.0 indicates that the switch is the first hop.
RPF idx	Interface on which the RPF neighbor is located
Upstream State	Upstream state: FORWARDING (upstream data is forwarded), PRUNED (upstream stops forwarding data), or ACKPENDING (waiting for an upstream response while forwarding upstream data)
Origin State	Origination state: ORIGINATOR (sends state refresh messages) or NON_ORIGINATOR (does not send state refresh messages)
Local	Local join interfaces: interfaces that received IGMP joins
Pruned	Pruned interfaces: interfaces that received Prune messages
Asserted	Assert state
Outgoing	Interfaces to which multicast data is finally sent, shown by index; in this example, the index is 2. Use **show ip pim interface** to view detailed interface information.

6.2.16 show ip pim neighbor

Command: `show ip pim neighbor`

Function: Displays PIM neighbors.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Global Mode.

Usage Guidelines: Displays the multicast router neighbors maintained by PIM.

Example:

```
Switch (config)#show ip pim neighbor
Neighbor          Interface          Uptime/Expires    Ver   DR
Address                                                    Priority/Mode
10.1.6.1          Vlan1              00:00:10/00:01:35 v2    1 /
10.1.6.2          Vlan1              00:00:13/00:01:32 v2    1 /
10.1.4.2          Vlan3              00:00:18/00:01:30 v2    1 /
10.1.4.3          Vlan3              00:00:17/00:01:29 v2    1 /
```

Output	Description
Neighbor Address	Neighbor address
Interface	Interface connected to the neighbor
Uptime/Expires	Uptime and expiration time
Ver	PIM version, usually v2
DR Priority/Mode	DR priority carried in Hello messages from the neighbor, and whether the neighbor is the DR of the interface

6.2.17 show ip pim nexthop

Command: `show ip pim nexthop`

Function: Displays the next-hop routers buffered by PIM from the unicast routing table.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Global Mode.

Usage Guidelines: Displays the next-hop router information buffered by PIM.

Example:

```
Switch(config)#show ip pim nexthop
Flags: N = New, R = RP, S = Source, U = Unreachable
Destination     Type  Nexthop  Nexthop      Nexthop  Nexthop Metric Pref
Refcnt                  Num      Addr        Ifindex    Name
192.168.1.1      N...   1       0.0.0.0        2006             0      0
1
192.168.1.9     ..S.    1       0.0.0.0        2006             0      0
1
```

Output	Description
Destination	Destination of the next-hop entry
Type	N: Newly created next hop; RP and source direction not yet determined. R: RP direction. S: Source direction. U: Unreachable.
Nexthop Num	Number of next hops
Nexthop Addr	Next-hop address
Nexthop Ifindex	Next-hop interface index
Nexthop Name	Next-hop interface name
Metric	Metric to the next hop
Pref	Route preference
Refcnt	Reference count

6.3 PIM-SM

6.3.1 clear ip pim bsr rp-set

Command: `clear ip pim bsr rp-set *`

Function: Clears all RPs.

Parameters: None.

Command Mode: Admin Mode.

Usage Guidelines: Quickly clears all RPs.

Example: Clear all RPs.

```
Switch# clear ip pim bsr rp-set *
```

Related Commands: **show ip pim bsr-router**

6.3.2 debug pim event

Command: debug pim event
no debug pim event

Function: Enables or disables PIM event debugging.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Enables PIM event debugging and displays information about PIM operation events.

Example:

```
Switch# debug ip pim event
Switch#
```

6.3.3 debug pim mfc

Command: debug pim mfc
no debug pim mfc

Function: Enables or disables PIM MFC debugging.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Enables PIM MFC debugging and displays information about the multicast forwarding entries that are generated and sent.

Example:

```
Switch# debug ip pim mfc
```

6.3.4 debug pim mib

Command: debug pim mib
no debug pim mib

Function: Enables or disables PIM MIB debugging.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Displays PIM MIB information. This function is not currently available and is reserved for future extension.

Example:

```
Switch# debug ip pim mib
```

6.3.5 debug pim nexthop

Command: **debug pim nexthop**
no debug pim nexthop

Function: Enables or disables PIM next-hop debugging.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Displays PIM next-hop change information.

Example:

```
Switch# debug ip pim nexthop
```

6.3.6 debug pim nsm

Command: **debug pim nsm**
no debug pim nsm

Function: Enables or disables debugging of communication between PIM and the Network Services Module (NSM).

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Displays information exchanged between PIM and the NSM.

Example:

```
Switch# debug ip pim nsm
```

6.3.7 debug pim packet

Command: **debug pim packet**
debug pim packet in
debug pim packet out
no debug pim packet
no debug pim packet in
no debug pim packet out

Function: Enables or disables PIM packet debugging.

Parameters: **in**: Displays only received PIM packets.

out: Displays only sent PIM packets.

If neither is specified, both are displayed.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Displays received and sent PIM packets.

Example:

```
Switch# debug ip pim packet in
```

6.3.8 debug pim state

Command: **debug pim state**
no debug pim state

Function: Enables or disables PIM state debugging.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Displays PIM state change information.

Example:

```
Switch# debug ip pim state
```

6.3.9 debug pim timer

Command: debug pim timer

```
debug pim timer assert
debug pim timer assert at
debug pim timer bsr bst
debug pim timer bsr crp
debug pim timer bsr
debug pim timer hello ht
debug pim timer hello nlt
debug pim timer hello tht
debug pim timer hello
debug pim timer joinprune et
debug pim timer joinprune jt
debug pim timer joinprune kat
debug pim timer joinprune ot
debug pim timer joinprune plt
debug pim timer joinprune ppt
debug pim timer joinprune pt
debug pim timer joinprune
debug pim timer register rst
debug pim timer register
no debug pim timer
no debug pim timer assert
no debug pim timer assert at
no debug pim timer bsr bst
no debug pim timer bsr crp
no debug pim timer bsr
no debug pim timer hello ht
no debug pim timer hello nlt
no debug pim timer hello tht
no debug pim timer hello
no debug pim timer joinprune et
no debug pim timer joinprune jt
no debug pim timer joinprune kat
no debug pim timer joinprune ot
no debug pim timer joinprune plt
no debug pim timer joinprune ppt
no debug pim timer joinprune pt
no debug pim timer joinprune
no debug pim timer register rst
no debug pim timer register
```

Function: Enables or disables debugging of individual PIM timers.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Enables debugging information for the specified timer.

Example:

```
Switch# debug pim timer assert
Switch#
```

6.3.10 ip mroute

Command: `ip mroute <A.B.C.D> <A.B.C.D> <ifname> <.ifname>`
`no ip mroute <A.B.C.D> <A.B.C.D> [<ifname> <.ifname>]`

Function: Configures a static multicast entry. The **no** form of this command deletes static multicast entries or egress interfaces.

Parameters: <A.B.C.D> <A.B.C.D> are the multicast source address and group address.

<ifname> <.ifname>: The first interface is the ingress interface; the following interfaces are egress interfaces.

Default: None. If the **no** form is entered without interface parameters, the static multicast entry is deleted.

Command Mode: Global Mode.

Usage Guidelines: Each **<ifname>** must be a valid VLAN interface. Multicast traffic is forwarded only if PIM is configured on the egress interface and the interface is up; if the interface is not up, PIM is not configured, or the RPF check fails, the traffic is not forwarded. With the **no** form, if all egress interfaces or no interfaces are specified, the multicast routing entry is removed; otherwise, only the specified interfaces are removed from the entry.

Example:

```
Switch(config)#ip mroute 10.1.1.1 225.1.1.1 v10 v20 v30
```

6.3.11 ip multicast unresolved-cache aging-time

Command: `ip multicast unresolved-cache aging-time <value>`
`no ip multicast unresolved-cache aging-time`

Function: Configures the cache time of unresolved kernel multicast route entries. The **no** form of this command restores the default.

Parameters: <value> is the cache time, ranging from 1 to 20 seconds.

Default: 10 seconds.

Command Mode: Global Mode.

Usage Guidelines: Configures the cache time of multicast route entries in the kernel.

Example:

```
Switch(config)# ip multicast unresolved-cache aging-time 18
```

6.3.12 ip pim accept-register

Command: `ip pim accept-register list <list-number>`
`no ip pim accept-register`

Function: Filters PIM register messages for the specified multicast sources and groups.

Parameters: <list-number> is the access list number, ranging from 1 to 99 (standard access lists) or 100 to 199 (extended access lists).

Default: Register messages from any source to any group are permitted.

Command Mode: Global Mode.

Usage Guidelines: Configures the access list used to filter PIM REGISTER packets. The addresses in the access list specify the multicast sources and groups to filter. For source-group pairs that match a deny rule, PIM immediately sends REGISTER-STOP and does not create group entries when it receives REGISTER packets. Unlike other access lists, the default action of this access list is permit.

Example: Configure access list 120 as the register message filter.

```
Switch(config)#ip pim accept-register list 120
Switch (config)#access-list 120 deny ip 10.1.0.2 0.0.0.255 239.192.1.10
0.0.0.255
Switch (config)#
```

6.3.13 ip pim bsr-border

Command: `ip pim bsr-border`
`no ip pim bsr-border`

Function: Configures or deletes a PIM BSR border interface.

Parameters: None.

Default: The interface is not a BSR border.

Command Mode: Interface Mode.

Usage Guidelines: Configures the interface as a BSR border. BSR messages are then neither received on nor sent from the interface, and all networks connected to the interface are treated as directly connected.

Example:

```
Switch(Config-if-Vlan1)#no ip pim bsr-border
```

6.3.14 ip pim bsr-candidate

Command: `ip pim bsr-candidate {vlan <vlan-id>| <ifname>} [hash-mask-length] [priority]`
`no ip pim bsr-candidate`

Function: Configures the switch as a candidate BSR so that it competes with other candidate BSRs to become the BSR. The **no ip pim bsr-candidate** command disables the candidate BSR.

Parameters: vlan <vlan-id> | <ifname> specifies the interface.

hash-mask-length is the hash mask length used for RP selection, ranging from 0 to 32.

priority is the candidate BSR priority, ranging from 0 to 255. The default is 0.

Default: The switch is not a candidate BSR.

Command Mode: Global Mode.

Usage Guidelines: Configures candidate BSR information for PIM-SM so that the switch competes with other candidate BSRs to become the BSR. The switch is a candidate BSR only when this command is configured.

Example: Configure interface VLAN 1 as the candidate BSR interface globally.

```
Switch (config)# ip pim bsr-candidate vlan1 30 10
```

6.3.15 ip pim cisco-register-checksum

Command: `ip pim cisco-register-checksum [group-list <simple-acl>]`
`no ip pim cisco-register-checksum [group-list <simple-acl>]`

Function: Calculates the checksum of register packets for the groups specified by the ACL over the entire packet length.

Default: The checksum is calculated over the register packet header (8 bytes).

Parameters: <simple-acl>: A standard access list, 1 to 99.

Command Mode: Global Mode.

Usage Guidelines: Use this command to interoperate with older Cisco IOS versions.

Example: Calculate the register packet checksum over the entire packet length for the groups specified by access list 23.

```
Switch (config)#ip pim cisco-register-checksum group-list 23
```

6.3.16 ip pim dr-priority

Command: `ip pim dr-priority <priority>`
`no ip pim dr-priority`

Function: Configures the DR priority of the interface. Neighbors on the same network segment elect the DR of the segment based on Hello packets. The **no ip pim dr-priority** command restores the default.

Parameters: <priority> is the priority, ranging from 0 to 4294967294. A higher value means a higher priority.

Default: 1

Command Mode: Interface Mode.

Usage Guidelines: The priority ranges from 0 to 4294967294; a higher value has higher priority.

Example: Set the DR priority of VLAN 1 to 100.

```
Switch (config)# interface vlan 1
Switch(Config-if-Vlan1)ip pim dr-priority 100
Switch (Config -if-Vlan1)#
```

6.3.17 ip pim exclude-genid

Command: `ip pim exclude-genid`
`no ip pim exclude-genid`

Function: Excludes the GenID option from Hello packets sent by PIM-SM. The **no ip pim exclude-genid** command restores the default.

Parameters: None.

Default: Hello packets include the GenID option.

Command Mode: Interface Mode.

Usage Guidelines: Use this command to interoperate with older Cisco IOS versions.

Example: Exclude the GenID option from Hello packets sent by the switch.

```
Switch (Config-if-Vlan1)#ip pim exclude-genid
Switch (Config-if-Vlan1)#
```

6.3.18 ip pim hello-holdtime

Command: `ip pim hello-holdtime <value>`
`no ip pim hello-holdtime`

Function: Configures the Holdtime option in Hello packets. This value is the neighbor hold time: if no Hello packet is received from a neighbor within this time, the neighbor is deleted. The **no ip pim hello-holdtime** command cancels the configured value and restores the default.

Parameters: <value> is the hold time.

Default: 3.5 × the Hello interval. The default Hello interval is 30 seconds, so the default hold time is 105 seconds.

Command Mode: Interface Mode.

Usage Guidelines: If this value is not configured, the hold time is 3.5 × the Hello interval. A configured hold time that is less than the current Hello interval is rejected. Whenever the Hello interval is changed, the hold time is updated as follows: if the hold time is not configured, or is configured but less than the current Hello interval, it is changed to 3.5 × the Hello interval; otherwise, the configured value is kept.

Example: Configure the Hello hold time of VLAN 1.

```
Switch (config)# interface vlan1
Switch (Config -if-Vlan1)#ip pim hello-holdtime 10
Switch (Config -if-Vlan1)#
```

6.3.19 ip pim hello-interval

Command: `ip pim hello-interval <interval>`
`no ip pim hello-interval`

Function: Configures the interval at which PIM Hello packets are sent on the interface. The **no ip pim hello-interval** command restores the default.

Parameters: <interval> is the interval at which PIM Hello packets are sent periodically, ranging from 1 to 18724 seconds.

Default: 30 seconds.

Command Mode: Interface Mode.

Usage Guidelines: Hello messages allow PIM switches to discover each other and establish neighbor relationships. A PIM switch announces its presence by periodically sending Hello messages to its neighbors; if it receives no Hello messages from a neighbor within the specified time, it considers the neighbor lost. This value must not exceed the neighbor timeout.

Example: Configure the PIM-SM Hello interval on VLAN 1.

```
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ip pim hello-interval 20
Switch(Config-if-Vlan1)#
```

6.3.20 ip pim ignore-rp-set-priority

Command: `ip pim ignore-rp-set-priority`
`no ip pim ignore-rp-set-priority`

Function: Configures the switch to use only the hash algorithm and ignore RP priority during RP selection. Use this command to interoperate with older Cisco IOS versions.

Default: Disabled.

Parameters: None.

Command Mode: Global Mode.

Usage Guidelines: PIM normally selects the RP based on RP priority. With this command configured, RP priority is ignored. Use this command only if older routers are present on the network.

Example:

```
Switch (config)#ip pim ignore-rp-set-priority
```

6.3.21 ip pim jp-timer

Command: **ip pim jp-timer <value>**
no ip pim jp-timer

Function: Configures the Join/Prune timer. The **no ip pim jp-timer** command restores the default.

Parameters: **<value>** ranges from 10 to 65535 seconds.

Default: 60 seconds.

Command Mode: Global Mode.

Usage Guidelines: Configures the interval at which PIM periodically sends JOIN-PRUNE packets. The default is 60 seconds; keeping the default is recommended unless there is a specific reason to change it.

Example: Configure the Join/Prune timer interval.

```
Switch (config)#ip pim jp-timer 59
```

6.3.22 ip pim multicast-routing

Command: **ip pim multicast-routing**
no ip pim multicast-routing

Function: Enables PIM-SM globally. The **no ip pim multicast-routing** command disables PIM-SM globally.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Enables PIM-SM globally. PIM-SM must also be enabled on interfaces for it to work.

Example: Enable PIM-SM globally.

```
Switch (config)#ip pim multicast-routing
Switch (config)#
```

6.3.23 ip pim neighbor-filter

Command: **ip pim neighbor-filter <list-number>**
no ip pim neighbor-filter <list-number>

Function: Configures a neighbor access list. If an existing neighbor is filtered by the list, its connection is torn down immediately; if no connection exists, it cannot be established.

Parameters: **<list-number>** is the standard access list number, ranging from 1 to 99.

Default: No neighbor filter is configured.

Command Mode: Interface Mode.

Usage Guidelines: The default action of an ACL is deny. For example, if access list 1 is configured, its default action is deny. In the following example, if **permit any** is not configured, **deny 10.1.4.10 0.0.0.255** has the same effect as **deny any**.

Example: Configure PIM neighbor filtering rules on a VLAN interface.

```
Switch #show ip pim neighbor
```

```
Neighbor          Interface          Uptime/Expires    Ver   DR
Address                                                      Priority/Mode
10.1.4.10         Vlan1              02:30:30/00:01:41 v2    4294967294 / DR
Switch (Config-if-Vlan1)#ip pim neighbor-filter 2
Switch (config)#access-list 2 deny 10.1.4.10 0.0.0.255
Switch (config)#access-list 2 permit any
Switch (config)#show ip pim neighbor
```

6.3.24 ip pim register-rate-limit

Command: ip pim register-rate-limit <limit>
no ip pim register-rate-limit

Function: Configures the rate at which the DR sends register packets, in packets per second. The **no ip pim register-rate-limit** command restores the default. The rate applies to each (S,G) state, not to the whole system.

Parameters: <limit> ranges from 1 to 65535.

Default: No rate limit.

Command Mode: Global Mode.

Usage Guidelines: This configuration protects the DR against attacks by limiting the rate at which REGISTER packets are sent.

Example: Limit the rate at which the DR sends register packets to 59 packets per second.

```
Switch (config)#ip pim register-rate-limit 59
Switch (config)#
```

6.3.25 ip pim register-rp-reachability

Command: ip pim register-rp-reachability
no ip pim register-rp-reachability

Function: Configures the DR to check RP reachability during registration.

Parameters: None.

Default: Not checked.

Command Mode: Global Mode.

Usage Guidelines: Configures whether the DR checks RP reachability.

Example: Configure the DR to check RP reachability.

```
Switch (config)#ip pim register-rp-reachability
Switch (config)#
```

6.3.26 ip pim register-source

Command: ip pim register-source {<A.B.C.D> | <ifname>| vlan <vlan-id>}
no ip pim register-source

Function: Configures the source address of register packets sent by the DR, overriding the default source address. The default source address is usually the address of the interface toward the source host (the RPF interface).

Parameters: <ifname> is the interface name.

<vlan-id> is the VLAN ID.

<A.B.C.D> is the configured source IP address.

Default: Not configured.

Command Mode: Global Mode.

Usage Guidelines: The **no ip pim register-source** command restores the default; no parameter is needed. The configured address must be reachable by Register-Stop messages sent by the RP. It is usually a loopback address but can be another physical address, and it must be advertised by the unicast routing protocol on the DR.

Example: Configure the source address of register packets sent by the DR.

```
Switch (config)#ip pim register-source 10.1.1.1
```

6.3.27 ip pim register-suppression

Command: ip pim register-suppression <value>
no ip pim register-suppression

Function: Configures the register suppression timer, in seconds. The **no ip pim register-suppression** command restores the default.

Parameters: <value> is the timer value, ranging from 10 to 65535 seconds.

Default: 60 seconds.

Command Mode: Global Mode.

Usage Guidelines: When configured on the DR, this value is the register suppression time. On the RP, the register keepalive time is the greater of the default RP register keepalive time (210 seconds) and three times the register suppression time plus 5. If this value is configured on the RP without **ip pim rp-register-kat**, this command may change the RP register keepalive time.

Example: Set the register suppression timer to 10 seconds.

```
Switch (config)#ip pim register- suppression 10
Switch (config)#
```

6.3.28 ip pim rp-address

Command: ip pim rp- address <A.B.C.D> <A.B.C.D/M>
no ip pim rp-address <A.B.C.D> [<A.B.C.D/M>|<all>]

Function: Configures a static RP globally or for a multicast address range. The **no ip pim rp-address <A.B.C.D> [<A.B.C.D/M>|<all>]** command cancels the static RP.

Parameters: <A.B.C.D> is the RP address.

<A.B.C.D/M> is the group range served by the RP.

<all> indicates all ranges.

Default: No static RP is configured.

Command Mode: Global Mode.

Usage Guidelines: Configures static RP information for PIM-SM globally or for a multicast address range. Note: When the RP is computed, the BSR-learned RP is used first; the static RP is used only if no BSR RP is available.

Example: Configure 10.1.1.1 as the static RP for group range 238.0.0.0/8.

```
Switch (config)# ip pim rp-address 10.1.1.1 238.0.0.0/8
Switch (config)#
```

6.3.29 ip pim rp-candidate

Command: ip pim rp-candidate {vlan < vlan-id > | <ifname>} [<A.B.C.D/M>]
[<priority>]
no ip pim rp-candiate

Function: Configures the switch as a candidate RP so that it competes with other candidate RPs to become the RP. The **no ip pim rp-candidate** command cancels the candidate RP.

Parameters: <vlan-id> is the VLAN ID.

<ifname> is the interface name.

<A.B.C.D/M> is the group prefix and mask length.

<priority> is the RP selection priority, ranging from 0 to 255. The default is 192; a lower value means a higher priority.

Default: The switch is not a candidate RP.

Command Mode: Global Mode.

Usage Guidelines: Configures candidate RP information for PIM-SM so that the switch competes with other candidate RPs to become the RP. The switch is a candidate RP only when this command is configured.

Example: Configure VLAN 1 as the interface that sends candidate RP advertisements.

```
Switch (config)# ip pim rp-candidate vlan1 100
```

6.3.30 ip pim rp-register-kat

Command: ip pim rp-register-kat <vaule>
no ip pim rp-register-kat

Function: Configures the keepalive timer (KAT) of (S,G) entries on the RP, in seconds. The **no ip pim rp-register-kat** command restores the default.

Parameters: <vaule> is the timer value, ranging from 1 to 65535 seconds.

Default: 185 seconds.

Command Mode: Global Mode.

Usage Guidelines: Configures the RP keepalive time. During this time, an (S,G) entry on the RP is not deleted even if no REGISTER packets are received. If no new REGISTER packet is received before the time expires, the entry ages out.

Example: Set the KAT of (S,G) entries on the RP to 180 seconds.

```
Switch (config)#ip pim rp-register- kat 180
Switch (config)#
```

6.3.31 ip pim scope-border

Command: ip pim scope-border [<1-99 >|<acl_name>]
no ip pim scope-border

Function: Configures or deletes a PIM administrative scope border.

Parameters: <1-99>: The number of the ACL for the administrative scope border.

<acl_name>: The name of the ACL for the administrative scope border.

Default: No administrative scope border is configured. If no ACL is specified, the default administrative scope border is used.

Command Mode: Interface Mode.

Usage Guidelines: Configures the administrative scope border and its ACL for PIM. Multicast traffic is not forwarded across the scope border.

Example:

```
Switch(Config-if-Vlan2)#ip pim scope-border 3
```

6.3.32 ip pim sparse-mode

Command: ip pim sparse-mode [passive]
no ip pim sparse-mode [passive]

Function: Enables PIM-SM on the interface. The **no ip pim sparse-mode [passive]** command disables PIM-SM.

Parameters: passive: Disables PIM-SM packet processing on the interface (PIM-SM receives no packets) and enables only IGMP (IGMP packets are received and sent).

Default: PIM-SM is not enabled.

Command Mode: Interface Mode.

Usage Guidelines: Enables PIM-SM on the interface.

Example: Enable PIM-SM on interface VLAN 1.

```
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ip pim sparse-mode
Switch(Config-if-Vlan1)#
```

6.3.33 show ip pim bsr-router

Command: show ip pim bsr-router

Function: Displays the BSR address.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays the BSR information maintained by PIM.

Example:

```
Switch#show ip pim bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 10.1.4.3 (?)
  Uptime:      00:06:07, BSR Priority: 0, Hash mask length: 10
  Next bootstrap message in 00:00:00
  Role: Candidate BSR
  State: Elected BSR
Next Cand_RP_advertisement in 00:00:58
  RP: 10.1.4.3(Vlan1)
```

Output	Description
BSR address	BSR address
Priority	BSR priority
Hash mask length	BSR hash mask length
State	Current state of this candidate BSR; "Elected BSR" indicates the elected BSR.

6.3.34 show ip pim interface

Command: show ip pim interface

Function: Displays PIM interface information.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Global Mode.

Usage Guidelines: Displays PIM interface information.

Example:

```
testS2(config)#show ip pim interface
Address          Interface VIFindex Ver/   Nbr    DR    DR
                                    Mode  Count  Prior
10.1.4.3         Vlan1     0        v2/S   1      1     10.1.4.3
10.1.7.1         Vlan2     2        v2/S   0      1     10.1.7.1
```

Output	Description
Address	Interface address
Interface	Interface name
VIF index	Interface index
Ver/Mode	PIM version and mode. The version is usually v2; S indicates sparse mode and D indicates dense mode.
Nbr Count	Number of neighbors on the interface
DR Prior	DR priority
DR	DR address of the interface

6.3.35 show ip pim mroute sparse-mode

Command: show ip pim mroute sparse-mode [group <A.B.C.D>] [source <A.B.C.D>]

Function: Displays the PIM-SM multicast routing table.

Parameters: group <A.B.C.D>: Displays entries for this multicast group address.

source <A.B.C.D>: Displays entries for this source.

Default: None.

Command Mode: Admin Mode and Global Mode.

Usage Guidelines: Displays the multicast routing entries maintained by PIM-SM.

Example:

```
Switch #show ip pim mroute sparse-mode
IP Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
(*, 239.192.1.10)
RP: 10.1.6.1
RPF nbr: 10.1.4.10
RPF idx: Vlan1
Upstream State: JOINED
 Local     ..l.............................
 Joined    ..............................
 Asserted  ..............................
 Outgoing  ..o............................
```

Output	Description
Entries	Number of entries of each type
RP	RP address of the shared tree
RPF nbr	Upstream neighbor toward the RP or the source
RPF idx	Interface of the RPF neighbor
Upstream State	Upstream state: Joined (joined the tree; expects to receive data from upstream) or Not Joined (left the tree; does not expect data from upstream). For (S,G,rpt) entries, the states RPT Not Joined, Pruned, and Not

	Pruned are also available.
Local	Local join interfaces: interfaces that received IGMP joins
Joined	PIM join interfaces: interfaces that received Join/Prune messages
Asserted	Assert state
Outgoing	Interfaces to which multicast data is finally sent; in this example, the egress interface index is 2. Use **show ip pim interface** to view interface information.

6.3.36 show ip pim neighbor

Command: `show ip pim neighbor`

Function: Displays PIM neighbors.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Global Mode.

Usage Guidelines: Displays the multicast router neighbors maintained by PIM.

Example:

```
Switch (config)#show ip pim neighbor
Neighbor          Interface          Uptime/Expires    Ver   DR
Address                                                    Priority/Mode
10.1.6.1          Vlan1              00:00:10/00:01:35 v2    1 /
10.1.6.2          Vlan1              00:00:13/00:01:32 v2    1 /
10.1.4.2          Vlan3              00:00:18/00:01:30 v2    1 /
10.1.4.3          Vlan3              00:00:17/00:01:29 v2    1 /
```

Output	Description
Neighbor Address	Neighbor address
Interface	Interface connected to the neighbor
Uptime/Expires	Uptime and expiration time
Ver	PIM version, usually v2
DR Priority/Mode	DR priority carried in Hello messages from the neighbor, and whether the neighbor is the DR of the interface

6.3.37 show ip pim nexthop

Command: `show ip pim nexthop`

Function: Displays the next-hop routers buffered by PIM from the unicast routing table.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Global Mode.

Usage Guidelines: Displays the next-hop router information buffered by PIM.

Example:

```
Switch(config)#show ip pim nexthop
Flags: N = New, R = RP, S = Source, U = Unreachable
Destination     Type  Nexthop  Nexthop      Nexthop  Nexthop Metric Pref
Refcnt
                      Num      Addr         Ifindex   Name
____
```

```
192.168.1.1     N...    1       0.0.0.0         2006              0     0
1
192.168.1.9     ..S.    1       0.0.0.0         2006              0     0
1
```

Output	Description
Destination	Destination of the next-hop entry
Type	N: Newly created next hop; RP and source direction not yet determined. R: RP direction. S: Source direction. U: Unreachable.
Nexthop Num	Number of next hops
Nexthop Addr	Next-hop address
Nexthop Ifindex	Next-hop interface index
Nexthop Name	Next-hop interface name
Metric	Metric to the next hop
Pref	Route preference
Refcnt	Reference count

6.3.38 show ip pim rp-hash

Command: `show ip pim rp-hash <A.B.C.D>`

Function: Displays the RP for the specified group address.

Parameters: <A.B.C.D>: The group address.

Default: None.

Command Mode: Admin Mode and Global Mode.

Usage Guidelines: Displays the RP address corresponding to the specified group address.

Example:

```
Switch (Config-if-Vlan1)#show ip pim rp-hash 239.192.1.10
    RP: 10.1.6.1
Info source: 10.1.6.1, via bootstrap
```

Output	Description
RP	RP of the queried group
Info source	Source of the bootstrap information

6.3.39 show ip pim rp mapping

Command: `show ip pim rp mapping`

Function: Displays group-to-RP mappings and RPs.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Global Mode.

Usage Guidelines: Displays the current RPs and group-to-RP mappings.

Example:

```
Switch (Config-if-Vlan1)#show ip pim rp mapping
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4
  RP: 10.1.6.1
    Info source: 10.1.6.1, via bootstrap, priority 6
         Uptime: 00:11:04
```

Output	Description
Group(s)	Group address range served by the RP
Info source	Source of the bootstrap messages

Priority	Priority in the bootstrap messages

6.4 MSDP

6.4.1 cache-sa-holdtime

Command: `cache-sa-holdtime <150-3600>`
`no cache-sa-holdtime`

Function: Configures the maximum hold time of SA entries in the MSDP cache.

Parameters: <150-3600>: The hold time in seconds, ranging from 150 to 3600.

Command Mode: MSDP Mode.

Default: 150 seconds.

Usage Guidelines: Configures the aging time of (S,G) entries in the MSDP cache as required.

Example:

```
Switch(config)#router msdp
Switch(router-msdp)#cache-sa-holdtime 350
```

6.4.2 cache-sa-maximum

Command: `cache-sa-maximum <sa-limit>`
`no cache-sa-maximum`

Function: Configures the maximum number of SA entries cached, globally or for the specified MSDP peer.

Parameters: <sa-limit>: The maximum number of cached SA entries, ranging from 1 to 75000.

Command Mode: MSDP Mode and MSDP Peer Mode.

Default: 20000.

Usage Guidelines: Use this command to limit the number of SA messages cached on the router to prevent denial-of-service (DoS) attacks. The limit can be configured in MSDP Configuration Mode or in MSDP Peer Configuration Mode. The configuration does not take effect if the configured value is less than the current number of cached SA messages, or if the global value is less than the value configured for a peer.

Example:

```
Switch(config)#router msdp
Switch(router-msdp)#cache-sa-maximum50000
Switch(router-msdp)#peer 20.1.1.1
Switch(router-msdp-peer)# cache-sa-maximum 22000
```

6.4.3 cache-sa-state

Command: `cache-sa-state`
`no cache-sa-state`

Function: Configures the SA cache state of the router.

Parameters: None.

Command Mode: MSDP Mode and MSDP Peer Mode.

Default: Enabled.

Usage Guidelines: Configures the SA cache state. When it is enabled, new group members can obtain information about all active sources from the SA cache and join the corresponding source trees without waiting for new SA messages. The SA cache should be enabled on all MSDP speakers.

The **no** form of this command disables the SA cache. Note: This command and the **sa-request** command are mutually exclusive.

Example:

```
Switch(config)#router msdp
Switch(router-msdp)#no cache-sa-state
```

6.4.4 clear msdp peer

Command: clear msdp peer {peer-address| *}

Function: Tears down the TCP connection with the specified MSDP peer and clears the statistics of the peer.

Parameters: peer-address: The IP address of the peer.

*****: Tears down the connections with all peers.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: If a peer address is specified, the TCP connection to that MSDP peer is torn down and all statistics for the peer are cleared. If * is specified, all MSDP connections and the related peer statistics are cleared.

Example:

```
Switch#clear msdp peer *
```

6.4.5 clear msdp sa-cache

Command: clear msdp sa-cache {group A.B.C.D|* }

Function: Clears Source Active information from the MSDP cache: either the entries for all sources of the specified group, or all entries.

Parameters: group A.B.C.D: The IP address of the multicast group whose (S,G) entries are cleared from the cache.

*****: Clears all entries in the cache.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: If a group is specified, the non-local SA entries of that group are removed from the MSDP cache. If * is specified, all non-local SA entries in the MSDP cache are removed.

Example:

```
Switch#clear msdp sa-cache group 224.1.1.1
```

6.4.6 clear msdp statistics

Command: clear msdp statistics {peer-address| *}

Function: Clears MSDP statistics without resetting the MSDP peer session.

Parameters: peer-address: The IP address of the peer.

*****: Clears the statistics of all peers.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example:

```
Switch#clear msdp statistics *
```

6.4.7 connect-source

Command: `connect-source <interface-type <interface-number>`
`no connect-source <interface-type> <interface-number>`

Function: Configures the interface whose address is used to set up connections with MSDP peers.

Parameters: <interface-type> <interface-number>: The interface type and number.

Command Mode: MSDP Mode and MSDP Peer Mode.

Default: No interface is specified.

Usage Guidelines: The router uses the IP address of this interface to set up connections with MSDP peers. Note: The connect-source address must match the peer address configured on the remote peer; otherwise, the TCP connection cannot be established. The configuration in MSDP Peer Configuration Mode overrides that in MSDP Configuration Mode. The **no** form cancels the configuration and re-establishes all MSDP connections that use this interface.

Example:

```
Switch(config)#router msdp
Switch(router-msdp)#connect-source vlan 2
Switch(router-msdp)#peer 20.1.1.1
Switch(router-msdp-peer)#connect-source loopback 10
```

6.4.8 debug msdp all

Command: `debug msdp all`
`no debug msdp all`

Function: Enables all MSDP debugging. The **no** form of this command disables all MSDP debugging.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: Enables all MSDP debugging, which displays MSDP peer packets sent and received (packet), keepalive messages sent and received (keepalive), events (event), interaction with the NSM (nsm), timers (timer), protocol state (fsm), and filter policies (filter).

Example:

```
Switch#debug msdp all
```

6.4.9 debug msdp events

Command: `debug msdp events`
`no debug msdp events`

Function: Enables or disables MSDP event debugging.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: With this debugging enabled, MSDP protocol events can be monitored.

Example:

```
Switch#debug msdp events
```

6.4.10 debug msdp filter

Command: **`debug msdp filter`**
`no debug msdp filter`

Function: Enables or disables debugging of MSDP filter policy information.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: With this debugging enabled, filtering of MSDP messages sent and received can be monitored.

Example:

```
Switch#debug msdp filter
```

6.4.11 debug msdp fsm

Command: **`debug msdp fsm`**
`no debug msdp fsm`

Function: Enables or disables MSDP state machine (FSM) debugging.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: With this debugging enabled, state machine information of MSDP peers is displayed.

Example:

```
Switch#debug msdp fsm
```

6.4.12 debug msdp keepalive

Command: **`debug msdp keepalive`**
`no debug msdp keepalive`

Function: Enables or disables debugging of MSDP keepalive messages.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: With this debugging enabled, MSDP keepalive messages sent and received can be monitored.

Example:

```
Switch#debug msdp keepalive
```

6.4.13 debug msdp nsm

Command: **`debug msdp nsm`**
`no debug msdp nsm`

Function: Enables or disables MSDP NSM debugging.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: With this debugging enabled, the interaction between MSDP and the NSM module can be monitored.

Example:

```
Switch#debug msdp nsm
```

6.4.14 debug msdp packet

Command: **`debug msdp packet {send | receive}`**
`no debug msdp packet {send | receive}`

Function: Enables or disables debugging of MSDP messages sent and received.

Parameters: **send**: Sent messages. **receive**: Received messages.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: With this debugging enabled, MSDP messages sent and received can be monitored.

Example:

```
Switch#debug msdp packet send
```

6.4.15 debug msdp peer

Command: **`debug msdp peer A.B.C.D`**
`no debug msdp peer`

Function: Enables or disables all debugging for the specified MSDP peer.

Parameters: **A.B.C.D**: The IP address of the MSDP peer.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Enables all debugging for the specified MSDP peer as required; debugging information for other MSDP peers is not displayed. The command applies only to the most recently specified MSDP peer.

Example:

```
Switch#debug msdp peer 10.1.1.1
```

6.4.16 debug msdp timer

Command: **`debug msdp timer`**
`no debug msdp timer`

Function: Enables or disables MSDP timer debugging.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Enables timer debugging information as required.

Example:

```
Switch#debug msdp timer
```

6.4.17 default-rpf-peer

Command: `default-rpf-peer <peer-address> [rp-policy <acl-list-number>| <word>]`
`no default-rpf-peer`

Function: Configures a static RPF peer.

Parameters: <peer-address>: The IP address of the MSDP peer.

<acl-list-number>: The ACL number. Only standard ACLs (1 to 99) are supported.

<word>: The standard ACL name.

Command Mode: MSDP Mode.

Default: No static RPF peer is configured. If only one MSDP peer is configured with the **peer** command, that peer is used as the default peer.

Usage Guidelines: To configure more than one static RPF peer, use one of the following two methods:

All peers use the **rp-policy** parameter: multiple RPF peers take effect at the same time, the RPs in SA messages are filtered according to the configured ACL, and only permitted SA messages are accepted.

No peer uses the **rp-policy** parameter: only the first static RPF peer (in configuration order) that is up is active. All SA messages from this peer are accepted, and those from other peers are dropped. If the active peer becomes invalid (for example, its configuration is removed or its connection goes down), the next static RPF peer that is up, in configuration order, becomes the active static RPF peer.

Example:

```
Switch(config)#router msdp
Switch(router-msdp)#default-rpf-peer 10.0.0.1 rp-policy 10
```

6.4.18 description

Command: `description <text>`
`no description`

Function: Adds a description to the specified MSDP peer.

Parameters: <text>: The description, 1 to 80 bytes long.

Command Mode: MSDP Peer Mode.

Default: No description.

Usage Guidelines: Adds a description to the specified MSDP peer to distinguish between MSDP configurations. The **no** form of this command removes the description.

Example:

```
Switch(config)#router msdp
Switch(router-msdp)#peer 20.1.1.1
Switch(router-msdp-peer)# description test-20
```

6.4.19 exit-peer-mode

Command: `exit-peer-mode`

Function: Exits MSDP Peer Configuration Mode and returns to MSDP Configuration Mode.

Command Mode: MSDP Peer Mode.

Default: None.

Usage Guidelines: After configuring an MSDP peer, use the **exit-peer-mode** command to return to MSDP Configuration Mode.

Example: Return from MSDP Peer Configuration Mode to MSDP Configuration Mode.

```
Switch(config-msdp-peer)# exit-peer-mode
```

6.4.20 mesh-group

Command: `mesh-group <name>`
`no mesh-group <name>`

Function: Adds the MSDP peer to the specified mesh group. If the same MSDP peer is added to several mesh groups, only the last mesh group takes effect.

Parameters: <name>: The mesh group name.

Command Mode: MSDP Peer Mode.

Default: The MSDP peer does not belong to any mesh group.

Usage Guidelines: Mesh groups reduce SA message flooding and simplify peer-RPF checks.

Example:

```
Switch(config)#router msdp
Switch(router-msdp)#peer 20.1.1.1
Switch(router-msdp-peer)# mesh-group test-1
```

6.4.21 originating-rp

Command: `originating-rp <interface-type> <interface-number>`
`no originating-rp`

Function: Configures the originating RP address; that is, the IP address of the specified interface is used as the RP address in SA messages.

Parameters: <interface-type> <interface-number>: The interface type and number.

Command Mode: MSDP Mode and MSDP Peer Mode.

Default: The RP address in SA messages is the configured PIM RP address.

Usage Guidelines: Uses the IP address of the specified interface as the RP address in SA messages. If the interface has no IP address or is down, no SA messages are advertised; if multiple RPs are configured on the device, SA messages for the other RPs are not advertised either. Therefore, the interface must be operational when it is configured.

Example:

```
Switch(config)#router msdp
Switch(router-msdp)#originating-rp vlan 20
```

6.4.22 peer

Command: `peer <A.B.C.D>`
`no peer <A.B.C.D>`

Function: Configures an MSDP peer and enters MSDP Peer Configuration Mode. The **no** form of this command deletes the MSDP peer.

Command Mode: MSDP Mode.

Default: There is no MSDP Peer configured by default.

Usage Guidelines: Configures the IP address of the MSDP peer and enters MSDP Peer Configuration Mode. When the command is entered, the router sets up a TCP session with the specified peer. The **no** form of this command deletes the MSDP peer and clears all sessions and statistics for the peer. Note: The peer address must match the interface address used by the peer. If a connect-source is configured, the peer address must be the address of the connect-source interface; otherwise, it must be the egress interface address. If not, the TCP connection cannot be established.

Example: Configure an MSDP peer in MSDP Configuration Mode.

```
Switch(config-msdp)#peer 10.1.1.1
Switch(config-msdp-peer)#
```

6.4.23 redistribute

Command: **`redistribute [list <acl-list-number | acl-name>]`**
`no redistribute`

Function: Configures the redistribution of SA messages.

Parameters: **<acl-list-number>**: The extended ACL number (100 to 199).

<acl-name>: The ACL name.

Command Mode: MSDP Mode.

Default: When SA messages are created, all local active sources are advertised, and (S,G) entries are not restricted.

Usage Guidelines: If an ACL is specified, only (S,G) entries that pass the ACL check are advertised in SA messages. If no ACL is specified, no (S,G) entries are advertised in SA messages.

Example:

```
Switch(config)#router msdp
Switch(router-msdp)#redistribute list 130
```

6.4.24 remote-as

Command: **`remote-as <as-num>`**
`no remote-as <as-num>`

Function: Configures the AS number of the specified MSDP peer.

Parameters: **<as-num>**: The AS number, ranging from 1 to 65535.

Command Mode: MSDP Peer Mode.

Default: The AS number is not initialized (0).

Usage Guidelines: Sets the AS number of the specified peer. The **no** form of this command restores the AS number of the MSDP peer.

Example:

```
Switch(config)#router msdp
Switch(router-msdp)#peer 20.1.1.1
Switch(router-msdp-peer)# remote-as 20
```

6.4.25 router msdp

Command: **`router msdp`**
`no router msdp`

Function: Enables MSDP on the switch and enters MSDP Configuration Mode. The **no** form of this command disables MSDP.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: Enables MSDP in Global Mode. MSDP works only if PIM-SM is also configured.

Example: Enable MSDP in Global Mode.

```
Switch(config)#router msdp
```

6.4.26 sa-filter

Command: sa-filter {in | out} [list <acl-number | acl-name> | rp-list <rp-acl-number | rp-acl-name>]
no sa-filter {in | out} [list <acl-number| acl-name> | rp-list <rp-acl-number | rp-acl-name>]

Function: Configures the filter policy for SA messages received or sent, which controls the source information received and sent.

Parameters: in: Filters SA messages received from the specified MSDP peer.

out: Filters SA messages sent to the specified MSDP peer.

acl-number: The extended ACL number (100 to 199).

acl-name: The extended ACL name.

rp-acl-number: The standard ACL number (1 to 99).

rp-acl-name: The standard ACL name.

If no ACL is specified, all SA messages containing (S,G) entries are filtered.

Command Mode: MSDP Mode and MSDP Peer Mode.

Default: SA messages received or sent are not filtered.

Usage Guidelines: The configuration in MSDP Peer Configuration Mode overrides that in MSDP Configuration Mode. The distribution of SA messages can be controlled with this command or with the **redistribute** command.

Example:

```
Switch(config)#router msdp
Switch(router-msdp)#sa-filter in
Switch(router-msdp)#peer 20.1.1.1
Switch(router-msdp-peer)# sa-filter in list 120
```

6.4.27 sa-request

Command: sa-request
no sa-request

Function: Configures the router to send SA request messages to the specified MSDP peer when it receives a join message for a new group.

Parameters: None.

Command Mode: MSDP Peer Mode.

Default: SA request messages are not sent.

Usage Guidelines: This command makes the switch (RP) send SA request messages to the specified MSDP peer. When there is a new group or member, the switch sends an SA request message to the peer and waits for the peer's response containing its cached local SA messages. After sending the request, the RP receives an SA response message from the peer and learns all active sources of the peer (excluding source information learned through MSDP SA messages). This command and **cache-sa-state** are mutually exclusive: if the SA cache state is configured, **sa-request** cannot be configured, and the switch displays a prompt. This command applies only to RPs.

Example:

```
Switch(config)#router msdp
Switch(router-msdp)#peer 20.1.1.1
Switch(router-msdp-peer)# sa-request
```

6.4.28 sa-request-filter

Command: `sa-request-filter [list <access-list-number | access-list-name>]`
`no sa-request-filter [list <access-list-number | access-list-name>]`

Function: Filters SA request messages from MSDP peers.

Parameters: access-list-number: The ACL number. Only standard ACLs (1 to 99) are supported.

access-list-name: The ACL name.

Command Mode: MSDP Mode.

Default: The router accepts all SA request messages from MSDP peers.

Usage Guidelines: If no list is specified, all SA request messages from MSDP peers are filtered. If a list is specified, SA request messages are filtered by the specified ACL.

Example:

```
Switch(config)#router msdp
Switch(router-msdp)# sa-request-filter list 1
```

6.4.29 show msdp global

Command: `show msdp global`

Function: Displays the MSDP configuration information.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the MSDP configuration, including the protocol and cache states.

Example:

```
Switch#show msdp global
Multicast Source Discovery Protocol (MSDP):
SA-Cached,  Originator: Vlan2,  Connect-Source: Vlan2
MAX External SA Entry: 200000
MAX Peer External SA Entry: 20000
TTL Threshold: 0
SA Entry Hold Time: 350
Filters:
   Redistribute_filter: Not set
   SA-filter:
        [IN]:  RP-list: None,  SG-list: None
        [OUT]: Not Configured
   SA-Request-Filter: Not Configured
Default Peer:
  Not Configured
Mesh Group:
  test-1
```

Field descriptions:

Field	Description
SA-Cached	MSDP SA cache state
Originator	RP interface from which MSDP originates
MAX External SA Entry	Maximum number of entries configured in MSDP Configuration Mode
MAX Peer External SA Entry	Maximum number of entries for each peer
TTL Threshold	TTL threshold
SA Entry Hold Time	Hold time of multicast sources in the MSDP cache
Redistribute_filter	Filter policy for creating SA messages
SA-filter [IN | OUT]	Filter policy for SA messages received or sent

Default Peer	Static RPF peer
Mesh Group	Name and members of the mesh group

6.4.30 show msdp local-sa-cache

Command: `show msdp local-sa-cache`

Function: Displays the local SA cache.

Parameters: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the local SA cache.

Example:

```
Switch#show msdp local-sa-cache
MSDP Flags:
E - set MRIB E flag, L - domain local source is active,
EA - externally active source, PI - PIM is interested in the group,
DE - SAs have been denied.
Cache SA Entry:
Source Address          Group Address       RP Address          TTL
5.5.5.9                   225.0.0.1           11.1.1.1            64
5.5.5.9                   225.0.0.2           11.1.1.1            64
5.5.5.9                   225.0.0.3           11.1.1.1            64
5.5.5.9                   225.0.0.4           11.1.1.1            64
```

6.4.31 show msdp peer

Command: `show msdp peer {A.B.C.D}`

Function: Displays information about the specified MSDP peer.

Parameters: A.B.C.D: The MSDP peer address.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays information about the specified MSDP peer.

Example:

```
Switch#show msdp peer 31.1.1.3
MSDP Peer 31.1.1.3, AS 0,  Description:
Connection status:
    State: Established, Resets: 0,
Connection Source: Not set, Connect address: 31.1.1.1
    Uptime (Downtime): 00h:07m:53s, SA messages received: 16
    TLV messages sent/received:     8/24
    SA messages incoming Rrjected:   0
    SA messages outgoing Rrjected:   0
SA Filtering:
    Input filter Not Configured
    Output filter Not Configured
SA-Requests:
    Input filter Not Configured
    Sending SA-Requests to peer: Disabled
Peer ttl threshold:  0
```

Field descriptions:

Field	Description
MSDP Peer	IP address of the MSDP peer
AS	AS number of the MSDP peer
State	MSDP peer state
Connection source	Interface used for the local TCP connection

Uptime(Downtime)	Uptime or downtime of the MSDP peer
Messages sent/received	Statistics of messages sent to and received from the peer
SA Filtering	Filter policy configured for the peer
SA-Requests	Filter policy configured for SA requests
SAs learned from this peer	Number of SA entries learned from the MSDP peer in the cache
SAs limit	SA limit configured for this MSDP peer

6.4.32 show msdp sa-cache

Command: `show msdp sa-cache {<source-address> [<group-address>] | as-num <sas-number> | peer <peer-address>| rpaddr <rp-address>}`

Function: Displays the external source entries in the MSDP cache.

Parameters: <source-address>: The source address.

<group-address>: The group address.

<sas-number>: The autonomous system number.

<peer-address>: The peer address.

<rp-address>: The RP address.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the external source entries in the MSDP cache.

Example:

```
Switch#show msdp sa-cache 30.30.30.1
MSDP Flags:
E - set MRIB E flag, L - domain local source is active,
EA - externally active source, PI - PIM is interested in the group,
DE - SAs have been denied.
Cache SA Entry:
(S:30.30.30.1, G: 224.1.1.1, RP: 10.1.1.2),  AS: 0,  00h:00m:11s/00h:02m:19s
Learn From Peer:20.1.1.1,  RPF Peer: 10.1.1.10
SA Received: 10    Encapsulated data received: 0
grp flags: None    source flags:  EA, DE
```

Field descriptions:

Field	Description
(S, G, RP)	Active source information (S, G, RP)
AS Num	Autonomous system number
update time	Time the SA entry has been cached
expire time	Time until the SA entry expires
Learn From Peer	Peer from which the entry was learned
RPF Peer	RPF peer of the entry
SA Received	Number of SA messages received that contain the entry
Encapsulated data received	Multicast data encapsulated in SA messages
grp flags	Multicast group flags of the entry
source flags	Multicast source flags of the entry

6.4.33 show msdp sa-cache summary

Command: `show msdp sa-cache summary`

Function: Displays a summary of the MSDP cache.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays a summary of the MSDP cache.

Example:

```
Switch#show msdp sa-cache summary

MSDP Flags:
E - set MRIB E flag, L - domain local source is active,
EA - externally active source, PI - PIM is interested in the group,
DE - SAs have been denied.

Cache SA Entry:
Total number of SA Entries = 1
Total number of Sources = 1
Total number of Groups = 1
Total number of RPs = 1
Originator-RP     SA total    RPF peer
10.1.1.2             1      10.1.1.10

AS-num   SA total
  0        1
```

Field descriptions:

Field	Description
Total number of SA Entries	Total number of SA entries in the cache
Total number of Sources	Total number of distinct multicast sources in the cache
Total number of Groups	Total number of distinct multicast groups in the cache
Total number of RPs	Total number of distinct RPs in the cache
Originator-RP	Originating RP address
SA total	Total number of SA messages received from the RP
RPF peer	RPF peer address of the RP
AS-num	Autonomous system number

6.4.34 show msdp statistics

Command: `show msdp statistics peer [Peer-address]`

Function: Displays message statistics for the specified peer or for all peers.

Parameters: Peer-address: Displays message statistics for the specified peer.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays message statistics for the specified peer or for all peers.

Example:

```
Switch#show msdp sta peer 2.2.2.4

MSDP Peer Statistics :
Peer  2.2.2.4 ,   AS is  0 ,   State is  Inactive
    TLV Rcvd :    76 total
                  39 keepalives,      37 SAs
                   0 SA Requests,     0 SA responses
    TLV Send :    80 total
                  41 keepalives,      39 SAs
                   0 SA Requests,     0 SA responses
    SA  msgs :    37 received,    39 sent
```

Field descriptions:

Field	Description

Peer	MSDP peer address
AS	Autonomous system number
State	MSDP peer state
TLV Rcvd	TLV types and counts received from the peer
TLV Send	TLV types and counts sent to the peer
SA msgs	Statistics of SA messages received from and sent to the peer

6.4.35 show msdp summary

Command: `show msdp summary`

Function: Displays an MSDP summary.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays an MSDP summary.

Example:

```
Switch#show msdp summary

Maximum External SA's Global : 20000
MSDP Peer Status Summary
Peer Address AS State   Uptime/   Reset  Peer   Active   Cfg.Max        TLV
                      Downtime  Count  Name   SA    Cnt Ext.SAs    recv/sent
 2.2.2.4    0  Established  THU JAN 01 00:00:00   10          0
121/100
```

Field descriptions:

Field	Description
Peer Address	IP address of the MSDP peer
AS	AS number of the MSDP peer
State	MSDP peer state
Uptime/Downtime	Uptime or downtime of the MSDP peer
Reset Count	Number of times the MSDP peer has been reset
Peer Name	Description of the MSDP peer
Active SA	Number of active SA entries
TLV sent/received	Statistics of TLV messages sent to and received from the peer

6.4.36 shutdown

Command: `shutdown`
`no shutdown`

Function: Disables the specified MSDP peer.

Parameters: None.

Command Mode: MSDP Peer Mode.

Default: Enabled.

Usage Guidelines: When an MSDP peer is configured with several commands, it may be necessary for the commands to take effect together rather than one at a time. Use **shutdown** to disable the peer before configuring it and **no shutdown** afterward so that the configuration takes effect at once. The **shutdown** command tears down all TCP sessions with the specified MSDP peer and clears its statistics.

Example:

```
Switch(config)#router msdp
Switch(router-msdp)#peer 20.1.1.1
Switch(router-msdp-peer)# shutdown
```

6.4.37 ttl-threshold

Command: **`ttl-threshold <ttl>`**
`no ttl-threshold`

Function: Configures the minimum TTL of multicast data encapsulated in SA messages.

Parameters: <ttl>: The minimum TTL, ranging from 1 to 255.

Command Mode: MSDP Mode.

Default: 0 (TTL values are not filtered).

Usage Guidelines: The TTL value controls the redistribution of multicast data. Multicast data is encapsulated and advertised in SA messages only if its TTL is not less than the TTL threshold.

Example:

```
Switch(config)#router msdp
Switch(router-msdp)#ttl-threshold 10
```

6.5 ANYCAST RP

6.5.1 debug pim anycast-rp

Command: **`debug pim anycast-rp`**
`no debug pim anycast-rp`

Function: Enables ANYCAST RP debugging. The **no** form of this command disables this debugging.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: Enables ANYCAST RP debugging on the router, which displays information about the PIM register packets handled by the switch (packet) and about events (event).

Example:

```
Switch#debug pim anycast-rp
```

6.5.2 ip pim anycast-rp

Command: **`ip pim anycast-rp`**
`no ip pim anycast-rp`

Function: Enables ANYCAST RP on the switch. The **no** form of this command disables ANYCAST RP.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: Enables ANYCAST RP globally. For ANYCAST RP to work, the self RP address and the set of other RP addresses must also be configured.

Example: Enable ANYCAST RP in Global Mode.

```
Switch(config)#ip pim anycast-rp
```

6.5.3 ip pim anycast-rp

Command: `ip pim anycast-rp <anycast-rp-addr> <other-rp-addr>`
`no ip pim anycast-rp <anycast-rp-addr> <other-rp-addr>`

Function: Configures the ANYCAST RP address (ARA) and the unicast addresses of the other RPs with which this router (as an RP) communicates. The **no** form of this command removes the unicast address of the other RP for the configured RP address.

Parameters: <anycast-rp-addr>: The RP address. The candidate interface with this address need not exist yet.

<other-rp-addr>: The unicast address of another RP with which this router (as an RP) communicates.

Command Mode: Global Mode.

Default: None.

Usage Guidelines:

1. The anycast-rp-addr configured on this router (as an RP) is the RP address shared by multiple RPs in the network; it corresponds to the address of the RP candidate interface (or loopback interface). The candidate interface with this address need not exist when the address is configured.

2. Configure the other-rp-address of each other RP with which this router (as an RP) communicates. This unicast address identifies the other RP and is used to communicate with the local router.

3. When this router (as an RP) receives a unicast register message from a DR, it forwards the message to the other RPs in the network to notify all RPs of the source (S,G) state. When forwarding, the router changes the destination address of the register message to the other-rp-address.

4. Multiple other-rp-addresses can be configured for one anycast-rp-addr. When a register message is received from a DR, it is forwarded to each of these other RPs in turn.

Example: Configure an other-rp-address in Global Mode.

```
Switch(config)#ip pim anycast-rp 1.1.1.1 192.168.3.2
```

6.5.4 ip pim anycast-rp self-rp-address

Command: `ip pim anycast-rp self-rp-address <self-rp-addr>`
`no ip pim anycast-rp self-rp-address`

Function: Configures the self-rp-address of this router (as an RP). This address uniquely identifies this router among the RPs and is used to communicate with the other RPs. The **no** form of this command removes the configured address.

Parameters: <self-rp-addr>: The unicast address used by this router (as an RP) to communicate with other RPs.

Command Mode: Global Mode.

Default: No self-rp-address is configured.

Usage Guidelines:

1. When this router (as an RP) receives a unicast register message from a DR, it forwards the message to all other RPs in the network to notify them of the source (S,G) state. When forwarding, the router changes the source address of the register message to the self-rp-address.

2. When this router (as an RP) receives a unicast register message from another RP, that is, a register message whose destination is the self-rp-address of this router, it creates the (S,G) state and sends back a register-stop message whose destination address is the source address of the register message.

3. The self-rp-address must be the address of a Layer 3 interface on this router, but it can be configured before the interface exists.

Example: Configure the self-rp-address of this router in Global Mode.

```
Switch(config)#ip pim anycast-rp self-rp-address 1.1.1.1
```

6.5.5 ip pim rp-candidate

Command: ip pim rp-candidate {vlan<vlan-id> |loopback<index> |<ifname>} [<A.B.C.D>] [<priority>]
no ip pim rp-candidate

Function: Extends the PIM-SM command so that a loopback interface can be configured as an RP candidate interface. The **no** form of this command cancels the RP candidate.

Parameters: <index>: The loopback interface index, ranging from 1 to 1024.

<vlan-id>: The VLAN ID.

<ifname>: The interface name.

<A.B.C.D>: The group prefix and mask.

<priority>: The RP election priority, ranging from 0 to 255. The default is 192; a smaller value means a higher priority.

Command Mode: Global Mode.

Default: No RP candidate interface is configured.

Usage Guidelines: To support ANYCAST RP, a loopback interface can be configured as the RP candidate interface. The RP candidate interface must be unique, and its address must be advertised by the routing protocol so that PIM routers can find the nearest RP. Use **no ip pim rp-candidate** to cancel the RP candidate.

Example: Configure interface Loopback1 as the RP candidate interface in Global Mode.

```
Switch(config)#ip pim rp-candidate loopback1
```

6.5.6 show debugging pim

Command: show debugging pim

Function: Displays the PIM debugging status.

Command Mode: Admin Mode.

Usage Guidelines: Displays the current state of the ANYCAST RP debugging.

Example:

```
Switch(config)#show debugging pim
Debugging status:
  PIM anycast-rp debugging is on
```

6.5.7 show ip pim anycast-rp first-hop

Command: show ip pim anycast-rp first-hop

Function: Displays ANYCAST RP multicast route entries created on the first-hop RP.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays ANYCAST RP state information, including the multicast route (MRT) entries created on the first-hop RP that are currently maintained by the protocol.

Example:

```
Switch(config)#show ip pim anycast-rp first-hop
IP Multicast Routing Table
(*,G) Entries: 0
```

```
(S,G) Entries: 1
(E,G) Entries: 0
INCLUDE (192.168.1.136, 224.1.1.1)
 Local     .l.............................
```

Output	Description
Entries	Number of entries of each type
INCLUDE	Multicast route entries created on the first-hop RP

6.5.8 show ip pim anycast-rp non-first-hop

Command: `show ip pim anycast-rp non-first-hop`

Function: Displays ANYCAST RP multicast route entries created on a non-first-hop RP.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays ANYCAST RP state information, including the multicast route (MRT) entries created on a non-first-hop RP that are currently maintained by the protocol, that is, entries created after the first-hop RP forwards a received register message to this RP.

Example:

```
Switch(config)#show ip pim anycast-rp non-first-hop
IP Multicast Routing Table
(*,G) Entries: 0
(S,G) Entries: 1
(E,G) Entries: 0
INCLUDE (192.168.10.120, 225.1.1.1)
 Local     .l.............................
```

Output	Description
Entries	Number of entries of each type
INCLUDE	Multicast route entries created after the first-hop RP forwards register messages to this RP

6.5.9 show ip pim anycast-rp status

Command: `show ip pim anycast-rp status`

Function: Displays the ANYCAST RP configuration.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the ANYCAST RP configuration: whether ANYCAST RP is enabled globally, whether the self-rp-address is configured, and the currently configured ANYCAST RP sets.

Example:

```
Switch(config)#show ip pim anycast-rp status
Anycast RP status:
anycast-rp:Enabled!
self-rp-address:192.168.3.2
anycast-rp address: 1.1.1.1
    other rp unicast rp address: 192.168.2.1
other rp unicast rp address: 192.168.5.1
anycast-rp address: 192.168.1.4
    other rp unicast rp address: 192.168.2.1
-------------------------------
```

Output	Description
anycast-rp:	Whether ANYCAST RP is enabled globally
self-rp-address:	Configured self-rp-address
anycast-rp address:	Configured anycast-rp-address
other rp unicast rp address:	Other RP addresses configured for the preceding anycast-

	rp-address
other rp unicast rp address:	Other RP addresses configured for the preceding anycast-rp-address
anycast-rp address:	Configured anycast-rp-address
other rp unicast rp address:	Other RP addresses configured for the preceding anycast-rp-address

6.6 PIM-SSM

6.6.1 ip multicast ssm

Command: `ip multicast ssm {default|range <access-list-number >}`
`no ip multicast ssm`

Function: Configures the PIM-SSM multicast group range. The **no ip multicast ssm** command deletes the configured PIM-SSM group range.

Parameters: default: Uses the default PIM-SSM group range, 232.0.0.0/8.

<access-list-number> is the access list to apply, ranging from 1 to 99.

Default: No PIM-SSM group range is configured.

Command Mode: Global Mode.

Usage Guidelines:

1. PIM-SSM is available only when this command is configured.

2. Before configuring this command, make sure that PIM multicast routing is enabled. This command cannot be used with DVMRP.

3. Only access lists created with the **access-list** command can be used; access lists created with **ip access-list** cannot.

4. You can configure this command before the corresponding ACL, and you can delete the ACL while it is bound. Once bound, the binding can be released only with the **no ip multicast ssm** command.

5. If SSM is required, configure this command on the relevant edge routers: the local switch running IGMP (required) and the multicast source DR or RP (at least one of them). Intermediate switches need only PIM-SM enabled.

Example: Enable PIM-SSM on the switch with the group range specified by access list 23.

```
Switch (config)#ip multicast ssm range 23
```

6.7 DVMRP

6.7.1 debug dvmrp

Command: **debug dvmrp [events[neighbor|packet|igmp|kernel|prune [detail] | route]| nsm|mfc|mib|timer [probe[probe-timer|neighbor-expiry-timer]|**
prune[prune-expiry-timer|prune-retx-timer|graft-retx-timer]|route[report-timer|flash-upd-timer|route-expiry-timer|route-holdown-timer|route-burst-timer]]|packet[[probe [in|out] | report [in|out | prune [in|out] graft [in|out] | graft-ack [in|out] |in|out]]|all]
no debug dvmrp [events[neighbor|packet|igmp|kernel|prune [detail] |route]|nsm|mfc|mib|timer[probe[probe-timer|neighbor-expiry-timer]|prune[prune-expiry-timer|prune-retx-timer|graft-retx-timer]|route[report-timer|flash-upd-timer|route-expiry-timer|route-holdown-timer|route-burst-timer]]|packet[[probe [in|out] | report [in|out | prune [in|out] graft [in|out] | graft-ack [in|out] |in|out]]|all]

Function: Displays DVMRP debugging messages. The **no debug dvmrp** command disables this debugging.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Displays messages related to DVMRP operation.

6.7.2 ip dvmrp enable

Command: **ip dvmrp enable**
no ip dvmrp

Function: Enables DVMRP on the interface. The **no ip dvmrp** command disables DVMRP.

Parameters: None.

Default: DVMRP is disabled.

Command Mode: Interface Mode.

Usage Guidelines: The interface processes DVMRP protocol messages only when DVMRP is enabled on it.

Example: Enable DVMRP on interface VLAN 1.

```
Switch (config)#interface vlan 1
Switch(Config-If-vlan1)#ip dvmrp enable
```

6.7.3 ip dvmrp metric

Command: **ip dvmrp metric <metric_val>**
no ip dvmrp metric

Function: Configures the metric of DVMRP report messages on the interface. The **no ip dvmrp metric** command restores the default.

Parameters: **<metric_val>** is the metric, ranging from 1 to 31.

Default: 1

Command Mode: Interface Mode.

Usage Guidelines: The routing information in DVMRP report messages consists of source networks and their metrics. After the interface metric is configured, the configured metric is added to the metric of each route received on the interface to give the new metric of the route. The metric is also used for poison reverse, which establishes upstream-downstream relationships: if the metric of a route on the switch is not less than 32, the route is unreachable. If the switch determines that it is downstream for a route, it sends a report message containing the route to the upstream router, adding 32 to the original metric to indicate that it is downstream.

Example: Set the metric of DVMRP report messages on the interface to 2.

```
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ip dvmrp metric 2
```

6.7.4 ip dvmrp multicast-routing

Command: ip dvmrp multicast-routing
no ip dvmrp multicast-routing

Function: Enables DVMRP globally. The **no ip dvmrp multicast-routing** command disables DVMRP globally.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: DVMRP can be enabled on interfaces only after this command is executed globally.

Example:

```
Switch (config)#ip dvmrp multicast-routing
```

6.7.5 ip dvmrp output-report-delay

Command: ip dvmrp output-report-delay <delay_val> [<burst_size>]
no ip dvmrp output-report-delay

Function: Configures the delay between DVMRP report messages sent on the interface and the number of messages sent each time. The **no ip dvmrp output-report-delay** command restores the defaults.

Parameters: <delay_val> is the delay between periodically sent DVMRP report messages, ranging from 1 to 5 seconds.

<burst_size> is the number of messages sent each time, ranging from 1 to 65535.

Default: The delay is 1 second, and two messages are sent each time.

Command Mode: Interface Mode.

Usage Guidelines: An appropriate delay prevents message bursts.

Example:

```
Switch (Config-If-vlan1)#ip dvmrp output-report-delay 1 1024
```

6.7.6 ip dvmrp reject-non-pruners

Command: ip dvmrp reject-non-pruners
no ip dvmrp reject-non-pruners

Function: Rejects neighbor relationships on the interface with DVMRP routers that do not support pruning or grafting. The **no ip dvmrp reject-non-pruners** command allows such neighbor relationships again.

Parameters: None.

Default: Not configured; neighbor relationships with non-pruning routers are allowed.

Command Mode: Interface Mode.

Usage Guidelines: Determines whether neighbor relationships are established with DVMRP routers that do not support pruning or grafting.

Example:

```
Switch (Config-If-vlan1)#ip dvmrp reject-non-pruners
```

6.7.7 ip dvmrp tunnel

Command: `ip dvmrp tunnel <index> <src-ip> <dst-ip>`
`no ip dvmrp tunnel {<index> |<src-ip> <dst-ip>}`

Function: Configures a DVMRP tunnel. The **no ip dvmrp tunnel {<index> | <src-ip> <dst-ip>}** command deletes the DVMRP tunnel.

Parameters: <src-ip> is the source IP address.

<dst-ip> is the IP address of the remote neighbor.

<index> is the tunnel index, ranging from 1 to 65535.

Default: No DVMRP tunnel is configured.

Command Mode: Global Mode.

Usage Guidelines: Because not all switches support multicast, DVMRP supports tunneled multicast communication. A tunnel carries multicast packets between DVMRP switches that are separated by switches that do not support multicast routing; it acts as a virtual network between the two DVMRP switches. Multicast packets are encapsulated in unicast packets and sent directly to the next multicast-capable switch. DVMRP treats tunnel interfaces the same as physical interfaces. After **no ip dvmrp multicast-routing** is configured, all tunnel configurations are deleted.

Example:

```
Switch(config)#ip dvmrp tunnel 1 12.1.1.1 24.1.1.1
```

6.7.8 show ip dvmrp

Command: `show ip dvmrp`

Function: Displays DVMRP protocol information.

Parameters: None.

Default: None.

Command Mode: All Modes.

Usage Guidelines: Displays overall DVMRP statistics.

Example:

```
Switch#show ip dvmrp
DVMRP Daemon Start Time: MON JAN 01 00:00:09 2001
DVMRP Daemon Uptime: 17:37:03
DVMRP Number of Route Entries: 2
DVMRP Number of Reachable Route Entries: 2
DVMRP Number of Prune Entries: 1
DVMRP Route Report Timer: Running
DVMRP Route Report Timer Last Update: 00:00:56
DVMRP Route Report Timer Next Update: 00:00:04
DVMRP Flash Route Update Timer: Not Running
```

6.7.9 show ip dvmrp interface

Command: show ip dvmrp interface [<ifname>]

Function: Displays DVMRP interfaces.

Parameters: <ifname> is the interface name; information for the specified interface is displayed.

Default: None.

Command Mode: All Modes.

Example:

```
Switch #show ip dvmrp neighbor vlan 4
Address           Interface   Vif   Ver.   Nbr  Type    Remote
                            Index        Cnt          Address
13.1.1.3          Vlan1       1    v3.ff  0    BCAST   N/A
10.1.35.3         Vlan2       0    v3.ff  0    BCAST   N/ASwitch #
```

Output	Description
Address	Interface address
Interface	Physical interface name of the interface
Vif Index	Virtual interface index
Ver	DVMRP version supported by the interface
Nbr Cnt	Number of neighbors
Type	Interface type
Remote Address	Remote address

6.7.10 show ip dvmrp neighbor

Command: show ip dvmrp neighbor [{<ifname> <A.B.C.D> [detail]}| { <ifname>[detail]}|detail]

Function: Displays DVMRP neighbors.

Parameters: <ifname> is the interface name; neighbor information for the specified interface is displayed.

Default: None.

Command Mode: All Modes.

Example: Display DVMRP neighbors.

```
Switch #show ip dvmrp neighbor
Neighbor          Interface   Uptime/Expires          Maj  Min  Cap
Address                                           Ver  Ver   Flg
10.1.35.5         Vlan2       00:00:16/00:00:29       3    255  2e
```

Output	Description
Neighbor Address	Neighbor address
Interface	Interface on which the neighbor was detected
Uptime/Expires	Neighbor uptime and expiration time
Maj Ver	Major version
Min Ver	Minor version
Cap Flg	Capability flags

6.7.11 show ip dvmrp prune

Command: show ip dvmrp prune [{group <A.B.C.D> [detail]}|{source <A.B.C.D/M> group <A.B.C.D> [detail]}|{source <A.B.C.D/M> [detail] }|detail]

Function: Displays DVMRP multicast forwarding entries.

Parameters: group <A.B.C.D>: The group address. **source <A.B.C.D/M>**: The source address and mask length. **detail**: Displays detailed information.

Default: None.

Command Mode: All Modes.

Usage Guidelines: Displays DVMRP multicast forwarding entries, that is, the multicast forwarding table calculated by DVMRP.

Example:

```
Switch#show ip dvmrp prune
Flags: P=Pruned,H=Host,D=Holddown,N=NegMFC,I=Init
Source           Mask Group           State  FCR Exptime  Prune/Graft
Address          Len  Address                 Cnt          ReXmit-Time
13.1.1.0          24   239.0.0.1        ..... 1   01:59:56      Off
```

Output	Description
Source Address	Source address
Mask Len	Mask length
Group Address	Group address
State	Entry state
FCR Exptime	FCR expiration time
Prune/Graft ReXmit-Time	Prune expiration time / graft retransmission time

6.7.12 show ip dvmrp route

Command: show ip dvmrp route [{<A.B.C.D/M>[detail]}|{nexthop <A.B.C.D>[detail]}|{best-match <A.B.C.D> [detail]}|detail]

Function: Displays the DVMRP routing table.

Parameters: <A.B.C.D/M>: The network address and mask length. **nexthop <A.B.C.D>**: The next-hop address. **best-match <A.B.C.D>**: Displays the best-matching route. **detail**: Displays detailed information.

Default: None.

Command Mode: All Modes.

Usage Guidelines: Displays DVMRP routing table entries. DVMRP maintains its own unicast routing table for RPF checks.

Example: Display DVMRP routes.

```
Switch #show ip dvmrp route
Flags: N = New, D = DirectlyConnected, H = Holddown
Network          Flags Nexthop   Nexthop            Metric  Uptime
Exptime
                       Xface     Neighbor
10.1.35.0/24       .D.   Vlan2     Directly Connected      1     00:11:16
00:00:00
13.1.1.0/24        .D.   Vlan1     Directly Connected      1      00:10:22
00:00:00
```

Output	Description
Network	Destination network segment or address and mask
Flags	Route state flags
Nexthop Xface	Next-hop interface
Nexthop Neighbor	Next-hop neighbor
Metric	Route metric
Uptime	Route uptime
Exptime	Route expiration time

6.8 Multicast Source and Destination Control

6.8.1 access-list (Multicast Destination Control)

Command: access-list <6000-7999> {{{add | delete} profile-id WORD} | {{deny|permit} (ip) {{<source/M> }|{host-source <source-host-ip> (range <2-65535>|)}|any-source} {{<destination/M>}|{host-destination <destination-host-ip> (range <2-255>|)}|any-destination}}

no access-list <6000-7999> {deny|permit} ip {{<source> <source-wildcard>}|{host-source <source-host-ip> {range <2-65535>|}}|any-source} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip> {range <2-255>|}}|any-destination}

Function: Configures a multicast destination control access list. The **no access-list <6000-7999>** command deletes the access list.

Parameters: <6000-7999>: The destination control access list number.

{add | delete} profile-id WORD: Adds or deletes the profile.

{deny|permit}: Deny or permit.

<source/M>: The multicast source address and mask length.

<source-host-ip>: The multicast source host address.

<2-65535>: The range of multicast source hosts.

<destination/M>: The multicast destination address and mask length.

<destination-host-ip>: The multicast destination host address.

<2-255>: The range of multicast destination hosts.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: Multicast destination control ACLs use the dedicated ACL numbers 6000 to 7999; this command configures them. A multicast destination control ACL specifies only the source IP address and the controlled destination (group) IP address. Configuration is similar to other ACLs: an address range is specified by mask length, or a single host or all addresses can be specified. Note that "all addresses" for the group address means 224.0.0.0/4, not 0.0.0.0/0 as in other access lists. Adding or deleting a profile ID changes the multicast destination control ACL.

Example:

```
Switch(config)#access-list 6000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0
0.0.0.255
Switch(config)#access-list 6000 add profile-id 1
Switch(config)#
```

6.8.2 access-list (Multicast Source Control)

Command: access-list <5000-5099> {deny|permit} ip {{<source> <source-wildcard>}|{host <source-host-ip>}|any-source} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip>}|any-destination}

no access-list <5000-5099> {deny|permit} ip {{<source> <source-wildcard>}|{host <source-host-ip>}|any} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip>}|any-destination}

Function: Configures a multicast source control access list. The **no access-list <5000-5099>** command deletes the access list.

Parameters: <5000-5099>: The source control access list number.

{deny|permit}: Deny or permit.

<source>: The multicast source address.

<source-wildcard>: The wildcard of the multicast source address.

<source-host-ip>: The multicast source host address.

<destination>: The multicast destination address.

<destination-wildcard>: The wildcard of the multicast destination address.

<destination-host-ip>: The multicast destination host address.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: Multicast source control ACLs use the dedicated ACL numbers 5000 to 5099; this command configures them. A multicast source control ACL specifies only the source IP address and the controlled destination (group) IP address. Configuration is similar to other ACLs: an address range is specified by wildcard, or a single host or all addresses can be specified. Note that "all addresses" for the group address means 224.0.0.0/4, not 0.0.0.0/0 as in other access lists.

Example:

```
Switch(config)#access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0
0.0.0.255
```

6.8.3 ip multicast destination-control

Command: ip multicast destination-control

no ip multicast destination-control

Function: Enables multicast destination control access lists. The **no** form of this command disables them.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Use this command together with the **ip multicast destination-control access-group** commands to apply multicast destination control access lists.

Example:

```
Switch (config)#ip multicast destination-control
Switch (config)#
```

6.8.4 ip multicast destination-control access-group (sip)

Command: ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>
no ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>

Function: Applies a multicast destination control access list to the specified network segment. The **no ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>** command deletes this configuration.

Parameters: <IPADDRESS/M>: The IP address and mask length.

<6000-7999>: The destination control access list number.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: This command takes effect only when multicast destination control is enabled globally. After this command is configured, when IGMP snooping or IGMP adds members to a multicast group, IGMP reports sent from the specified network segment are checked against the configured access list: if they match a permit rule, the interface is added; otherwise, it is not. If the corresponding group or source already appears in **show ip igmp groups detail** before this command is executed, run **clear ip igmp groups** in Admin Mode to clear those groups.

Example:

```
Switch(config)#ip multicast destination-control 10.1.1.0/24 access-group 6000
```

6.8.5 ip multicast destination-control access-group (vmac)

Command: ip multicast destination-control <1-4094> <macaddr >access-group <6000-7999>
no ip multicast destination-control <1-4094> <macaddr >access-group <6000-7999>

Function: Applies a multicast destination control access list to the specified VLAN and MAC address. The **no ip multicast destination-control <1-4094> <macaddr> access-group <6000-7999>** command deletes this configuration.

Parameters: <1-4094>: The VLAN ID.

<macaddr>: The source MAC address of the IGMP report, in the format xx-xx-xx-xx-xx-xx.

<6000-7999>: The destination control access list number.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: This command takes effect only when multicast destination control is enabled globally. After this command is configured, when IGMP snooping adds members to a multicast group, IGMP reports from the specified source MAC address are checked against the configured access list: if they match a permit rule, the interface is added; otherwise, it is not.

Example:

```
Switch(config)#ip multicast destination-control 1 00-01-03-05-07-09 access-group 6000
```

6.8.6 ip multicast policy

Command: ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos <priority>
no ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos

Function: Configures a multicast policy. The **no ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos** command deletes it.

Parameters:

<IPADDRESS/M> <IPADDRESS/M>: The multicast source address and mask length, and the destination address and mask length.

<priority>: The priority, ranging from 0 to 7.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: This command sets the priority of multicast packets in the specified range to the specified value, and sets the TOS to the same value. Note: The priority of packets sent untagged is not changed.

Example:

```
Switch(config)#ip multicast policy 10.1.1.0/24 225.1.1.0/24 cos 7
```

6.8.7 ip multicast source-control

Command: ip multicast source-control
no ip multicast source-control

Function: Enables multicast source control globally. The **no ip multicast source-control** command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Source control access lists can be applied to interfaces only when multicast source control is enabled globally, and global multicast source control can be disabled only after the source control access lists are removed from all interfaces. After this command is configured, multicast data received on any interface that does not match a source control entry is discarded; only multicast data that matches a permit rule is received and forwarded.

Example:

```
Switch(config)#ip multicast source-control
```

6.8.8 ip multicast source-control access-group

Command: ip multicast source-control access-group <5000-5099>
no ip multicast source-control access-group <5000-5099>

Function: Applies a multicast source control access list to the interface. The **no ip multicast source-control access-group <5000-5099>** command deletes the configuration.

Parameters: <5000-5099>: The source control access list number.

Default: None.

Command Mode: Interface Mode.

Usage Guidelines: This command can be configured only when multicast source control is enabled globally. Multicast data received on the interface is then matched against the configured access list: if it matches a permit rule, it is received and forwarded; otherwise, it is discarded.

Example:

```
Switch (config)#interface ethernet1/0/4
Switch (Config-If-Ethernet1/0/4)#ip multicast source-control access-group
5000
Switch (Config-If-Ethernet1/0/4)#
```

6.8.9 multicast destination-control

Command: `multicast destination-control`
`no multicast destination-control`

Function: Enables IPv4 and IPv6 multicast destination control globally; both take effect at the same time. The **no** form of this command disables IPv4 and IPv6 multicast destination control globally.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Other destination control configurations take effect only after multicast destination control is enabled globally. Destination control access lists can be applied to ports, VLAN-MAC, and source IP addresses. After this command is configured, IGMP snooping and IGMP check IGMP reports against these rules before adding ports.

Example:

```
switch(config)# multicast destination-control
```

6.8.10 profile-id (Multicast Destination Control Rule List)

Command: `profile-id <1-50> {deny|permit} {{<source/M> }|{host-source <source-host-ip> (range <2-65535>|)}|any-source} {{<destination/M>}|{host-destination <destination-host-ip> (range <2-255>|)}|any-destination}`
`no profile-id <1-50>`

Function: Configures a destination control profile rule. The **no** form of this command deletes the profile rule.

Parameters: <1-50>: The profile ID.

{deny|permit}: Deny or permit.

<source/M>: The multicast source address and mask length.

<source-host-ip>: The multicast source host address.

<2-65535>: The range of multicast source hosts.

<destination/M>: The multicast destination address and mask length.

<destination-host-ip>: The multicast destination host address.

<2-255>: The range of multicast destination hosts.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: Multicast destination control profiles use profile IDs 1 to 50. This command configures a profile, which is then added to an ACL. A profile specifies only the source IP address and the controlled destination (group) IP address. Configuration is similar to ACLs: an address range is specified by mask length, or a single host or all addresses can be specified. Note that "all addresses" for the group address means 224.0.0.0/4, not 0.0.0.0/0 as in other access lists.

Example:

```
Switch (config)# profile-id 1 deny ip any-source host-destination 224.1.1.2
```

6.8.11 show ip multicast destination-control

Command: show ip multicast destination-control [detail]
show ip multicast destination-control interface <Interfacename> [detail]
show ip multicast destination-control host-address <ipaddress> [detail]
show ip multicast destination-control <vlan-id> <mac-address> [detail]

Function: Displays the multicast destination control configuration.

Parameters: detail: Displays detailed information.

<Interfacename>: The interface or aggregated interface name, such as Ethernet1/0/1 or port-channel 1.

Default: None.

Command Mode: Admin Mode and Global Mode.

Usage Guidelines: Displays the configured multicast destination control rules; with **detail**, the applied access lists are also displayed.

Example:

```
Switch (config)#show ip multicast destination-control
ip multicast destination-control is enabled
ip multicast destination-control 11.0.0.0/8 access-group 6003
ip multicast destination-control 1 00-03-05-07-09-11 access-group 6001
multicast destination-control access-group 6000 used on interface
Ethernet1/0/13
switch(config)#
```

6.8.12 show ip multicast destination-control access-list

Command: show ip multicast destination-control access-list
show ip multicast destination-control access-list <6000-7999>

Function: Displays the configured multicast destination control access lists.

Parameters: <6000-7999>: The access list number.

Default: None.

Command Mode: Admin Mode and Global Mode.

Usage Guidelines: Displays the configured multicast destination control access lists.

Example:

```
Switch# sh ip multicast destination-control acc
access-list 6000 deny ip any any-destination
access-list 6000 deny ip any host-destination 224.1.1.1
access-list 6000 deny ip host 2.1.1.1 any-destination
access-list 6001 deny ip host 2.1.1.1 225.0.0.0 0.255.255.255
access-list 6002 permit ip host 2.1.1.1 225.0.0.0 0.255.255.255
access-list 6003 permit ip 2.1.1.0 0.0.0.255 225.0.0.0 0.255.255.255
```

6.8.13 show ip multicast destination-control filter-profile-list

Command: show ip multicast destination-control filter-profile-list
show ip multicast destination-control filter-profile-list <1-50>

Function: Displays the configured destination control profile rules.

Parameters: <1-50>: The profile ID.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the configured destination control profile rules.

Example:

```
Switch#show ip multicast destination-control filter-profile-list
profile-id 1 deny ip any-source any-destination
profile-id 2 deny ip any-source host-destination 224.1.1.1
profile-id 3 deny ip host-source 2.1.1.1 any-destination
```

6.8.14 show ip multicast policy

Command: show ip multicast policy

Function: Displays the configured multicast policies.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Global Mode.

Usage Guidelines: Displays the configured multicast policies.

Example:

```
Switch#show ip multicast policy
ip multicast-policy 10.1.1.0/24 225.0.0.0/8 cos 5
```

6.8.15 show ip multicast source-control

Command: show ip multicast source-control [detail]
show ip multicast source-control interface <Interfacename> [detail]

Function: Displays the multicast source control configuration.

Parameters: detail: Displays detailed information.

<Interfacename>: The interface name, such as Ethernet1/0/1.

Default: None.

Command Mode: Admin Mode and Global Mode.

Usage Guidelines: Displays the configured multicast source control rules; with **detail**, the applied access lists are also displayed.

Example:

```
Switch#show ip multicast source-control detail
ip multicast source-control is enabled
Interface Ethernet1/0/13 use multicast source control access-list 5000
access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255
access-list 5000 deny ip 10.1.1.0 0.0.0.255 233.0.0.0 0.255.255.255
```

6.8.16 show ip multicast source-control access-list

Command: show ip multicast source-control access-list
show ip multicast source-control access-list <5000-5099>

Function: Displays the configured multicast source control access lists.

Parameters: <5000-5099>: The access list number.

Default: None.

Command Mode: Admin Mode and Global Mode.

Usage Guidelines: Displays the configured multicast source control access lists.

Example:

```
Switch#sh ip multicast source-control access-list
access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255
access-list 5000 deny ip 10.1.1.0 0.0.0.255 233.0.0.0 0.255.255.255
```

6.9 IGMP

6.9.1 clear ip igmp group

Command: `clear ip igmp group [A.B.C.D | IFNAME]`

Function: Deletes the group records of the specified group or interface.

Parameters: A.B.C.D: The group address. **IFNAME**: The interface.

Command Mode: Admin Mode.

Usage Guidelines: Use the **show** command to verify that the group records were deleted.

Example: Delete all groups.

```
Switch#clear ip igmp group
```

Related Commands: **show ip igmp groups**

6.9.2 debug igmp event

Command: `debug igmp event`
`no debug igmp event`

Function: Enables IGMP event debugging. The **no debug igmp event** command disables this debugging.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Enable this debugging to view IGMP event information.

Example:

```
Switch# debug igmp event
igmp event debug is on
Switch# 01:04:30:56: IGMP: Group 224.1.1.1 on interface vlan1 timed out
```

6.9.3 debug igmp snooping all/packet/event/timer/mfc/authentication/ha

Command: `debug igmp snooping all/packet/event/timer/mfc/authentication/ha`
`no debug igmp snooping all/packet/event/timer/mfc/authentication/ha`

Function: Enables IGMP snooping debugging on the switch. The **no debug igmp snooping** command disables this debugging.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: Enables IGMP snooping debugging on the switch. **packet** displays IGMP packets, **event** displays events, **timer** displays timer messages, **mfc** displays messages about hardware entries written, **authentication** displays authentication messages, **ha** displays high availability messages, and **all** displays all debugging messages.

6.9.4 ip igmp access-group

Command: `ip igmp access-group {<acl_num | acl_name>}`
`no ip igmp access-group`

Function: Configures IGMP group filtering on the interface. The **no ip igmp access-group** command cancels the filter.

Parameters: <acl_num | acl_name> is the number or name of the access list. **acl_num** ranges from 1 to 99.

Default: No filter.

Command Mode: Interface Mode.

Usage Guidelines: Configures group filtering on the interface to permit or deny joining of specific groups.

Example: Configure interface VLAN 1 to permit group 224.1.1.1 and deny group 224.1.1.2.

```
Switch (config)#access-list 1 permit 224.1.1.1 0.0.0.0
Switch (config)#access-list 1 deny 224.1.1.2 0.0.0.0
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ip igmp access-group 1
```

6.9.5 ip igmp immediate-leave

Command: `ip igmp immediate-leave group-list {<number>|<name>}`
`no ip igmp immediate-leave`

Function: Configures IGMP immediate-leave mode: when a host sends a leave message for a group, the router does not send a group-specific query but immediately concludes that the group has no members on the subnet. The **no ip igmp immediate-leave** command cancels immediate-leave mode.

Parameters: <number> is the access list number, ranging from 1 to 99.

<name> is the access list name.

Default: No immediate-leave groups are configured on the interface.

Command Mode: Interface Mode.

Usage Guidelines: Use this command only when there is a single host on the subnet.

Example: Configure immediate-leave mode for the groups in access list 1.

```
Switch (Config-if-Vlan1)#ip igmp immediate-leave group-list 1
Switch (Config-if-Vlan1)#
```

6.9.6 ip igmp join-group

Command: `ip igmp join-group <A.B.C.D >`
`no ip igmp join-group <A.B.C.D >`

Function: Configures the interface to join an IGMP group. The **no ip igmp join-group** command cancels the join.

Parameters: <A.B.C.D> is the group address.

Default: Not joined.

Command Mode: Interface Mode.

Usage Guidelines: This command makes the switch act as a host that joins the group. For example, if the interface joins group 224.1.1.1, the switch sends an IGMP membership report for 224.1.1.1 whenever it receives an IGMP query from another switch. Note the difference between this command and **ip igmp static-group**.

Example: Join group 224.1.1.1 on interface VLAN 1.

```
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ip igmp join-group 224.1.1.1
```

6.9.7 ip igmp last-member-query-interval

Command: ip igmp last-member-query-interval <interval>
no ip igmp last-member-query-interval

Function: Configures the interval at which group-specific queries are sent on the interface. The **no ip igmp last-member-query-interval** command cancels the configured value and restores the default.

Parameters: <interval> is the group-specific query interval, ranging from 1000 to 25500 ms. The value must be a multiple of 1000 ms; any other value is rounded to a multiple of 1000 ms.

Default: 1000 ms.

Command Mode: Interface Mode.

Example: Set the IGMP last member query interval of interface VLAN 1 to 2000 ms.

```
Switch (config)#int vlan 1
Switch (Config-if-vlan1)#ip igmp last-member-query-interval 2000
```

6.9.8 ip igmp limit

Command: ip igmp limit <state-count>
no ip igmp limit

Function: Configures the maximum number of IGMP states on the interface. The **no ip igmp limit** command cancels the configured value and restores the default.

Parameters: <state-count> is the maximum number of IGMP states kept on the interface, ranging from 1 to 65000.

Default: 0 (no limit).

Command Mode: Interface Mode.

Usage Guidelines: After the maximum is configured, the interface keeps no more than state-count group and source states. When the limit is reached, new membership reports are not processed. If IGMP group states were saved before this command is configured, all of them are deleted, and an IGMP general query is sent immediately to collect membership reports for up to state-count groups. Static groups and static sources are not counted toward the limit.

Example: Set the IGMP limit of interface VLAN 1 to 4000.

```
Switch (config)#int vlan 1
Switch (Config-if-vlan1)#ip igmp limit 4000
```

6.9.9 ip igmp query-interval

Command: ip igmp query-interval <time_val>
no ip igmp query-interval

Function: Configures the interval at which IGMP queries are sent periodically. The **no ip igmp query-interval** command restores the default.

Parameters: <time_val> is the interval at which IGMP queries are sent periodically, ranging from 1 to 65535 seconds.

Default: 125 seconds.

Command Mode: Interface Mode.

Usage Guidelines: When a multicast protocol is enabled on an interface, the interface sends IGMP queries periodically. Use this command to configure the query interval.

Example: Set the interval for periodically sending IGMP queries to 10 seconds.

```
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ip igmp query-interval 10
```

6.9.10 ip igmp query-max-response-time

Command: ip igmp query-max-response-time <time_val>
no ip igmp query- max-response-time

Function: Configures the IGMP maximum query response time of the interface. The **no ip igmp query-max-response-time** command restores the default.

Parameters: <time_val> is the IGMP maximum query response time, ranging from 1 to 25 seconds.

Default: 10 seconds.

Command Mode: Interface Mode.

Usage Guidelines: When a host receives a query message, it starts a timer for each multicast group it belongs to, with a value selected randomly between 0 and the maximum response time; when the timer expires, the host sends a membership report for the group. A suitable maximum response time lets hosts respond quickly to queries, so that the router can learn the state of group members quickly.

Example: Set the IGMP maximum query response time to 20 seconds.

```
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ip igmp query- max-response-time 20
```

6.9.11 ip igmp query-timeout

Command: ip igmp query-timeout <time_val>
no ip igmp query-timeout

Function: Configures the IGMP querier timeout of the interface. The **no ip igmp query-timeout** command restores the default.

Parameters: <time_val> is the IGMP querier timeout, ranging from 60 to 300 seconds.

Default: 255 seconds.

Command Mode: Interface Mode.

Usage Guidelines: When several switches running IGMP are on a shared network, one switch is elected as the querier, and the other switches start a timer to monitor the querier. If they receive no query message from the querier before the timeout expires, a new querier is elected.

Example: Set the IGMP querier timeout of the interface to 100 seconds.

```
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ip igmp query-timeout 100
```

6.9.12 ip igmp robust-variable

Command: ip igmp robust-variable <value>
no ip igmp robust-variable

Function: Configures the robustness variable. The **no ip igmp robust-variable** command restores the default.

Parameters: <value>: The robustness variable, ranging from 2 to 7.

Command Mode: Interface Mode.

Default: 2.

Usage Guidelines: Using the default value is recommended.

Example:

```
Switch (config-if-vlan1)#ip igmp robust-variable 3
```

6.9.13 ip igmp static-group

Command: ip igmp static-group <A.B.C.D > [source <A.B.C.D >]
no ip igmp static -group <A.B.C.D > [source <A.B.C.D >]

Function: Configures the interface to join an IGMP static group. The **no ip igmp static-group** command cancels the join.

Parameters: <A.B.C.D> is the group address.

source <A.B.C.D> specifies the SSM source address.

Default: No static group is joined.

Command Mode: Interface Mode.

Usage Guidelines: When an interface joins a static group, it receives multicast packets for the group whether or not it has an actual receiver. For example, if the interface joins static group 224.1.1.1, it always receives multicast packets for group 224.1.1.1, whether or not there is a receiver on the interface. Note the difference between this command and **ip igmp join-group**.

Example: Configure static group 224.1.1.1 on interface VLAN 1.

```
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ip igmp static-group 224.1.1.1
```

6.9.14 ip igmp version

Command: ip igmp version <version>
no ip igmp version

Function: Configures the IGMP version of the interface. The **no ip igmp version** command restores the default.

Parameters: <version> is the IGMP version. Versions 1, 2, and 3 are supported.

Default: Version 2.

Command Mode: Interface Mode.

Usage Guidelines: This command mainly provides compatibility between versions. Versions 1 and 2 cannot interoperate, so the same IGMP version must be configured on the same network. If routers on the connected subnet that have not been upgraded to IGMPv3 need to take part in collecting membership information for the subnet, configure the interface to the corresponding version.

Example: Set the IGMP version of the interface to 3.

```
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ip igmp version 3
```

6.9.15 show ip igmp groups

Command: show ip igmp groups [<A.B.C.D>] [detail]

Function: Displays IGMP group information.

Parameters: <A.B.C.D> is the group address; information about the specified group is displayed. **detail** displays detailed group information.

Default: None.

Command Mode: Admin Mode.

Example:

```
Switch (config)#show ip igmp groups
IGMP Connected Group Membership (2 group(s) joined)
Group Address    Interface            Uptime    Expires   Last Reporter
226.0.0.1        Vlan1                00:00:01  00:04:19  1.1.1.1
239.255.255.250  Vlan1                00:00:10  00:04:10  10.1.1.1
Switch#
```

Output	Description
Group Address	Multicast group IP address
Interface	Interface to which the multicast group belongs
Uptime	Multicast group uptime
Expires	Multicast group expiration time
Last Reporter	Last host that reported membership in the multicast group

```
Switch (config)#show ip igmp groups 234.1.1.1 detail
IGMP Connect Group Membership (2 group(s) joined)
Flags: SG - Static Group, SS - Static Source, SSM - SSM Group, V1 - V1 Host
Pres
ent, V2 - V2 Host Present
Interface:       Vlan1
Group:           234.1.1.1
Flags:
Uptime:          00:00:19
Group Mode:  INCLUDE
Last Reporter:   10.1.1.1
Exptime:     stopped
Source list: (2 members  S - Static)
Source Address   Uptime    v3 Exp    Fwd  Flags
 1.1.1.1          00:00:19  00:04:01   Yes
 2.2.2.2          00:00:19  00:04:01   Yes
```

Output	Description
Group	Multicast group IP address
Interface	Interface to which the multicast group belongs
Flags	Group flags
Uptime	Multicast group uptime
Group Mode	Group mode, INCLUDE or EXCLUDE. This applies to IGMPv3 groups; IGMPv1 and IGMPv2 groups are treated as EXCLUDE mode.
Exptime	Multicast group expiration time
Last Reporter	Last host that reported membership in the multicast group
Source Address	Source address of this group
V3 Exp	Source expiration time
Fwd	Whether data from the source is forwarded
Flags	Source flags

6.9.16 show ip igmp interface

Command: `show ip igmp interface {vlan <vlan_id>|<ifname>}`

Function: Displays IGMP information for the interface.

Parameters: vlan <vlan_id> | <ifname> is the interface; IGMP information for the specified interface is displayed.

Default: None.

Command Mode: Admin Mode.

Example: Display IGMP information for interface VLAN 1.

```
Switch (config)#show ip igmp interface Vlan1
Interface Vlan1(2005)
 Index 2005
 Internet address is 10.1.1.2
```

```
IGMP querier
IGMP current version is V3, 2 group(s) joined
IGMP query interval is 125 seconds
IGMP querier timeout is 255 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1000 ms
Group Membership interval is 260 seconds
IGMP is enabled on interface
```

6.10 IGMP Snooping

6.10.1 clear ip igmp snooping vlan

Command: `clear ip igmp snooping vlan <1-4094> groups [A.B.C.D]`

Function: Deletes the group records of the specified VLAN.

Parameters: <1-4094>: The VLAN ID. **A.B.C.D**: The group address.

Command Mode: Admin Mode.

Usage Guidelines: Use the **show** command to verify that the group records were deleted.

Example: Delete all groups in VLAN 1.

```
Switch#clear ip igmp snooping vlan 1 groups
```

Related Commands: **show ip igmp snooping vlan <1-4094>**

6.10.2 clear ip igmp snooping vlan <1-4094> mrouter-port

Command: `clear ip igmp snooping vlan <1-4094> mrouter-port [ethernet IFNAME | IFNAME]`

Function: Deletes the mrouter ports of the specified VLAN.

Parameters: <1-4094>: The VLAN ID. **ethernet**: Ethernet port name. **IFNAME**: The port name.

Command Mode: Admin Mode.

Usage Guidelines: Use the **show** command to verify that the mrouter ports of the VLAN were deleted.

Example: Delete the mrouter ports in VLAN 1.

```
Switch# clear ip igmp snooping vlan 1 mrouter-port
```

Related Commands: **show ip igmp snooping mrouter-port**

6.10.3 debug igmp snooping all/packet/event/timer/mfc

Command: `debug igmp snooping all/packet/event/timer/mfc`
`no debug igmp snooping all/packet/event/timer/mfc`

Function: Enables IGMP snooping debugging on the switch. The **no debug igmp snooping** command disables this debugging.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: Enables IGMP snooping debugging on the switch. **packet** displays IGMP packets, **event** displays events, **timer** displays timer messages, **mfc** displays messages about hardware entries written, and **all** displays all debugging messages.

6.10.4 ip igmp snooping

Command: `ip igmp snooping`
`no ip igmp snooping`

Function: Enables IGMP snooping. The **no ip igmp snooping** command disables this function.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: Enables IGMP snooping globally, which allows IGMP snooping to be configured on each VLAN. The **no ip igmp snooping** command disables this function.

Example: Enable IGMP Snooping.

```
Switch(config)#ip igmp snooping
```

6.10.5 ip igmp snooping proxy

Command: `ip igmp snooping proxy`
`no ip igmp snooping proxy`

Function: Enables the IGMP snooping proxy function. The **no** form of this command disables the function.

Parameters: None.

Command Mode: Global Mode.

Default: Enabled.

Example:

```
Switch(config)#no ip igmp snooping proxy
```

6.10.6 ip igmp snooping vlan

Command: `ip igmp snooping vlan <vlan-id>`
`no ip igmp snooping vlan <vlan-id>`

Function: Enables IGMP snooping on the specified VLAN. The **no ip igmp snooping vlan <vlan-id>** command disables IGMP snooping on the VLAN.

Parameters: <vlan-id> is the VLAN ID.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: Global IGMP snooping must be enabled before IGMP snooping can be configured on a VLAN. Use **no ip igmp snooping vlan <vlan-id>** to disable IGMP snooping on the VLAN.

Example: Enable IGMP snooping on VLAN 100 in Global Mode.

```
Switch(config)#ip igmp snooping vlan 100
```

6.10.7 ip igmp snooping vlan immediate-leave

Command: `ip igmp snooping vlan <vlan-id> immediate-leave`
`no ip igmp snooping vlan <vlan-id> immediate-leave`

Function: Enables IGMP snooping immediate leave on the specified VLAN. The **no ip igmp snooping vlan <vlan-id> immediate-leave** command disables it.

Parameters: <vlan-id> is the VLAN ID.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: Enables IGMP snooping immediate leave on the specified VLAN; the **no** form of this command disables it.

Example: Enable IGMP snooping immediate leave on VLAN 100.

```
Switch(config)#ip igmp snooping vlan 100 immediate-leave
```

6.10.8 ip igmp snooping vlan <id> immediately-leave mac-based

Command: **`ip igmp snooping vlan <id> immediately-leave mac-based`**
`no ip igmp snooping vlan <id> immediately-leave mac-based`

Function: When the switch running IGMP snooping receives a leave packet, deletes the existing IGMP snooping entry based on the source MAC address of the leave packet. The entry is deleted only if the receiving port, source MAC address, and multicast group of the leave packet match the port, host MAC address, and multicast group of the entry. If this command is not configured, the entry is deleted based on the port and multicast group of the leave packet.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: For this command to take effect, immediate leave must also be configured on the same VLAN. Entries are then processed based on the host MAC address on the port.

Example: Delete entries based on the host MAC address on the port.

```
switch(config)#ip igmp snooping vlan 12 immediately-leave
switch(config)#ip igmp snooping vlan 12 immediately-leave mac-based
```

6.10.9 ip igmp snooping vlan l2-general-querier

Command: **`ip igmp snooping vlan < vlan-id > l2-general-querier`**
`no ip igmp snooping vlan < vlan-id > l2-general-querier`

Function: Configures the VLAN as a Layer 2 general querier.

Parameters: <vlan-id>: The VLAN ID, ranging from 1 to 4094.

Command Mode: Global Mode.

Default: The VLAN is not an IGMP snooping Layer 2 general querier.

Usage Guidelines: Configuring one Layer 2 general querier on a segment is recommended. If IGMP snooping is not enabled on the VLAN, this command enables it; disabling the Layer 2 general querier does not disable IGMP snooping. This command mainly sends general queries periodically to help the switches on this segment learn mrouter ports.

Note: IGMP snooping learns mrouter ports in three ways:

1. The port receives IGMP query messages.
2. The port receives multicast protocol packets (DVMRP and PIM are supported).
3. The port is configured statically.

6.10.10 ip igmp snooping vlan l2-general-querier-source

Command: **`ip igmp snooping vlan <vlanid> L2-general-query-source <A.B.C.D>`**
`no ip igmp snooping vlan <vlanid> L2-general-query-source`

Function: Configures the source address of IGMP snooping queries.

Parameters: <vlanid>: The VLAN ID, ranging from 1 to 4094. **<A.B.C.D>** is the source address of the queries.

Command Mode: Global Mode.

Default: 0.0.0.0

Usage Guidelines: Windows 2000/XP clients do not support queries with source address 0.0.0.0; with that source address, the Layer 2 query does not work. The client stops sending reports after sending one, and after a while it can no longer receive multicast data.

Example:

```
Switch(config)#iip igmp snooping vlan 2 L2-general-querier-source 192.168.1.2
```

6.10.11 ip igmp snooping vlan l2-general-querier-version

Command: ip igmp snooping vlan <vlanid> L2-general-query-version <version>

Function: Configures the IGMP version of Layer 2 general queries sent by IGMP snooping.

Parameters: <vlanid> is the VLAN ID, ranging from 1 to 4094. **<version>** is the version number, ranging from 1 to 3.

Command Mode: Global Mode.

Default: Version 3.

Usage Guidelines: When the switch is connected to an IGMPv1 or IGMPv2 environment, a VLAN configured with a Layer 2 query source can send queries only after the version is specified. Use this command to set the version of Layer 2 queries.

Example:

```
Switch(config)#ip igmp snooping vlan 2 l2-general-querier-version 2
```

6.10.12 ip igmp snooping vlan limit

Command: ip igmp snooping vlan <vlan-id> limit {group <g_limit> | source <s_limit>}
no ip igmp snooping vlan <vlan-id> limit

Function: Configures the maximum number of groups in the VLAN and the maximum number of sources in each group. The **no ip igmp snooping vlan <vlan-id> limit** command cancels this configuration.

Parameters: <vlan-id> is the VLAN ID.

<g_limit>: The maximum number of groups joined, ranging from 1 to 65535.

<s_limit>: The maximum number of source entries in each group, including include and exclude sources, ranging from 1 to 65535.

Command Mode: Global Mode.

Default: A maximum of 50 groups, each with up to 40 source entries.

Usage Guidelines: When the number of joined groups reaches the limit, requests to join new groups are rejected to prevent malicious attacks. IGMP snooping must be enabled on the VLAN before this command can be used. The **no** form of this command restores the default rather than removing the limit; for security reasons, the limit cannot be removed. Using the default value is recommended; if Layer 3 IGMP is running, keep this configuration consistent with the IGMP configuration where possible.

Example:

```
Switch(config)#ip igmp snooping vlan 2 limit group 300
```

6.10.13 ip igmp snooping vlan interface (ethernet | port-channel|) IFNAME limit

Command: ip igmp snooping vlan <1-4094> interface (ethernet | port-channel|) IFNAME limit {group <1-65535>| source <1-65535>} strategy (replace | drop)

no ip igmp snooping vlan <1-4094> interface (ethernet | port-channel|) IFNAME limit group source strategy

Function: Configures the maximum number of groups that can be joined and the maximum number of sources in each group on an IGMP snooping port, and the action taken when the limit is reached: replace or drop.

Parameters: <1-4094>: The VLAN ID.

ethernet: Ethernet port.

IFNAME: The interface name.

port-channel: Port aggregation.

group <1-65535>: The maximum number of groups that can be joined.

source <1-65535>: The maximum number of source entries in each group, including include and exclude sources.

replace: Replaces existing group and source information.

drop: Drops the new group and source information.

Command Mode: Global Mode.

Default: No limit.

Usage Guidelines: When the number of groups joined on the port, or the number of sources in a group, exceeds the limit, the configured strategy is applied. With **drop**, the new group and source information is dropped; with **replace**, a dynamic group and source on the port is deleted and replaced with the new group and source information. IGMP snooping must be enabled on the VLAN before this command can be used. The **no** form of this command removes the limit.

Example:

```
Switch(config)#ip igmp snooping vlan 2  interface ethernet 1/0/11 limit
group 300 source 200 strategy replace
Switch(config)#
```

6.10.14 ip igmp snooping vlan mrouter-port interface

Command: ip igmp snooping vlan <vlan-id> mrouter-port interface[<ehternet> | <port-channel>] <ifname>

no ip igmp snooping vlan <vlan-id> mrouter-port interface[<ehternet> | <port-channel>] <ifname>

Function: Configures a static mrouter port for the VLAN. The **no** form of this command cancels this configuration.

Parameters: <vlan-id>: The VLAN ID, ranging from 1 to 4094.

ethernet: Ethernet port.

<ifname>: The interface name.

port-channel: Port aggregation.

Command Mode: Global Mode.

Default: No static mrouter port is configured.

Usage Guidelines: A port that is both a static and a dynamic mrouter port is treated as a static mrouter port. A static mrouter port can be deleted only with the **no** form of the command.

Example:

```
Switch(config)#ip igmp snooping vlan 2 mrouter-port interface ethernet1/0/13
```

6.10.15 ip igmp snooping vlan mrouter-port learnpim

Command: **`ip igmp snooping vlan <vlan-id> mrouter-port learnpim`**
`no ip igmp snooping vlan <vlan-id> mrouter-port learnpim`

Function: Enables the specified VLAN to learn mrouter ports from PIM packets. The **no** form of this command disables the function.

Parameters: <vlan-id>: The VLAN ID, ranging from 1 to 4094.

Command Mode: Global Mode.

Default: Enabled.

Usage Guidelines: When enabled, a port that receives PIM packets is automatically set as an mrouter port.

Example: Disable learning of mrouter ports from PIM packets on VLAN 100.

```
Switch(config)#no ip igmp snooping vlan 100 mrouter-port learnpim
```

6.10.16 ip igmp snooping vlan mrpt

Command: **`ip igmp snooping vlan <vlan-id> mrpt <value>`**
`no ip igmp snooping vlan <vlan-id> mrpt`

Function: Configures the aging time of mrouter ports.

Parameters: <vlan-id>: The VLAN ID, ranging from 1 to 4094.

<value>: The mrouter port aging time, ranging from 1 to 65535 seconds.

Command Mode: Global Mode.

Default: 255 seconds.

Usage Guidelines: This command applies to dynamic mrouter ports, not static mrouter ports. IGMP snooping must be enabled on the VLAN before this command can be used.

Example:

```
Switch(config)#ip igmp snooping vlan 2 mrpt 100
```

6.10.17 ip igmp snooping vlan query-interval

Command: **`ip igmp snooping vlan <vlan-id> query-interval <value>`**
`no ip igmp snooping vlan <vlan-id> query-interval`

Function: Configures the query interval.

Parameters: <vlan-id>: The VLAN ID, ranging from 1 to 4094.

<value>: The query interval, ranging from 1 to 65535 seconds.

Command Mode: Global Mode.

Default: 125 seconds.

Usage Guidelines: Using the default value is recommended. If Layer 3 IGMP is running, keep this configuration consistent with the IGMP configuration where possible.

Example:

```
Switch(config)#ip igmp snooping vlan 2 query-interval 130
```

6.10.18 ip igmp snooping vlan query-mrsp

Command: `ip igmp snooping vlan <vlan-id> query-mrsp <value>`
`no ip igmp snooping vlan <vlan-id> query-mrsp`

Function: Configures the maximum query response time. The **no ip igmp snooping vlan <vlan-id> query-mrsp** command restores the default.

Parameters: <vlan-id>: The VLAN ID, ranging from 1 to 4094.

<value>: The maximum query response time, ranging from 1 to 25 seconds.

Command Mode: Global Mode.

Default: 10 seconds.

Usage Guidelines: Using the default value is recommended. If Layer 3 IGMP is running, keep this configuration consistent with the IGMP configuration where possible.

Example:

```
Switch(config)#ip igmp snooping vlan 2 query-mrsp 18
```

6.10.19 ip igmp snooping vlan query-robustness

Command: `ip igmp snooping vlan <vlan-id> query-robustness <value>`
`no ip igmp snooping vlan <vlan-id> query-robustness`

Function: Configures the query robustness variable. The **no ip igmp snooping vlan <vlan-id> query-robustness** command restores the default.

Parameters: <vlan-id>: The VLAN ID, ranging from 1 to 4094.

<value>: The robustness variable, ranging from 2 to 10.

Command Mode: Global Mode.

Default: 2

Usage Guidelines: Using the default value is recommended. If Layer 3 IGMP is running, keep this configuration consistent with the IGMP configuration where possible.

Example:

```
Switch(config)#ip igmp snooping vlan 2 query- robustness 3
```

6.10.20 ip igmp snooping vlan report source-address

Command: `ip igmp snooping vlan <vlan-id> report source-address <A.B.C.D>`
`no ip igmp snooping vlan <vlan-id> report source-address`

Function: Configures the source address of IGMP reports forwarded by IGMP snooping. The **no ip igmp snooping vlan <vlan-id> report source-address** command restores the default.

Parameters: <vlan-id>: The VLAN ID, ranging from 1 to 4094.

<A.B.C.D>: The IP address; 0.0.0.0 is allowed.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: Using the default configuration is recommended. The source address of IGMP messages forwarded by IGMP snooping can be 0.0.0.0. If the upstream device requires IGMP messages to use the same network address, configure the source address on the same network as the upstream device.

Example:

```
Switch (config)#ip igmp snooping vlan 2 report source-address 10.1.1.1
```

6.10.21 ip igmp snooping vlan specific-query-mrsp

Command: ip igmp snooping vlan <vlan-id> specific-query-mrsp <value>
no ip igmp snooping vlan <vlan-id> specific-query-mrspt

Function: Configures the maximum response time of group-specific or group-and-source-specific queries. The **no** form of this command restores the default.

Parameters: <vlan-id>: The VLAN ID, ranging from 1 to 4094.

<value>: The maximum query response time in seconds, ranging from 1 to 25. The default is 1.

Command Mode: Global Mode.

Default: Enabled.

Usage Guidelines: After IGMP snooping is enabled on the VLAN in Global Mode, use this command to configure the maximum response time of group-specific queries.

Example: Set the specific query maximum response time of VLAN 3 to 2 seconds, and then cancel it.

```
Swith(config)#ip igmp snooping vlan 3 specific-query-mrsp 2
Swith(config)#no ip igmp snooping vlan 3 specific-query-mrspt
```

6.10.22 ip igmp snooping vlan static-group

Command: ip igmp snooping vlan <vlan-id> static-group <A.B.C.D> [source <A.B.C.D>] interface [ethernet | port-channel] <IFNAME>
no ip igmp snooping vlan <vlan-id> static-group <A.B.C.D> [source <A.B.C.D>]interface [ethernet | port-channel] <IFNAME>

Function: Configures a static group on the specified port of the VLAN. The **no** form of this command cancels this configuration.

Parameters: <vlan-id>: The VLAN ID, ranging from 1 to 4094.

A.B.C.D: The group or source address.

ethernet: Ethernet port.

port-channel: Port aggregation.

<IFNAME>: The interface name.

Command Mode: Global Mode.

Default: Not configured.

Usage Guidelines: A group that is both static and dynamic is treated as a static group. A static group can be deleted only with the **no** form of the command.

Example:

```
Switch(config)#ip igmp snooping vlan 1 static-group 224.1.1.1 source
192.168.1.1 interface ethernet 1/0/1
```

6.10.23 ip igmp snooping vlan passthrough-group

Command: ip igmp snooping vlan <vlan-id> passthrough-group <A.B.C.D>
no ip igmp snooping vlan <vlan-id> passthrough-group <A.B.C.D>

Function: Configures a pass-through group. The **no** form of this command restores the default.

Parameters: <vlan-id>: The VLAN ID, ranging from 1 to 4094.

A.B.C.D: The group IP address.

Command Mode: Global Mode.

Default: No pass-through group is configured.

Usage Guidelines: Multicast traffic for a pass-through group is forwarded to all ports in the VLAN.

Example:

```
Switch(config)#ip igmp snooping vlan 1 passthrough-group 224.1.1.1
```

6.10.24 ip igmp snooping vlan not-forward

Command: `ip igmp snooping vlan <vlan-id> not-forward`
`no ip igmp snooping vlan <vlan-id> not-forward`

Function: Prevents multicast traffic from being forwarded to mrouter ports. The **no** form of this command cancels this configuration.

Parameters: <vlan-id>: The VLAN ID, ranging from 1 to 4094.

Command Mode: Global Mode.

Default: Not configured.

Usage Guidelines: After this function is enabled, multicast traffic is no longer forwarded to mrouter ports.

Example:

```
Switch(config)#ip igmp snooping vlan 1 not-forward
```

6.10.25 ip igmp snooping vlan suppression-query-time

Command: `ip igmp snooping vlan <vlan-id> suppression-query-time <value>`
`no ip igmp snooping vlan <vlan-id> suppression-query-time`

Function: Configures the query suppression time. The **no ip igmp snooping vlan <vlan-id> suppression-query-time** command restores the default.

Parameters: <vlan-id>: The VLAN ID, ranging from 1 to 4094.

<value>: The suppression time, ranging from 1 to 65535 seconds.

Command Mode: Global Mode.

Default: 255 seconds.

Usage Guidelines: This command can be configured only on a Layer 2 general querier. The suppression query time is the duration of the suppressed state that the querier enters when it receives a query from a Layer 3 IGMP router on the segment.

Example:

```
Switch(config)#ip igmp snooping vlan 2 suppression-query-time 270
```

6.10.26 show ip igmp snooping

Command: `show ip igmp snooping [vlan <vlan-id>]`

Function: Displays IGMP snooping information.

Parameters: <vlan-id> is the VLAN ID for which IGMP snooping information is displayed.

Command Mode: Admin Mode.

Usage Guidelines: If no VLAN is specified, the command shows whether global IGMP snooping is enabled and which VLANs are configured as Layer 2 general queriers. If a VLAN is specified, detailed IGMP snooping information for that VLAN is displayed.

Example:

Example 1: Display the IGMP snooping summary of the switch.

```
 Switch(config)#show ip igmp snooping
Global igmp snooping status:  Enabled
L3 multicasting:             running
Igmp snooping is turned on for vlan 1(querier)
Igmp snooping is turned on for vlan 2
```

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

Output	Description
Global igmp snooping status	Whether global IGMP snooping is enabled on the switch
L3 multicasting	Whether the Layer 3 multicast protocol of the switch is running
Igmp snooping is turned on for vlan 1(querier)	The VLANs on which IGMP snooping is enabled, and whether each is a Layer 2 general querier

Example 2: Display the IGMP snooping information of VLAN 1.

```
Switch#show ip igmp snooping vlan 1
Igmp snooping information for vlan 1
Igmp snooping L2 general querier                    :Yes(COULD_QUERY)
Igmp snooping query-interval                        :125(s)
Igmp snooping max reponse time                     :10(s)
Igmp snooping robustness                           :2
Igmp snooping mrouter port keep-alive time            :255(s)
Igmp snooping query-suppression time                :255(s)
IGMP Snooping Connect Group Membership
Note:*-All Source, (S)- Include Source, [S]-Exclude Source
Groups          Sources             Ports               Exptime  System Level
238.1.1.1       (192.168.0.1)       Ethernet1/1/8         00:04:14     V2
              (192.168.0.2)       Ethernet1/1/8          00:04:14     V2
Igmp snooping vlan 1 mrouter port
Note:"!"-static mrouter port
!Ethernet1/1/2
```

Output	Description
Igmp snooping L2 general querier	Whether the VLAN is a Layer 2 general querier, and whether the querier state is COULD_QUERY or suppressed
Igmp snooping query-interval	Query interval of the VLAN
Igmp snooping max reponse time	Maximum response time of the VLAN
Igmp snooping robustness	IGMP snooping robustness variable configured on the VLAN
Igmp snooping mrouter port keep-alive time	Aging time of dynamic mrouter ports of the VLAN
Igmp snooping query-suppression time	Suppression timeout of the VLAN when it acts as a Layer 2 general querier
IGMP Snooping Connect Group Membership	Group membership of the VLAN, that is, the mapping between ports and (S,G)
Igmp snooping vlan 1 mrouter port	Mrouter ports of the VLAN, both static and dynamic

6.11 IGMP Proxy

6.11.1 clear ip igmp proxy agggroup

Command: `clear ip igmp proxy agggroup`

Function: Deletes all group records.

Parameters: None.

Command Mode: Admin Mode.

Usage Guidelines: Use the **show** command to verify that the group records were deleted.

Example: Delete all groups.

```
Switch#clear ip igmp proxy agggroup
```

Related Commands: **show ip igmp proxy upstream groups**

6.11.2 debug igmp proxy all

Command: `debug igmp proxy all`
`no debug igmp proxy all`

Function: Enables all IGMP proxy debugging. The **no debug igmp proxy all** command disables all IGMP proxy debugging.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: Enables IGMP proxy debugging, which displays the IGMP packets, events, timers, and MFC entries processed by the switch.

Example:

```
Switch# debug igmp proxy all
```

6.11.3 debug igmp proxy event

Command: `debug igmp proxy event`
`no debug igmp proxy event`

Function: Enables or disables IGMP proxy event debugging.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode and Global Mode.

Usage Guidelines: Enable this debugging to view IGMP proxy event information.

Example:

```
Switch# debug igmp proxy event
```

6.11.4 debug igmp proxy mfc

Command: `debug igmp proxy mfc`
`no debug igmp proxy mfc`

Function: Enables or disables debugging of the IGMP proxy multicast forwarding cache (MFC).

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode and Global Mode.

Usage Guidelines: Enables IGMP proxy MFC debugging, which displays the multicast forwarding entries created and written.

Example:

```
Switch# debug igmp proxy mfc
```

6.11.5 debug igmp proxy packet

Command: `debug igmp proxy packet`
`no debug igmp proxy packet`

Function: Enables or disables IGMP proxy packet debugging.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode and Global Mode.

Usage Guidelines: With this debugging enabled, IGMP proxy packets received and sent can be monitored.

Example:

```
Switch# debug igmp proxy packet
```

6.11.6 debug igmp proxy timer

Command: debug igmp proxy timer
no debug igmp proxy timer

Function: Enables or disables IGMP proxy timer debugging.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode and Global Mode.

Usage Guidelines: Enables debugging of the IGMP proxy timers.

Example:

```
Switch# debug ip igmp proxy timer
```

6.11.7 ip igmp proxy

Command: ip igmp proxy
no ip igmp proxy

Function: Enables IGMP proxy. The **no ip igmp proxy** command disables this function.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: Use this command to enable IGMP proxy. For IGMP proxy to work, configure one upstream interface and at least one downstream interface in Interface Mode.

Example: Enable IGMP proxy in Global Mode.

```
Switch (config)#ip igmp proxy
```

6.11.8 ip igmp proxy aggregate

Command: ip igmp proxy aggregate
no ip igmp proxy aggregate

Function: Enables non-querier downstream interfaces to aggregate IGMP operations.

Command Mode: Global Mode.

Default: Non-querier downstream interfaces do not aggregate IGMP operations.

Usage Guidelines: By default, non-querier downstream interfaces do not aggregate and redistribute multicast messages. This command enables all downstream interfaces to aggregate and redistribute multicast traffic.

Example:

```
Switch(config)#ip igmp proxy aggregate
```

6.11.9 ip igmp proxy downstream

Command: ip igmp proxy downstream
no ip igmp proxy downstream

Function: Configures the interface as an IGMP proxy downstream interface. The **no ip igmp proxy downstream** command disables this function.

Command Mode: Interface Mode.

Default: Disabled.

Usage Guidelines: Configures the interface as an IGMP proxy downstream interface. For IGMP proxy to work, at least one upstream interface must also be configured. The **no ip igmp proxy downstream** command removes the configuration.

Example: Configure interface VLAN 2 as an IGMP proxy downstream interface in Interface Mode.

```
Switch (config)#interface vlan 2
Switch(Config-if-Vlan2)#ip igmp proxy downstream
```

6.11.10 ip igmp proxy limit

Command: ip igmp proxy limit {group <g_limit> | source <s_limit>}
no ip igmp proxy limit

Function: Configures the maximum number of groups that the upstream interface can join and the maximum number of sources in each group.

Parameters: <g_limit>: The maximum number of groups, ranging from 1 to 500.

<s_limit>: The maximum number of sources, ranging from 1 to 500.

Command Mode: Global Mode.

Default: A maximum of 50 groups, each with up to 40 sources.

Usage Guidelines: When the group limit is exceeded, new group membership requests are rejected. This command protects against malicious group membership requests.

Example:

```
Switch(config)#ip igmp proxy limit group 30 source 20
```

6.11.11 ip igmp proxy multicast-source

Command: ip igmp proxy multicast-source
no ip igmp proxy multicast-source

Function: Configures the downstream interface as a multicast source interface. The **no** form of this command disables the configuration.

Command Mode: Interface Mode.

Default: The downstream interface is not a multicast source interface.

Usage Guidelines: When a downstream interface is configured as a multicast source interface, the switch can receive multicast traffic on that interface and forward it to the upstream interface. For this to work, the multicast router connected to the upstream interface of the switch must be configured to treat the multicast source as directly connected on the interface toward the switch.

Example: Enable **ip igmp proxy multicast-source** on downstream interface VLAN 1.

```
Switch (config)#interface vlan 1
Switch (Config-if-Vlan1)#ip igmp proxy multicast-source
```

6.11.12 ip igmp proxy unsolicited-report interval

Command: ip igmp proxy unsolicited-report interval <value>
no ip igmp proxy unsolicited-report interval

Function: Configures how often the upstream interface sends unsolicited reports.

Parameters: <value>: The interval at which the upstream interface sends unsolicited reports, ranging from 1 to 5 seconds.

Command Mode: Global Mode.

Default: 1 second.

Usage Guidelines: The upstream interface retransmits unsolicited reports so that the router does not miss reports because of link failures or packet loss. This command configures the retransmission interval.

Example:

```
Switch(config)#ip igmp proxy unsolicited-report interval 3
```

6.11.13 ip igmp proxy unsolicited-report robustness

Command: `ip igmp proxy unsolicited-report robustness <value>`
`no ip igmp proxy unsolicited-report robustness`

Function: Configures how many times the upstream interface sends unsolicited reports.

Parameters: <value>: The number of retransmissions, ranging from 2 to 10.

Command Mode: Global Mode.

Default: 2.

Usage Guidelines: The upstream interface retransmits unsolicited reports so that the router does not miss reports because of link failures or packet loss.

Example:

```
Switch(config)#ip igmp proxy unsolicited-report robustness 3
```

6.11.14 ip igmp proxy upstream

Command: `ip igmp proxy upstream`
`no ip igmp proxy upstream`

Function: Configures the interface as an IGMP proxy upstream interface. The **no ip igmp proxy upstream** command disables this function.

Command Mode: Interface Mode.

Default: Disabled.

Usage Guidelines: Configures the interface as an IGMP proxy upstream interface. For IGMP proxy to work, at least one downstream interface must also be configured. The **no ip igmp proxy upstream** command removes the configuration.

Example: Configure interface VLAN 1 as an IGMP proxy upstream interface in Interface Mode.

```
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ip igmp proxy upstream
```

6.11.15 ip multicast ssm

Command: `ip multicast ssm {range <access-list-number> | default}`
`no ip multicast ssm`

Function: Configures the SSM multicast group range for IGMP proxy. The **no** form of this command deletes the SSM group range.

Parameters: default: Uses the default SSM group range, 232.0.0.0/8.

<access-list-number>: The access list to apply, ranging from 1 to 99.

Command Mode: Global Mode.

Default: 232.0.0.0/8.

Usage Guidelines: This command configures an address filter for group membership requests; requests for the specified address range are dropped. The command applies to both IGMP proxy and PIM configurations. Note: This command cannot be used with DVMRP.

Example: Enable SSM on the switch, using the addresses in access list 23 as the SSM filter addresses.

```
Switch(config)# access-list 23 permit host-source 224.1.1.1
Switch(config)#ip multicast ssm range 23
```

6.11.16 ip pim bsr-border

Command: `ip pim bsr-border`
`no ip pim bsr-border`

Function: Configures the PIM-enabled interface to treat all multicast sources as directly connected. The **no** form of this command removes the configuration.

Command Mode: Interface Mode.

Default: Disabled.

Usage Guidelines: Treating multicast sources as directly connected on the PIM-enabled interface is used to determine the DR and originator roles.

Example: Configure PIM-enabled VLAN 2 as a BSR border. For all multicast traffic from the external network through VLAN 2, the switch treats the multicast source as directly connected.

```
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)#ip pim bsr-border
```

6.11.17 show debugging igmp proxy

Command: `show debugging igmp proxy`

Function: Displays the status of IGMP proxy debugging.

Command Mode: Admin Mode.

Usage Guidelines: Displays the IGMP proxy debugging status.

Example:

```
Switch(config)#show debugging igmp proxy
IGMP PROXY debugging status:
  IGMP PROXY event debugging is on
  IGMP PROXY packet debugging is on
  IGMP PROXY timer debugging is on
  IGMP PROXY mfc debugging is on
```

6.11.18 show ip igmp proxy

Command: `show ip igmp Proxy`

Function: Displays the IGMP proxy configuration.

Command Mode: Admin Mode.

Usage Guidelines: Displays whether IGMP proxy is enabled globally and whether upstream and downstream interfaces are configured.

Example:

```
Switch(config)#show ip igmp Proxy
IGMP PROXY MRT running: Enabled
 Total active interface number: 2
Global igmp proxy configured: YES
Total configured interface number: 2
Upstream Interface configured: YES
  Upstream Interface Vlan1(2005)
Upstream Interface configured: YES
  Downstream Interface Vlan2(2006)
 -------------------------------
```

Output	Description
IGMP PROXY MRT running	Whether the protocol is running
Total active interface number	Number of active upstream and downstream interfaces
Global igmp proxy configured	Whether IGMP proxy is enabled globally
Upstream Interface configured	Whether an upstream interface is configured
Upstream Interface Vlan	VLAN of the upstream interface
Upstream Interface configured	Whether a downstream interface is configured
Downstream Interface Vlan	VLAN of the downstream interface

6.11.19 show ip igmp proxy mroute

Command: `show ip igmp Proxy mroute`

Function: Displays IGMP proxy multicast route status.

Command Mode: Admin Mode.

Usage Guidelines: Displays IGMP proxy multicast route status and multicast route (MRT) entry information.

Example:

```
Switch(config)#show ip igmp proxy mroute
IP Multicast Routing Table
(*,G) Entries: 0
(S,G) Entries: 2
(1.1.1.2, 225.0.0.1)
 Local_include_olist    ..l.............................
 Local_exclude_olist    ................................
 Outgoing             ..o.............................
(1.1.1.3, 225.0.0.1)
 Local_include_olist    ..l.............................
 Local_exclude_olist    ................................
 Outgoing             ..o.............................
```

Output	Description
Entries	Number of entries of each type
Local_include_olist	Index of the local include outgoing interface list
Local_exclude_olist	Index of the local exclude outgoing interface list
Outgoing	Final outgoing interface index of the multicast data (S,G)

6.11.20 show ip igmp proxy upstream groups

Command: `show ip igmp proxy upstream groups {A.B.C.D}`

Function: Displays the group membership of the upstream interface.

Command Mode: Admin Mode.

Usage Guidelines: Displays the group membership of the upstream interface. If no group is specified, all groups are displayed; otherwise, only the specified group is displayed.

Example:

```
Switch(config)#show ip igmp proxy upstream groups
IGMP PROXY Connect Group Membership
Groups          Filter-mode         source
224.1.1.1       INCLUDE             192.168.1.136
226.1.1.1       *
```

Output	Description
Groups	IP address of the multicast group

Filter-mode	Filter mode of the multicast group
source	Source of the multicast group

6.12 Multicast VLAN

6.12.1 multicast-vlan

Command: `multicast-vlan`
`no multicast-vlan`

Function: Enables the multicast VLAN function on a VLAN. The **no** form of this command disables the multicast VLAN function.

Parameters: None.

Command Mode: VLAN Mode.

Default: Disabled.

Usage Guidelines: The multicast VLAN function cannot be enabled on a private VLAN. Before disabling the multicast VLAN function of a VLAN, delete the VLANs associated with it. The default VLAN cannot be configured with this command, and only one multicast VLAN is allowed on a switch.

Example:

```
Switch(config)#vlan 2
Switch(Config-Vlan2)# multicast-vlan
```

6.12.2 multicast-vlan association

Command: `multicast-vlan association <vlan-list>`
`no multicast-vlan association <vlan-list>`

Function: Associates VLANs with a multicast VLAN. The **no** form of this command cancels the associations.

Parameters: <vlan-list>: The list of VLAN IDs to associate with the multicast VLAN. Each VLAN can be associated with only one multicast VLAN, and the association succeeds only if every VLAN in the list exists.

Command Mode: VLAN Configuration Mode.

Default: The multicast VLAN is not associated with any VLAN.

Usage Guidelines: After a VLAN is associated with the multicast VLAN, when a port in that VLAN requests multicast traffic, the multicast data is sent from the multicast VLAN to the port, which reduces traffic. A VLAN associated with the multicast VLAN must not be a private VLAN. VLANs can be associated only after the multicast VLAN is enabled. Only one multicast VLAN can be enabled on a switch.

Example:

```
Switch(config)#vlan 2
Switch(Config-Vlan2)# multicast-vlan association 3, 4
```

6.12.3 multicast-vlan association interface

Command: `multicast-vlan association interface (ethernet | port-channel|) IFNAME`
`no multicast-vlan association interface (ethernet | port-channel|) IFNAME`

Function: Associates the specified port with the multicast VLAN so that the port can receive the multicast traffic. The **no** form of this command cancels the association.

Parameters: IFNAME: The name of the Ethernet port or port channel.

Command Mode: VLAN Mode.

Default: None.

Usage Guidelines:

1. The associated VLANs and the associated ports of a multicast VLAN are independent; they do not affect each other when they overlap.

2. A port that is a member of an aggregation group cannot be associated; however, an associated port can be added to a port group, which cancels the association.

3. The port must be a port channel or Ethernet port configured in Access mode.

4. The port to be associated must not belong to the multicast VLAN, and an associated port cannot be assigned to the multicast VLAN.

5. The mode of an associated port cannot be changed to a mode other than Access.

Example: VLAN 2 is the multicast VLAN.

```
Switch(config-vlan2)#multicast-vlan association interface ethernet 1/0/2
Switch(config-vlan2)#multicast-vlan association interface port-channel 2
Switch(config-vlan2)#no multicast-vlan association interface ethernet 1/0/2
Switch(config-vlan2)#no multicast-vlan association interface port-channel 2
```

6.12.4 multicast-vlan mode

Command: `multicast-vlan mode {dynamic| compatible}`
`no multicast-vlan mode {dynamic| compatible}`

Function: Configures the mode of the multicast VLAN. The **no** form of this command cancels this configuration.

Parameters: dynamic: Dynamic mode.

compatible: Compatible mode.

Command Mode: VLAN Configuration Mode.

Default: Neither mode is configured.

Usage Guidelines: In dynamic mode, mrouter ports are no longer added automatically when multicast entries are written. In compatible mode, report packets are no longer forwarded to mrouter ports. When neither mode is configured, mrouter ports are added when multicast entries are written, and received report packets are forwarded to mrouter ports.

Example:

```
Switch(Config-Vlan2)#multicast vlan mode dynamic
Switch(Config-Vlan2)#
```

6.12.5 switchport association multicast-vlan

Command: `switchport association multicast-vlan <vlan-id> out-tag <tag-id>`
`no switchport association multicast-vlan <vlan-id>`

Function: Associates a port with the specified multicast VLAN. The **no** form of this command cancels the association.

Parameters: <vlan-id> is the multicast VLAN associated with the port. Each port can be associated with only one multicast VLAN, and the association succeeds only if the multicast VLAN exists.

<tag-id>, ranging from 1 to 4094, specifies the VLAN tag carried by multicast data forwarded from this port. The tag takes effect only if the port allows the multicast VLAN as tagged.

Command Mode: Interface Mode.

Default: The port is not associated with any multicast VLAN.

Usage Guidelines: A port associated with a multicast VLAN is added to that VLAN. When the port requests traffic from a multicast source in the multicast VLAN, multicast data is sent from the multicast VLAN to the port without configuring the port as a trunk, which reduces multicast replication. If the associated port is a trunk port that allows the multicast VLAN, multicast traffic is forwarded with the VLAN tag specified by this command. Associating multicast VLANs with trunk ports allows the downstream port to reach the receivers through a Layer 2 network instead of requiring a direct connection. Associated ports can be configured only after the multicast VLAN function is configured.

Example:

```
Switch(config)#vlan 2
Switch(Config-Vlan2)#multicast-vlan
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#switchport mode trunk
Switch(config-if-ethernet1/0/1)#switchport association multicast-vlan 2 out-
tag 5
```

Chapter 7 Commands for Security Function

7.1 ACL

7.1.1 absolute-periodic/periodic

Command: [no] absolute-periodic {Monday|Tuesday|Wednesday|Thursday|Friday |Saturday|Sunday}<start_time>to{Monday|Tuesday|Wednesday|Thursday| Friday|Saturday| Sunday} <end_time>
[no]periodic{{Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Su nday}|daily| weekdays | weekend} <start_time> to <end_time>

Function: Defines periodic time ranges within a week; the time range repeats every week.

Parameters:

Friday: Friday.

Monday: Monday.

Saturday: Saturday.

Sunday: Sunday.

Thursday: Thursday.

Tuesday: Tuesday.

Wednesday: Wednesday.

daily: Every day of the week.

weekdays: Monday through Friday.

weekend: Saturday and Sunday.

<start_time>: The start time, in HH:MM:SS (hour:minute:second).

<end_time>: The end time, in HH:MM:SS (hour:minute:second).

Note: Time ranges are polled once per minute, so the time error is up to one minute.

Command Mode: Time-Range Mode.

Default: No time range is configured.

Usage Guidelines: Configures a periodic time range, that is, a specific time period on the days from Monday to Sunday each week, in one of the following formats:

```
day1 hh:mm:ss To day2 hh:mm:ss  or
{[day1+day2+day3+day4+day5+day6+day7]|weekend|weekdays|daily} hh:mm:ss To
hh:mm:ss
```

Example: Make the configuration effective from 9:15:30 on Tuesday to 12:30:00 on Saturday.

```
Switch(config)#time-range dc_timer
Switch(Config-Time-Range-dc_timer)#absolute-periodic Tuesday 9:15:30 to
Saturday 12:30:00
```

Make the configuration effective from 14:30:00 to 16:45:00 on Monday, Wednesday, Friday, and Sunday.

```
Switch(Config-Time-Range-dc_timer)#periodic Monday Wednesday Friday Sunday
14:30:00 to 16:45:00
```

7.1.2 absolute start

Command: [no] absolute start <start_time> <start_data> [end <end_time> <end_data>]

Function: Defines an absolute time range based on the clock of the device.

Parameters: <start_time>: The start time, in HH:MM:SS (hour:minute:second).

<end_time>: The end time, in HH:MM:SS (hour:minute:second).

<start_data>: The start date, in YYYY.MM.DD (year.month.day).

<end_data>: The end date, in YYYY.MM.DD (year.month.day).

Note: Time ranges are polled once per minute, so the time error is up to one minute.

Command Mode: Time-Range Mode.

Default: No time range is configured.

Usage Guidelines: Configures an absolute time range by specifying the start year, month, day, hour, and minute. Only one absolute time range can be configured; if it is configured again, the new configuration overwrites the previous one.

Example: Make the configuration effective from 6:00:00 on October 1, 2004, to 13:30:00 on January 26, 2005.

```
Switch(config)#Time-range dcn_timer
Switch(Config-Time-Range-dcn_timer)#absolute start 6:00:00 2004.10.1 end
13:30:00 2005.1.26
```

7.1.3 access-list deny-preemption

Command: `[no] access-list deny-preemption`

Function: Enables the deny-preemption function. The **no** form of this command disables it.

Parameters: None.

Command Mode: Global Mode.

Default: Enabled.

Usage Guidelines: Deny-preemption ensures that deny rules in the ACL module take precedence over other modules, but it limits the number of ACL rules. The firewall must be enabled before this command is used. If ACLs have already been written to hardware, this command takes effect after the firewall is reset.

Note: The switch does not support the **no access-list deny-preemption** command.

7.1.4 access-list (ip extended)

Command: access-list <num> {deny | permit} icmp {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [<icmp-type> [<icmp-code>]] [precedence <prec>] [tos <tos>][time-range<time-range-name>]

access-list <num> {deny | permit} igmp {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [<igmp-type>] [precedence <prec>] [tos <tos>][time-range<time-range-name>]

access-list <num> {deny | permit} tcp {{ <sIpAddr> <sMask> } | any-source | {host-source <sIpAddr> }} [s-port { <sPort> | range <sPortMin> <sPortMax> }] {{ <dIpAddr> <dMask> } | any-destination | {host-destination <dIpAddr> }} [d-port { <dPort> | range <dPortMin> <dPortMax> }] [ack+ fin+ psh+ rst+ urg+ syn] [precedence <prec>] [tos <tos>][time-range <time-range-name>]

access-list <num> {deny | permit} udp {{ <sIpAddr> <sMask> } | any-source | {host-source <sIpAddr> }} [s-port { <sPort> | range <sPortMin> <sPortMax>] {{ <dIpAddr> <dMask> } | any-destination | {host-destination <dIpAddr> }} [d-port { <dPort> | range <dPortMin> <dPortMax> }] [precedence <prec>] [tos <tos>][time-range<time-range-name>]

access-list <num> {deny | permit} {eigrp | gre | igrp | ipinip | ip | ospf | <protocol-num> } {{ <sIpAddr> <sMask> } | any-source | {host-source <sIpAddr> }} {{ <dIpAddr> <dMask> } | any-destination | {host-destination <dIpAddr> }} [precedence <prec>] [tos <tos>] [time-range <time-range-name>]

no access-list <num>

Function: Creates a numbered extended IP access rule that matches a specific IP protocol or all IP protocols. If the numbered extended access list does not exist, it is created.

Parameters: <num> is the access list number, ranging from 100 to 299. **<protocol-num>** is the IP upper-layer protocol number, ranging from 0 to 255. **<sIpAddr>** is the source IP address in dotted decimal notation. **<sMask>** is the wildcard (inverse) mask of the source IP address in dotted decimal notation. **<dIpAddr>** is the destination IP address in dotted decimal notation. **<dMask>** is the wildcard (inverse) mask of the destination IP address in dotted decimal notation; a 0 bit means the bit is matched and a 1 bit means it is ignored. **<igmp-type>** is the IGMP type, ranging from 0 to 255. **<icmp-type>** is the ICMP type, ranging from 0 to 255. **<icmp-code>** is the ICMP code, ranging from 0 to 255. **<prec>** is the IP precedence, ranging from 0 to 7. **<tos>** is the ToS value, ranging from 0 to 15. **<sPort>** is the source port number, ranging from 0 to 65535. **<sPortMin>** is the lower bound of the source port range. **<sPortMax>** is the upper bound of the source port range. **<dPortMin>** is the lower bound of the destination port range. **<dPortMax>** is the upper bound of the destination port range. **<dPort>** is the destination port number, ranging from 0 to 65535. **<time-range-name>** is the name of the time range.

Command Mode: Global Mode.

Default: No access list is configured.

Usage Guidelines: When a **<num>** is specified for the first time, an ACL with that number is created and rules are then added to it. Access lists numbered 200 to 299 can use non-contiguous wildcard masks for IP addresses.

<igmp-type> specifies the IGMP packet type. Common values are as follows:

```
17(0x11): IGMP QUERY packet
18(0x12): IGMP V1 REPORT packet
22(0x16): IGMP V2 REPORT packet
23(0x17): IGMP V2 LEAVE packet
```

```
34(0x22): IGMP V3 REPORT packet
19(0x13): DVMR packet
20(0x14): PIM V1 packet
```

Note: These packet types apply only to packets without IP options. IGMP packets normally contain IP option fields, so this configuration has no effect on them. To match packets that contain options, configure an offset-based rule instead.

Example: Create numbered extended access list 110 to deny ICMP packets and permit UDP packets with destination address 192.168.0.1 and destination port 32.

```
Switch(config)#access-list 110 deny icmp any any-destination
Switch(config)#access-list 110 permit udp any host-destination 192.168.0.1 d-
port 32
```

7.1.5 access-list (ip standard)

Command: access-list <num> {deny | permit} {{<sIpAddr> <sMask >} | any-source| {host-source <sIpAddr>}}
no access-list <num>

Function: Creates a numbered standard IP access list. If the access list exists, a rule is added. The **no access-list <num>** command deletes the numbered standard IP access list.

Parameters: <num> is the access list number, ranging from 1 to 99. **<sIpAddr>** is the source IP address in dotted decimal notation. **<sMask>** is the wildcard (inverse) mask of the source IP address in dotted decimal notation.

Command Mode: Global Mode.

Default: No access list is configured.

Usage Guidelines: When a **<num>** is specified for the first time, an ACL with that number is created and rules are then added to it.

Example: Create numbered standard IP access list 20 to permit packets with source address 10.1.1.0/24 and deny other packets with source address 10.1.1.0/16.

```
Switch(config)#access-list 20 permit 10.1.1.0 0.0.0.255
Switch(config)#access-list 20 deny 10.1.1.0 0.0.255.255
```

7.1.6 access-list(mac extended)

Command: access-list <num> {deny | permit} {any-source-mac | {host-source-mac <host_smac>} | {<smac> <smac-mask>}} {any-destination-mac | {host-destination-mac <host_dmac>} | {<dmac> <dmac-mask>}} {untagged-eth2 | tagged-eth2 | untagged-802-3 | tagged-802-3} [<offset1> <length1> <value1> [<offset2> <length2> <value2> [<offset3> <length3> <value3> [<offset4> <length4> <value4>]]]]]
no access-list <num>

Function: Defines a numbered extended MAC ACL rule. The **no access-list <num>** command deletes the numbered extended MAC access list.

Parameters: <num> is the access list number, a decimal number from 1100 to 1199. **deny**: Denies access if the rule matches. **permit**: Permits access if the rule matches. **any-source-mac**: Any source MAC address. **any-destination-mac**: Any destination MAC address. **<host_smac>**, **<smac>**: The source MAC address. **<smac-mask>**: The wildcard (inverse) mask of the source MAC address. **<host_dmac>**, **<dmac>**: The destination MAC address. **<dmac-mask>**: The wildcard (inverse) mask of the destination MAC address. **untagged-eth2**: Untagged Ethernet II frames. **tagged-eth2**: Tagged Ethernet II frames. **untagged-802-3**: Untagged Ethernet 802.3 frames. **tagged-802-3**: Tagged Ethernet 802.3 frames. **<offset(x)>**: The offset from the start of the frame, ranging from 12 to 79. Windows must start after the source MAC address and must not overlap; that is, Offset(x+1) must be greater than Offset(x) + Length(x). **<length(x)>**: The length, ranging from 1 to 4; Offset(x) + Length(x) must not exceed 80 (currently 64). **<value(x)>**: A hexadecimal value. When Length(x) is 1, the range is 0 to ff; when 2, 0 to ffff; when 3, 0 to ffffff; when 4, 0 to ffffffff.

The value range of Offset(x) depends on the frame type:

For untagged-eth2 frames: 12 to 75

For untagged-802-3 frames: 20 to 75

For tagged-eth2 frames: 12 to 79

For tagged-802-3 frames: 12 to 15 and 24 to 79

Command Mode: Global Mode.

Default: No access list is configured.

Usage Guidelines: When a **<num>** is specified for the first time, an ACL with that number is created and rules are then added to it.

Example: Permit tagged Ethernet II frames with any source and destination MAC address whose 17th and 18th bytes are 0x08 and 0x00.

```
Switch(config)#access-list 1100 permit any-source-mac any-destination-mac
tagged-eth2 16 2 0800
```

7.1.7 access-list(mac-ip extended)

Command:

```
access-list<num>{deny|permit}{any-source-mac| {host-source-
mac<host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-
destination-mac <host_dmac>}|{<dmac><dmac-mask>}}icmp
{{<source><source-wildcard>}|any-source|{host-source<source-host-
ip>}} {{<destination><destination-wildcard>}|any-destination|
{host-destination<destination-host-ip>}}[<icmp-type> [<icmp-
code>]] [precedence <precedence>] [tos <tos>][time-range<time-
range-name>]
access-list<num>{deny|permit}{any-source-mac| {host-source-
mac<host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-
destination-mac <host_dmac>}|{<dmac><dmac-mask>}}igmp
{{<source><source-wildcard>}|any-source|{host-source<source-host-
ip>}} {{<destination><destination-wildcard>}|any-destination|
{host-destination<destination-host-ip>}} [<igmp-type>] [precedence
<precedence>] [tos <tos>][time-range<time-range-name>]
access-list <num> {deny|permit}{any-source-mac| {host-source-mac
<host_smac> }|{ <smac> <smac-mask> }}{any-destination-mac| {host-
destination-mac <host_dmac> }|{ <dmac> <dmac-mask> }}tcp
{{ <source> <source-wildcard> }|any-source| {host-source <source-
host-ip> }}[s-port{ <port1> | range <sPortMin> <sPortMax> }]
{{ <destination> <destination-wildcard> } | any-destination |
{host-destination <destination-host-ip> }} [d-port { <port3> |
range <dPortMin> <dPortMax> }] [ack+fin+psh+rst+urg+syn]
[precedence  <precedence> ] [tos <tos> ] [time-range <time-range-
name> ]
access-list <num> {deny|permit}{any-source-mac| {host-source-mac
<host_smac> }|{ <smac> <smac-mask> }}{any-destination-mac| {host-
destination-mac <host_dmac> }|{ <dmac> <dmac-mask> }}udp
{{ <source> <source-wildcard> }|any-source| {host-source <source-
host-ip> }}[s-port{ <port1> | range <sPortMin> <sPortMax> }]
{{ <destination> <destination-wildcard> }|any-destination| {host-
destination <destination-host-ip> }}[d-port{ <port3> | range
<dPortMin> <dPortMax> }]        [precedence <precedence> ] [tos
<tos> ][time-range <time-range-name> ]
access-list <num> {deny|permit}{any-source-mac| {host-source-mac
<host_smac> }|{ <smac> <smac-mask> }} {any-destination-mac|{host-
destination-mac <host_dmac> }|{ <dmac> <dmac-mask> }} {eigrp|gre|
igrp|ip|ipinip|ospf|{ <protocol-num> }} {{ <source> <source-
wildcard> }|any-source|{host-source <source-host-ip> }}
{{ <destination> <destination-wildcard> }|any-destination| {host-
destination <destination-host-ip> }} [precedence <precedence> ]
[tos <tos> ][time-range <time-range-name> ]
```

Function: Defines a numbered extended MAC-IP ACL rule. The **no** form of this command deletes the numbered extended MAC-IP access list.

Parameters: <num>: The access list number, a decimal number from 3100 to 3299. **deny**: Denies access if the rule matches. **permit**: Permits access if the rule matches. **any-source-mac**: Any source MAC address. **any-destination-mac**: Any destination MAC address. **<host_smac>**, **<smac>**: The source MAC address. **<smac-mask>**: The wildcard (inverse) mask of the source MAC address. **<host_dmac>**, **<dmac>**: The destination MAC address. **<dmac-mask>**: The wildcard (inverse) mask of the destination MAC address. **protocol**: The name or number of the IP protocol, either a keyword (eigrp, gre, icmp, igmp, igrp, ip, ipinip, ospf, tcp, or udp) or an integer from 0 to 255. Use the keyword **ip** to match all Internet protocols (including ICMP, TCP, and UDP). **<source-host-ip>**, **<source>**: The source network or host from which the packet is sent, a 32-bit number in dotted decimal notation; **host-source** indicates a source host address, otherwise a network address. **<source-wildcard>**: The wildcard (inverse) mask of the source, a 32-bit number in dotted decimal notation. **<destination-host-ip>**, **<destination>**: The destination network or host to which the packet is sent, a 32-bit number in dotted decimal notation; **host-destination** indicates a destination host address, otherwise a network address. **<destination-wildcard>**: The wildcard (inverse) mask of the destination, a 32-bit number in dotted decimal notation. **s-port** (optional): Matches the TCP/UDP source port. **<port1>** (optional): The TCP/UDP source port number, an integer from 0 to 65535. **d-port** (optional): Matches the TCP/UDP destination port. **<sPortMin>**: The lower bound of the source port range. **<sPortMax>**: The upper bound of the source port range. **<port3>** (optional): The TCP/UDP destination port number, an integer from 0 to 65535. **<dPortMin>**: The lower bound of the destination port range. **<dPortMax>**: The upper bound of the destination port range. **ack, fin, psh, rst, urg, syn** (optional): TCP only. Multiple flags can be selected; packets match when the corresponding TCP flags are set. **precedence** (optional): Filters packets by precedence, a number from 0 to 7. **tos** (optional): Filters packets by type of service, a number from 0 to 15. **icmp-type** (optional): Filters ICMP packets by type, a number from 0 to 255. **icmp-code** (optional): Filters ICMP packets by code, a number from 0 to 255. **igmp-type** (optional): Filters IGMP packets by type, a number from 0 to 255. **<time-range-name>**: The name of the time range.

Command Mode: Global Mode.

Default: No access list is configured.

Usage Guidelines: When a **<num>** is specified for the first time, an ACL with that number is created and rules are then added to it. Access lists numbered 3200 to 3299 can use non-contiguous wildcard masks for IP addresses.

Example: Permit TCP packets with source MAC address 00-12-34-45-XX-XX, any destination MAC address, source IP address 100.1.1.0 0.255.255.255, source port 100, and destination port 40000.

```
Switch(config)#access-list 3199 permit 00-12-34-45-67-00 00-00-00-00-FF-FF
any-destination-mac tcp 100.1.1.0 0.255.255.255 s-port 100 any-destination d-
port 40000
```

7.1.8 access-list(mac standard)

Command: access-list <num> {deny|permit} {any-source-mac | {host-source-mac <host_smac> } | {<smac> <smac-mask>} }
no access-list <num>

Function: Defines a numbered standard MAC ACL rule. The **no** form of this command deletes the numbered standard MAC access list.

Parameters: <num> is the access list number, a decimal number from 700 to 799. **deny**: Denies access if the rule matches. **permit**: Permits access if the rule matches. **<host_smac>**, **<smac>**: The source MAC address. **<smac-mask>**: The wildcard (inverse) mask of the source MAC address.

Command Mode: Global Mode.

Default: No access list is configured.

Usage Guidelines: When a **<num>** is specified for the first time, an ACL with that number is created and rules are then added to it.

Example: Permit packets with source MAC address 00-00-XX-XX-00-01 and deny packets with source MAC address 00-00-00-XX-00-ab.

```
Switch(config)# access-list 700 permit 00-00-00-00-00-01 00-00-FF-FF-00-00
Switch(config)# access-list 700 deny 00-00-00-00-00-ab 00-00-00-FF-00-00
```

7.1.9 clear access-group

Command: clear access-group (in | out) statistic interface { <interface-name> | ethernet<interface-name> }

Function: Clears the packet statistics of the specified interface.

Parameters: <interface-name>: The interface name.

Command Mode: Admin Mode.

Default: None.

Example: Clear the outbound packet statistics of interface Ethernet 1/0/1.

```
Switch#clear access-group out statistic interface ethernet 1/0/1
```

7.1.10 firewall

Command: firewall {enable | disable}

Function: Enables or disables the firewall.

Parameters: enable: Enables the firewall. **disable**: Disables the firewall.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Access rules can be configured whether the firewall is enabled or disabled, but they can be applied to specific directions of specific ports only when the firewall is enabled. When the firewall is disabled, all ACLs bound to ports are deleted.

Example: Enable the firewall.

```
Switch(config)#firewall enable
```

7.1.11 ip access extended

Command: ip access extended <name>
no ip access extended <name>

Function: Creates a named extended IP access list. The **no** form of this command deletes the named extended IP access list, including all its rules.

Parameters: <name> is the name of the access list, 1 to 64 characters, not all digits.

Command Mode: Global Mode.

Default: No access list is configured.

Usage Guidelines: When this command is issued for the first time, an empty access list is created.

Example: Create an extended IP access list named tcpFlow.

```
Switch(config)#ip access-list extended tcpFlow
```

7.1.12 ip access standard

Command: ip access standard <name>
no ip access standard <name>

Function: Creates a named standard IP access list. The **no** form of this command deletes the named standard access list, including all its rules.

Parameters: <name> is the name of the access list, 1 to 64 characters, not all digits.

Command Mode: Global Mode.

Default: No access list is configured.

Usage Guidelines: When this command is issued for the first time, an empty access list is created.

Example: Create a standard IP access list named ipFlow.

```
Switch(config)#ip access-list standard ipFlow
```

7.1.13 ipv6 access-list

Command: ipv6 access-list <num-std> {deny | permit} {<sIPv6Prefix/sPrefixlen> | any-source | {host-source <sIPv6Addr>}}

ipv6 access-list <num-ext> {deny | permit} icmp {{ <sIPv6Prefix/sPrefixlen> } | any-source | {host-source <sIPv6Addr> }} { <dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr> }} [<icmp-type> [<icmp-code>]] [dscp <dscp>] [flow-label <fl>][time-range <time-range-name>]

ipv6 access-list <num-ext> {deny | permit} tcp {{ <sIPv6Prefix/<sPrefixlen> } | any-source | {host-source <sIPv6Addr> }} [s-port { <sPort> | range <sPortMin> <sPortMax> }] {{ <dIPv6Prefix/<dPrefixlen> } | any-destination | {host-destination <dIPv6Addr> }} [dPort { <dPort> | range <dPortMin> <dPortMax> }] [syn | ack | urg | rst | fin | psh] [dscp <dscp>] [flow-label <flowlabel>][time-range <time-range-name>]

ipv6 access-list <num-ext> {deny | permit} udp {{ <sIPv6Prefix/<sPrefixlen> } | any-source | {host-source <sIPv6Addr> }} [s-port { <sPort> | range <sPortMin> <sPortMax> }] {{ <dIPv6Prefix/<dPrefixlen> } | any-destination | {host-destination <dIPv6Addr> }} [dPort { <dPort> | range <dPortMin> <dPortMax> }] [dscp <dscp>] [flow-label <flowlabel>][time-range <time-range-name>]

ipv6 access-list <num-ext> {deny | permit} <next-header> { <sIPv6Prefix/sPrefixlen> | any-source | {host-source <sIPv6Addr> }} { <dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr> }} [dscp <dscp>] [flow-label <fl>][time-range <time-range-name>]

no ipv6 access-list { <num-std> | <num-ext> }

Function: Creates a numbered standard or extended IPv6 access list. If the access list already exists, a rule is added to it. The **no ipv6 access-list {<num-std>|<num-ext>}** command deletes the numbered IPv6 access list.

Parameters: <num-std> is the standard list number, ranging from 500 to 599. **<num-ext>** is the extended list number, ranging from 600 to 699. **<sIPv6Prefix>** is the prefix of the IPv6 source address. **<sPrefixlen>** is the prefix length of the IPv6 source address, ranging from 1 to 128. **<sIPv6Addr>** is the IPv6 source address. **<dIPv6Prefix>** is the prefix of the IPv6 destination address. **<dPrefixlen>** is the prefix length of the IPv6 destination address, ranging from 1 to 128. **<dIPv6Addr>** is the IPv6 destination address. **<icmp-type>** is the ICMP type. **<icmp-code>** is the ICMP code. **<dscp>** is the IPv6 DSCP value, ranging from 0 to 63. **<flowlabel>** is the flow label value, ranging from 0 to 1048575. **syn, ack, urg, rst, fin, psh** are TCP flags. **<sPort>** is the source port number, ranging from 0 to 65535. **<sPortMin>** is the lower bound of the source port range. **<sPortMax>** is the upper bound of the source port range. **<dPort>** is the destination port number, ranging from 0 to 65535. **<dPortMin>** is the lower bound of the destination port range. **<dPortMax>** is the upper bound of the destination port range. **<next-header>** is the IPv6 next header, ranging from 0 to 255. **<time-range-name>** is the name of the time range.

Command Mode: Global Mode.

Default: No access list is configured.

Usage Guidelines: The first time this command is entered with a number (for example, 520), a numbered standard IPv6 access list is created; subsequent rules are added to it.

Example: Create numbered standard IPv6 access list 520 to permit packets from source 2003:1:2:3::1/64 and deny all other packets from source 2003:1:2::1/48.

```
Switch (config)#ipv6 access-list 520 permit 2003:1:2:3::1/64
Switch (config)#ipv6 access-list 520 deny 2003:1:2:::1/48
```

7.1.14 ipv6 access standard

Command: ipv6 access-list standard <name>
no ipv6 access-list standard <name>

Function: Creates a named standard IPv6 access list. The **no ipv6 access-list standard <name>** command deletes the named standard IPv6 access list, including all its entries.

Parameters: <name> is the name of the access list, 1 to 64 characters long.

Command Mode: Global Mode.

Default: No access list is configured.

Usage Guidelines: When this command is run for the first time, an empty access list with no entries is created.

Example: Create a standard IPv6 access list named ip6Flow.

```
Switch(config)#ipv6 access-list standard ip6Flow
```

7.1.15 ipv6 access extended

Command: ipv6 access-list extended <name>
no ipv6 access-list extended <name>

Function: Creates a named extended IPv6 access list. The **no** form of this command deletes the named extended IPv6 access list.

Parameters: <name> is the name of the access list, 1 to 64 characters long.

Command Mode: Global Mode.

Default: No access list is configured.

Usage Guidelines: When this command is run for the first time, an empty access list with no entries is created.

Example: Create an extended IPv6 access list named tcpFlow.

```
Switch (config)#ipv6 access-list extended tcpFlow
```

7.1.16 {ip|ipv6|mac|mac-ip} access-group

Command: {ip|ipv6|mac|mac-ip} access-group <name> {in | out} [traffic-statistic]
no {ip|ipv6|mac|mac-ip} access-group <name> {in | out}

Function: Applies an access list to a direction of the port and, optionally, adds statistics counters to the ACL rules. The **no** form of this command removes the access list from the port.

Parameters: <name> is the name of the access list, 1 to 32 characters long. **in**: Ingress direction. **out**: Egress direction. **traffic-statistic**: Enables statistics counters for the ACL rules.

Command Mode: Port Mode.

Default: No ACL is bound to the port.

Usage Guidelines: Ingress and egress rules can both be bound to a port. ACLs filter packets in the ingress and egress directions, permitting or denying packets that match the rules. IP, MAC, MAC-IP, and IPv6 ACLs are supported. All four ACL types can be bound in the ingress direction at the same time. The egress direction has four resources: IP and MAC ACLs each use one resource, and MAC-IP and IPv6 ACLs each use two, so all four types cannot be bound in the egress direction at the same time. When three types are bound, they must be IP, MAC, and MAC-IP, or IP, MAC, and IPv6. When two types are bound, any combination is valid. Only one ACL of each type can be applied to a port.

Currently, note the following when binding egress ACLs to a port:

1. IP ACLs that match TCP/UDP port ranges cannot be bound.

2. MAC-IP ACLs that match TCP/UDP port ranges cannot be bound.

3. IP ACLs that match the flow label cannot be bound.

There are four ACL types based on the header fields they match: MAC, IP, MAC-IP, and IPv6. When a packet matches ACLs of several types, their filter actions (permit or deny) may conflict. Each ACL type has a strict priority, which determines the final filter action when a conflict occurs.

The following limits apply when binding ACLs to a port:

1. Each port can be bound with one MAC-IP ACL, one IP ACL, one MAC ACL, and one IPv6 ACL.

2. When four ACLs are bound and a packet matches several of them, the priorities from high to low are as follows:

Ingress IPv6 ACL

Ingress MAC-IP ACL

Ingress MAC ACL

Ingress IP ACL

Example: Bind access list aaa to the ingress direction of the port.

```
Switch(Config-If-Ethernet1/0/5)#ip access-group aaa in
```

7.1.17 mac access extended

Command: mac-access-list extended <name>
no mac-access-list extended <name>

Function: Defines a named MAC ACL or enters its access list configuration mode. The **no mac-access-list extended <name>** command deletes the ACL.

Parameters: <name>: The name of the access list. It cannot contain spaces or quotation marks, must start with a letter, can be up to 64 characters long, and is case-sensitive.

Command Mode: Global Mode.

Default: No access list is configured.

Usage Guidelines: The first time this command is entered, an empty named access list with no entries is created.

Example: Create a MAC ACL named mac_acl.

```
Switch(config)# mac-access-list extended mac_acl
Switch(Config-Mac-Ext-Nacl-mac_acl)#
```

7.1.18 mac-ip access extended

Command: mac-ip-access-list extended <name>
no mac-ip-access-list extended <name>

Function: Defines a named MAC-IP ACL or enters its access list configuration mode. The **no mac-ip-access-list extended <name>** command deletes the ACL.

Parameters: <name>: The name of the access list. It cannot contain spaces or quotation marks, must start with a letter, can be up to 64 characters long, and is case-sensitive.

Command Mode: Global Mode.

Default: No named MAC-IP access list is configured.

Usage Guidelines: The first time this command is entered, an empty named access list with no entries is created.

Example: Create a MAC-IP ACL named macip_acl.

```
Switch(config)# mac-ip-access-list extended macip_acl
Switch(Config-MacIp-Ext-Nacl-macip_acl)#
```

7.1.19 permit | deny (ip extended)

Command: [no] {deny | permit} icmp {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [<icmp-type> [<icmp-code>]] [precedence <prec>] [tos <tos>][time-range<time-range-name>]

[no] {deny | permit} igmp {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [<igmp-type>] [precedence <prec>] [tos <tos>][time-range<time-range-name>]

[no] {deny | permit} tcp {{ <sIpAddr> <sMask> } | any-source | {host-source <sIpAddr> }} [s-port { <sPort> | range <sPortMin> <sPortMax> }] {{ <dIpAddr> <dMask> } | any-destination | {host-destination <dIpAddr> }} [d-port { <dPort> | range <dPortMin> <dPortMax> }] [ack+fin+psh+rst+urg+syn] [precedence <prec>] [tos <tos>][time-range <time-range-name>]

[no] {deny | permit} udp {{ <sIpAddr> <sMask> } | any-source | {host-source <sIpAddr> }} [s-port { <sPort> | range <sPortMin> <sPortMax> }] {{ <dIpAddr> <dMask> } | any-destination | {host-destination <dIpAddr> }} [d-port { <dPort> | range <dPortMin> <dPortMax> }] [precedence <prec>] [tos <tos>][time-range<time-range-name>]

[no] {deny | permit} {eigrp | gre | igrp | ipinip | ip | ospf | <protocol-num>} {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [precedence <prec>] [tos <tos>][time-range<time-range-name>]

Function: Creates a named extended IP access rule that matches a specific IP protocol or all IP protocols.

Parameters: <sIpAddr> is the source IP address in dotted decimal notation. **<sMask>** is the wildcard (inverse) mask of the source IP address in dotted decimal notation. **<dIpAddr>** is the destination IP address in dotted decimal notation. **<dMask>** is the wildcard (inverse) mask of the destination IP address in dotted decimal notation; a 0 bit means the bit is matched and a 1 bit means it is ignored. **<igmp-type>** is the IGMP type, ranging from 0 to 255. **<icmp-type>** is the ICMP type, ranging from 0 to 255. **<icmp-code>** is the ICMP code, ranging from 0 to 255. **<prec>** is the IP precedence, ranging from 0 to 7. **<tos>** is the ToS value, ranging from 0 to 15. **<sPort>** is the source port number, ranging from 0 to 65535. **<sPortMin>** is the lower bound of the source port range. **<sPortMax>** is the upper bound of the source port range. **<dPort>** is the destination port number, ranging from 0 to 65535. **<dPortMin>** is the lower bound of the destination port range. **<dPortMax>** is the upper bound of the destination port range. **<time-range-name>** is the name of the time range.

Command Mode: Named Extended IP Access List Mode.

Default: No access list is configured.

Example: Create an extended access list that denies IGMP packets and permits UDP packets with destination address 192.168.0.1 and destination port 32.

```
Switch(config)# access-list ip extended udpFlow
Switch(Config-IP-Ext-Nacl-udpFlow)#deny igmp any any-destination
Switch(Config-IP-Ext-Nacl-udpFlow)#permit udp any host-destination
192.168.0.1 d-port 32
```

7.1.20 permit | deny(ip standard)

Command: {deny | permit} {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}}

no {deny | permit} {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}}

Function: Creates a named standard IP access rule. The **no** form of this command deletes the named standard IP access rule.

Parameters: <sIpAddr> is the source IP address in dotted decimal notation. **<sMask>** is the wildcard (inverse) mask of the source IP address in dotted decimal notation.

Command Mode: Named Standard IP Access List Mode.

Default: No access list is configured.

Example: Permit packets with source address 10.1.1.0/24 and deny other packets with source address 10.1.1.0/16.

```
Switch(config)# access-list ip standard ipFlow
Switch(Config-Std-Nacl-ipFlow)# permit 10.1.1.0 0.0.0.255
Switch(Config-Std-Nacl-ipFlow)# deny 10.1.1.0 0.0.255.255
```

7.1.21 permit | deny(ipv6 extended)

Command: [no] {deny | permit} icmp {{<sIPv6Prefix/sPrefixlen>} | any-source | {host-source <sIPv6Addr>}} {<dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr>}} [<icmp-type> [<icmp-code>]] [dscp <dscp>] [flow-label <fl>][time-range <time-range-name>]

[no] {deny | permit} tcp { <sIPv6Prefix/sPrefixlen> | any-source | {host-source <sIPv6Addr> }} [s-port { <sPort> | range <sPortMin> <sPortMax> }] { <dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr> }} [d-port { <dPort> | range <dPortMin> <dPortMax> }] [syn | ack | urg | rst | fin | psh] [dscp <dscp>] [flow-label <fl>][time-range <time-range-name>]

[no] {deny | permit} udp { <sIPv6Prefix/sPrefixlen> | any-source | {host-source <sIPv6Addr> }} [s-port { <sPort> | range <sPortMin> <sPortMax> }] { <dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr> }} [d-port { <dPort> | range <dPortMin> <dPortMax> }] [dscp <dscp>] [flow-label <fl>][time-range <time-range-name>]

[no] {deny | permit} <next-header> {<sIPv6Prefix/sPrefixlen> | any-source | {host-source <sIPv6Addr>}} {<dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr>}} [dscp <dscp>] [flow-label <fl>][time-range <time-range-name>]

[no] {deny | permit} {<sIPv6Prefix/sPrefixlen> | any-source | {host-source <sIPv6Addr>}} {<dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr>}} [dscp <dscp>] [flow-label <fl>] [time-range<time-range-name>]

Function: Creates a named extended IPv6 access control rule for a specific IPv6 protocol.

Parameters: <sIPv6Addr> is the source IPv6 address. **<sPrefixlen>** is the prefix length of the source IPv6 address, ranging from 1 to 128. **<dIPv6Addr>** is the destination IPv6 address. **<dPrefixlen>** is the prefix length of the destination IPv6 address, ranging from 1 to 128. **<icmp-type>** is the ICMP type. **<icmp-code>** is the ICMP code. **<dscp>** is the IPv6 DSCP value, ranging from 0 to 63. **<fl>** is the flow label value, ranging from 0 to 1048575. **syn, ack, urg, rst, fin, psh** are TCP flags. **<sPort>** is the source port number, ranging from 0 to 65535. **<sPortMin>** is the lower bound of the source port range. **<sPortMax>** is the upper bound of the source port range. **<dPort>** is the destination port number, ranging from 0 to 65535. **<dPortMin>** is the lower bound of the destination port range. **<dPortMax>** is the upper bound of the destination port range. **<next-header>** is the IPv6 next header. **<time-range-name>** is the name of the time range.

Command Mode: Named Extended IPv6 Access List Mode.

Default: No access list is configured.

Example: Create an extended access list named udpFlow that denies IGMP packets and permits UDP packets with destination address 2001:1:2:3::1 and destination port 32.

```
Switch(config)#ipv6 access-list extended udpFlow
Switch(Config-IPv6-Ext-Nacl-udpFlow)#deny igmp any any-destination
Switch(Config-IPv6-Ext-Nacl-udpFlow)#permit udp any-source host-destination
2001:1:2:3::1 dPort 32
```

7.1.22 permit | deny(ipv6 standard)

Command: [no] {deny | permit} {{<sIPv6Prefix/sPrefixlen>} | any-source | {host-source <sIPv6Addr>}}

Function: Creates a named standard IPv6 access control rule. The **no** form of this command deletes the rule.

Parameters: <sIPv6Prefix> is the prefix of the source IPv6 address. **<sPrefixlen>** is the prefix length, ranging from 1 to 128. **<sIPv6Addr>** is the source IPv6 address.

Command Mode: Named Standard IPv6 Access List Mode.

Default: No access list is configured.

Usage Guidelines: None.

Example: Permit packets with source address 2001:1:2:3::1/64 and deny packets with source address 2001:1:2:3::1/48.

```
Switch(config)#ipv6 access-list standard ipv6Flow
Switch(Config-IPv6-Std-Nacl-ipv6Flow)# permit 2001:1:2:3::1/64
Switch(Config-IPv6-Std-Nacl-ipv6Flow)# deny 2001:1:2:3::1/48
```

7.1.23 permit | deny(mac extended)

Command:

[no]{deny|permit} {any-source-mac|{host-source-mac <host_smac> }|{ <smac> <smac-mask> }} {any-destination-mac|{host-destination-mac <host_dmac> }|{ <dmac> <dmac-mask> }} [cos <cos-val> [<cos-bitmask>][vlanid <vid-value> [<vid-mask>][ethertype <protocol> [<protocol-mask>]]]]

[no]{deny|permit} {any-source-mac|{host-source-mac <host_smac> }|{ <smac> <smac-mask> }} {any-destination-mac|{host-destination-mac <host_dmac> }|{ <dmac> <dmac-mask> }} [ethertype <protocol> [<protocol-mask>]]

[no]{deny|permit} {any-source-mac|{host-source-mac <host_smac> }|{ <smac> <smac-mask> }} {any-destination-mac|{host-destination-mac <host_dmac> }|{ <dmac> <dmac-mask> }} [vlanid <vid-value> [<vid-mask>][ethertype <protocol> [<protocol-mask>]]]

[no]{deny|permit} {any-source-mac|{host-source-mac <host_smac> }|{ <smac> <smac-mask> }} {any-destination-mac|{host-destination-mac <host_dmac> }|{ <dmac> <dmac-mask> }} [untagged-eth2 [ethertype <protocol> [protocol-mask]]]

[no]{deny|permit}{any-source-mac|{host-source-mac <host_smac> }|{ <smac> <smac-mask> }} {any-destination-mac|{host-destination-mac <host_dmac> }|{ <dmac> <dmac-mask> }} [untagged-802-3]

[no]{deny|permit} {any-source-mac|{host-source-mac <host_smac> }|{ <smac> <smac-mask> }} {any-destination-mac|{host-destination-mac <host_dmac> }|{ <dmac> <dmac-mask> }} [tagged-eth2 [cos <cos-val> [<cos-bitmask>]] [vlanId <vid-value> [<vid-mask>]] [ethertype <protocol> [<protocol-mask>]]]

[no]{deny|permit}{any-source-mac|{host-source-mac <host_smac> }|{ <smac> <smac-mask> }} {any-destination-mac|{host-destination-mac <host_dmac> }|{ <dmac> <dmac-mask> }} [tagged-802-3 [cos <cos-val> [<cos-bitmask>]] [vlanId <vid-value> [<vid-mask>]]]

Function: Defines a named extended MAC ACL rule. The **no** form of this command deletes the rule.

Parameters: any-source-mac: Any source MAC address. **any-destination-mac**: Any destination MAC address. **<host_smac>**, **<smac>**: The source MAC address. **<smac-mask>**: The wildcard (inverse) mask of the source MAC address. **<host_dmac>**, **<dmac>**: The destination MAC address. **<dmac-mask>**: The wildcard (inverse) mask of the destination MAC address. **untagged-eth2**: Untagged Ethernet II frames. **tagged-eth2**: Tagged Ethernet II frames. **untagged-802-3**: Untagged Ethernet 802.3 frames. **tagged-802-3**: Tagged Ethernet 802.3 frames. **<cos-val>**: The CoS value, ranging from 0 to 7. **<cos-bitmask>**: The CoS mask, ranging from 0 to 7; a wildcard mask with contiguous mask bits. **<vid-value>**: The VLAN ID, ranging from 1 to 4094. **<vid-mask>**: The VLAN mask, ranging from 0 to 4095; a wildcard mask with contiguous mask bits. **<protocol>**: The Ethernet protocol number, ranging from 1536 to 65535. **<protocol-mask>**: The protocol mask, ranging from 0 to 65535; a wildcard mask with contiguous mask bits.

Note: Contiguous mask bits means that the significant bits must be contiguous starting from the leftmost bit, with no insignificant bits in between. For example, the wildcard mask 00001111b (mask 11110000b) is valid, but 00010011b is not.

Command Mode: Named Extended MAC Access List Mode.

Default: No access list is configured.

Example: Deny 802.3 frames with source MAC address 00-12-11-23-XX-XX.

```
Switch(config)# mac-access-list extended macExt
Switch(Config-Mac-Ext-Nacl-macExt)#deny 00-12-11-23-00-00 00-00-00-00-ff-ff
any-destination-mac untagged-802-3
Switch(Config-Mac-Ext-Nacl-macExt)#deny 00-12-11-23-00-00 00-00-00-00-ff-ff
any tagged-802
```

7.1.24 permit | deny(mac-ip extended)

Command:

```
[no] {deny|permit} {any-source-mac|{host-source-mac<host_smac>}|
{<smac><smac-mask>}} {any-destination-mac|{host-destination-
mac<host_dmac>}|{<dmac><dmac-mask>}} icmp{{<source><source-
wildcard>}|any-source|{host-source<source-host-ip>}}
{{<destination><destination-wildcard>}|any-destination|{host-
destination <destination-host-ip>}} [<icmp-type> [<icmp-code>]]
[precedence <precedence>] [tos <tos>][time-range<time-range-name>]
```

```
[no]{deny|permit}
{any-source-mac|{host-source-mac<host_smac>}|{<smac><smac-mask>}}
{any-destination-mac|{host-destination-mac<host_dmac>}|
{<dmac><dmac-mask>}} igmp{{<source><source-wildcard>}|any-source|
{host-source<source-host-ip>}} {{<destination><destination-
wildcard>}|any-destination|{host-destination <destination-host-
ip>}} [<igmp-type>] [precedence <precedence>] [tos <tos>][time-
range<time-range-name>]
```

```
[no]{deny|permit}{any-source-mac|{host-source-mac <host_smac> }| {
<smac> <smac-mask> }}{any-destination-mac|{host-destination-mac
<host_dmac> }|{ <dmac> <dmac-mask> }}tcp{{ <source> <source-
wildcard> }|any-source| {host-source <source-host-ip> }}[s-port
{ <port1> | range <sPortMin> <sPortMax> }] {{ <destination>
<destination-wildcard> } | any-destination| {host-destination
<destination-host-ip> }} [d-port { <port3> | range <dPortMin>
<dPortMax> }] [ack+fin+psh+rst+urg+syn] [precedence
<precedence> ] [tos <tos> ][time-range <time-range-name> ]
```

```
[no]{deny|permit}{any-source-mac|{host-source-mac <host_smac> }|
{ <smac> <smac-mask> }}{any-destination-mac|{host-destination-mac
<host_dmac> }| { <dmac> <dmac-mask> }}udp{{ <source> <source-
wildcard> }|any-source| {host-source <source-host-ip> }}[s-
port{ <port1> | range <sPortMin> <sPortMax> }] {{ <destination>
<destination-wildcard> }|any-destination| {host-destination
<destination-host-ip> }} [d-port { <port3> | range <dPortMin>
<dPortMax> }] [precedence <precedence> ] [tos <tos> ][time-range
<time-range-name> ]
```

```
[no]{deny|permit}{any-source-mac|{host-source-mac<host_smac>}|
{<smac> <smac-mask>}}{any-destination-mac|{host-destination-
mac<host_dmac>}| {<dmac><dmac-mask>}}{eigrp|gre|igrp|ip|ipinip|
ospf|{<protocol-num>}} {{<source><source-wildcard>}|any-source|
{host-source<source-host-ip>}}
{{<destination><destination-wildcard>}|any-destination|{host-
destination <destination-host-ip>}} [precedence <precedence>] [tos
<tos>][time-range<time-range-name>]
```

Function: Defines a named extended MAC-IP ACL rule. The **no** form of this command deletes the rule.

Parameters: <num>: The access list number, a decimal number from 3100 to 3199. **deny**: Denies access if the rule matches. **permit**: Permits access if the rule matches. **any-source-mac**: Any source MAC address. **any-destination-mac**: Any destination MAC address. **<host_smac>**, **<smac>**: The source MAC address. **<smac-mask>**: The wildcard (inverse) mask of the source MAC address. **<host_dmac>**, **<dmac>**: The destination MAC address. **<dmac-mask>**: The wildcard (inverse) mask of the destination MAC address. **protocol**: The name or number of the IP protocol, either a keyword (eigrp, gre, icmp, igmp, igrp, ip, ipinip, ospf, tcp, or udp) or an integer from 0 to 255. Use the keyword **ip** to match all Internet protocols (including ICMP, TCP, and UDP). **<source-host-ip>**, **<source>**: The source network or host from which the packet is sent, a 32-bit number in dotted decimal notation; **host-source** indicates a source host address, otherwise a network address. **<source-wildcard>**: The wildcard (inverse) mask of the source, a 32-bit number in dotted decimal notation. **<destination-host-ip>**, **<destination>**: The destination network or host to which the packet is sent, a 32-bit number in dotted decimal notation; **host-destination** indicates a destination host address, otherwise a network address. **<destination-wildcard>**: The wildcard (inverse) mask of the destination, a 32-bit number in dotted decimal notation. **s-port** (optional): Matches the TCP/UDP source port. **<port1>** (optional): The TCP/UDP source port number, an integer from 0 to 65535. **<sPortMin>**: The lower bound of the source port range. **<sPortMax>**: The upper bound of the source port range. **d-port** (optional): Matches the TCP/UDP destination port. **<port3>** (optional): The TCP/UDP destination port number, an integer from 0 to 65535. **<dPortMin>**: The lower bound of the destination port range. **<dPortMax>**: The upper bound of the destination port range. **ack, fin, psh, rst, urg, syn** (optional): TCP only. Multiple flags can be selected; packets match when the corresponding TCP flags are set. **precedence** (optional): Filters packets by precedence, a number from 0 to 7. **tos** (optional): Filters packets by type of service, a number from 0 to 15. **icmp-type** (optional): Filters ICMP packets by type, a number from 0 to 255. **icmp-code** (optional): Filters ICMP packets by code, a number from 0 to 255. **igmp-type** (optional): Filters IGMP packets by type, a number from 0 to 255. **<time-range-name>**: The name of the time range.

Command Mode: Named Extended MAC-IP Access List Mode.

Default: No access list is configured.

Example:

Deny UDP packets with any source and destination MAC address, any source and destination IP address, source port 100, and destination port 40000.

```
Switch(config)# mac-ip-access-list extended macIpExt
Switch(Config-MacIp-Ext-Nacl-macIpExt)# deny any-source-mac any-destination-
mac udp any-source s-port 100 any-destination d-port 40000
```

7.1.25 show access-lists

Command: `show access-lists [<num>|<acl-name>]`

Function: Displays the configured ACLs.

Parameters: <acl-name>: The name of the ACL. **<num>**: The number of the ACL.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: If no ACL is specified, all ACLs are displayed. "used x time(s)" indicates how many times the ACL is applied.

Example:

```
Switch#show access-lists
access-list 10(used 0 time(s))
   access-list 10 deny any-source
access-list 100(used 1 time(s))
   access-list 100 deny ip any any-destination
   access-list 100 deny tcp any any-destination
```

```
access-list 1100(used 0 time(s))
   access-list 1100 permit any-source-mac any-destination-mac tagged-eth2 14
2 0800
access-list 3100(used 0 time(s))
   access-list 3100 deny any-source-mac any-destination-mac udp any-source s-
port 100 any-destination d-port 40000
```

Output	Description
access-list 10(used 1 time(s))	ACL 10, applied 0 times
access-list 10 deny any-source	Denies IP packets from any source.
access-list 100(used 1 time(s))	ACL 100, applied once
access-list 100 deny ip any-source any-destination	Denies IP packets from any source IP address to any destination address.
access-list 100 deny tcp any-source any-destination	Denies TCP packets from any source IP address to any destination address.
access-list 1100 permit any-source-mac any-destination-mac tagged-eth2 14 2 0800	Permits tagged Ethernet II frames with any source and destination MAC address whose 15th and 16th bytes are 0x08 and 0x00.
access-list 3100 permit any-source-mac any-destination-mac udp any-source s-port 100 any-destination d-port 40000	Denies UDP packets with any source and destination MAC address, any source and destination IP address, source port 100, and destination port 40000.

7.1.26 show access-group

Command: `show access-group in (interface {Ethernet | Ethernet IFNAME | port-channel IFNAME})`

Function: Displays the ACL bindings on ports.

Parameters: IFNAME: The port name.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: If no interface is specified, the ACLs bound to all ports are displayed.

Example:

```
Switch#show access-group
interface name: Ethernet 1/0/1
    IP Ingress access-list used is 100, traffic-statistics Disable.
interface name: Ethernet1/0/2
IP Ingress access-list used is 1, packet(s) number is 11110.
```

Output	Description
interface name: Ethernet 1/0/1	ACL bindings on port Ethernet1/0/1
IP Ingress access-list used is 100	Numbered extended ACL 100 is bound to the ingress direction of port Ethernet1/0/1.
packet(s) number is 11110	Number of packets that matched this ACL rule

7.1.27 show firewall

Command: `show firewall`

Function: Displays the packet filtering (firewall) configuration.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch#show firewall
```

```
Firewall status: Enable.
```

Output	Description
fire wall is enable	Packet filtering is enabled.

7.1.28 show ipv6 access-lists

Command: `show ipv6 access-lists [<num>|<acl-name>]`

Function: Displays the configured IPv6 access control lists.

Parameters: <num> is the number of the access control list, ranging from 500 to 699: 500 to 599 for numbered standard IPv6 ACLs and 600 to 699 for numbered extended IPv6 ACLs. **<acl-name>** is the name of the access control list, 1 to 16 characters long.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: If no access control list is specified, all access control lists are displayed. "used x time(s)" indicates how many times the ACL is referenced.

Example:

```
Switch #show ipv6 access-lists
ipv6 access-list 500(used 1 time(s))
   ipv6 access-list 500 deny any-source
ipv6 access-list 510(used 1 time(s))
   ipv6 access-list 510 deny ip any-source any-destination
   ipv6 access-list 510 deny tcp any-source any-destination
ipv6 access-list 520(used 1 time(s))
   ipv6 access-list 520 permit ip any-source any-destination
```

7.1.29 show time-range

Command: `show time-range <word>`

Function: Displays the time range configuration.

Parameters: <word>: The name of the time range to display.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: If no time range name is specified, all time ranges are displayed.

Example:

```
Switch#show time-range
time-range timer1 (inactive, used 0 times)
         absolute-periodic Saturday 0:0:0 to Sunday 23:59:59
time-range timer2 (inactive, used 0 times)
absolute-periodic Monday 0:0:0 to Friday 23:59:59
```

7.1.30 time-range

Command: `[no] time-range <time_range_name>`

Function: Creates a time range with the specified name and enters Time-range Mode.

Parameters: <time_range_name>: The time range name. It must start with a letter and can be up to 16 characters long.

Command Mode: Global Mode.

Default: No time range is configured.

Usage Guidelines: None.

Example: Create a time range named dc_timer.

```
Switch(config)#Time-range dc_timer
```

7.2 Self-defined ACL

7.2.1 userdefined-access-list standard offset

Command: userdefined-access-list standard offset [window1 <offset>] [window2 <offset>] [window3 <offset>] [window4 <offset>][window5 <offset>][l2start <offset> | l3start <offset>| l4start <offset>]

no userdefined-access-list standard offset [window1] [window2] [window3] [window4][window5]

Function: Creates a standard self-defined ACL template. If the template exists, the corresponding windows of the template can be modified. The **no** form of this command deletes the specified windows of the template; if no window is specified, the template is deleted.

Parameters:

window1-window5: Self-defined windows 1 to 5.

<offset>: The offset, ranging from 0 to 31, in units of 2 bytes.

Command Mode: Global Mode.

Default: No template is configured.

Usage Guidelines: <offset> configures the offset of a window, ranging from 0 to 31 in units of 2 bytes; that is, 0 is an offset of 0 bytes and 1 is an offset of 2 bytes. Up to four window start positions and offsets can be configured. The basic self-defined ACL template is shared globally. While a self-defined ACL rule uses a window, that window in the template cannot be modified; when no rule references a window, use this command to modify it.

The **no** form can delete the offset configuration of one or more windows in the template, or the entire template (if no window is specified). Deletion succeeds only if the corresponding windows are not used by self-defined ACL rules.

Example: Create a global template that uses window 3 and configure its start position and offset.

```
Switch(config)#userdefined-access-list standard offset window3 l2 0 window4
```

7.2.2 userdefined-access-list standard

Command: userdefined-access-list standard <num> {deny | permit} [any-source-mac | host-source-mac <mac-address>|<mac-address> <mac-address> (any-source-mac | host-source-mac <mac-address>|<mac-address> <mac-address>) }] [window1 <word> <word>] [window2 <word> <word>] [window3 <word> <word>] [window4 <word> <word>] [window5 <word> <word>]

no userdefined-access-list <num>

Function: Creates a numbered standard self-defined ACL. If the ACL exists, a rule is added to it. The **no** form of this command deletes the numbered standard self-defined ACL.

Parameters: <num>: The access list number, a decimal number from 1200 to 1299. **deny**: Denies access if the rule matches. **permit**: Permits access if the rule matches. **<word>**: A 2-byte hexadecimal number. **<mac-address>**: The MAC address.

Command Mode: Global Mode.

Default: No access list is configured.

Usage Guidelines: When a **<num>** is specified for the first time, an ACL with that number is created and the entry is added to it.

Example: Permit packets whose first and second bytes are 0x4501.

```
Switch(config)#userdefined-access-list standard 1200 permit any-source-mac
any-destination-mac window1 45 01
Switch(config)#
```

7.2.3 vacl userdefined access-group

Command: vacl userdefined access-group <name> {in} vlan <vlanId>
[traffic-statistic]
no vacl userdefined access-group <name> {in} vlan <vlanId>

Function: Applies a self-defined access list to a direction of the specified VLAN and, optionally, adds statistics counters to the ACL. The **no** form of this command deletes the binding to the VLAN.

Parameters: <name> is the access list number, a decimal number from 1200 to 1399. **<vlanId>** is the VLAN to bind, ranging from 1 to 4095.

Command Mode: Global Mode.

Default: No self-defined access list is bound to any VLAN.

Usage Guidelines: A self-defined access list can be bound to the ingress direction of a VLAN together with other access lists. When several access lists match, deny takes precedence: if any access list matches a deny rule, the deny rule is executed; otherwise, the permit rule is executed.

Example: Configure the following self-defined access lists:

```
Switch(config)#userdefined-access-list standard offset window1 l3 0 window2
l4 1 window3 l3 1
Switch(config)#userdefined-access-list standard 1300 permit window1 4501 FFFF
window2 00FF 00FF
Switch(config)#userdefined-access-list standard 1300 deny window1 FFAA0000
FFFF0000
```

Bind the self-defined access list to VLAN 1:

```
Switch(config)#vacl userdefined access-group 1300 in vlan 1.
```

7.3 802.1x

7.3.1 debug dot1x detail

Command: debug dot1x detail {pkt-send | pkt-receive | internal | all |
userbased | webbased} interface [ethernet] <interface-name>
no debug dot1x detail { pkt-send | pkt-receive | internal | all |
userbased | webbased} interface [ethernet] <interface-name> |
port-channel <interface-name>

Function: Enables detailed 802.1X debugging. The **no** form of this command disables this debugging.

Parameters: pkt-send: Debugging of packets sent by 802.1X.

pkt-receive: Debugging of packets received by 802.1X.

internal: Debugging of 802.1X internal details.

all: All of the above debugging.

userbased: User-based authentication.

webbased: Web-based authentication.

<interface-name>: The interface name.

Command Mode: Admin Mode.

Usage Guidelines: Detailed 802.1X debugging shows the detailed operation of the RADIUS protocol, which can help diagnose faults.

Example: Enable all detailed 802.1X debugging on interface Ethernet 1/0/1.

```
Switch#debug dot1x detail all interface ethernet1/0/1
```

7.3.2 debug dot1x error

Command: **debug dot1x error**
no debug dot1x error

Function: Enables 802.1X error debugging. The **no** form of this command disables this debugging.

Parameters: None.

Command Mode: Admin Mode.

Usage Guidelines: 802.1X error debugging shows errors that occur during RADIUS protocol operation, which can help diagnose faults.

Example: Enable 802.1X error debugging.

```
Switch#debug dot1x error
```

7.3.3 debug dot1x fsm

Command: **debug dot1x fsm {all | aksm | asm | basm | ratsm} interface <interface-name>| port-channel <interface-name>**
no debug dot1x fsm {all | aksm | asm | basm | ratsm} interface <interface-name> | port-channel <interface-name>

Function: Enables 802.1X state machine debugging. The **no** form of this command disables this debugging.

Command Mode: Admin Mode.

Parameters: all: Debugging of all 802.1X state machines.

aksm: Debugging of the Authenticator Key Transmit state machine.

asm: Debugging of the Authenticator state machine.

basm: Debugging of the Backend Authentication state machine.

ratsm: Debugging of the Re-Authentication Timer state machine.

<interface-name>: The interface name.

Usage Guidelines: 802.1X debugging shows the 802.1X protocol negotiation process, which can help diagnose faults.

Example: Enable 802.1X state machine debugging.

```
Switch#debug dot1x fsm asm interface ethernet1/0/1
```

7.3.4 debug dot1x packet

Command: **debug dot1x packet {all | receive | send} interface <interface-name>| port-channel <interface-name> | port-channel <interface-name>**
no debug dot1x packet {all | receive | send} interface <interface-name>| port-channel <interface-name> | port-channel <interface-name>

Function: Enables 802.1X packet debugging. The **no** form of this command disables this debugging.

Command Mode: Admin Mode.

Parameters: send: Debugging of packets sent by 802.1X.

receive: Debugging of packets received by 802.1X.

all: Debugging of packets sent and received by 802.1X.

<interface-name>: The interface name.

Usage Guidelines: 802.1X packet debugging shows the 802.1X protocol negotiation process, which can help diagnose faults.

Example: Enable 802.1X packet debugging.

```
Switch#debug dot1x packet all interface ethernet1/0/1
```

7.3.5 dot1x accept-mac

Command: **dot1x accept-mac <mac-address> [interface <interface-name>]**
no dot1x accept-mac <mac-address> [interface <interface-name>]

Function: Adds a MAC address entry to the 802.1X address filter table. If a port is specified, the entry applies only to that port; otherwise, it applies to all ports. The **no dot1x accept-mac <mac-address> [interface <interface-name>]** command deletes the entry from the table.

Parameters: **<mac-address>** is the MAC address.

<interface-name> is the interface name and port number.

Command Mode: Global Mode.

Default: None.

Usage Guidelines: The 802.1X address filter function uses the MAC address filter table, whose entries are added and deleted manually. An entry added with a port specified applies only to that port; an entry added without a port applies to all ports on the switch. When the 802.1X address filter function is enabled, the switch filters authenticating users by MAC address: only authentication requests from users in the 802.1X address filter table are accepted, and all others are rejected.

Example: Add MAC address 00-01-34-34-2e-0a to the filter table of Ethernet 1/0/5.

```
Switch(config)#dot1x accept-mac 00-01-34-34-2e-0a interface ethernet 1/0/5
```

7.3.6 dot1x eapor enable

Command: **dot1x eapor enable**
no dot1x eapor enable

Function: Enables EAP relay authentication on the switch. The **no dot1x eapor enable** command selects EAP local termination authentication.

Command Mode: Global Mode.

Default: EAP relay authentication.

Usage Guidelines: The switch can connect to the RADIUS server over Ethernet or PPP. With an Ethernet connection, the switch authenticates users by EAP relay (EAPoR authentication); with a PPP connection, it uses EAP local termination (CHAP authentication). Select the authentication method according to how the switch connects to the authentication server.

Example: Configure EAP local termination authentication on the switch.

```
Switch(config)#no dot1x eapor enable
```

7.3.7 dot1x enable

Command: **dot1x enable**
no dot1x enable

Function: Enables 802.1X on the switch and on ports. The **no dot1x enable** command disables 802.1X.

Command Mode: Global Mode and Port Mode.

Default: 802.1X is disabled globally. When 802.1X is enabled in Global Mode, it is still disabled on ports by default.

Usage Guidelines: 802.1X must be enabled globally before it can be enabled on ports. 802.1X cannot be enabled on a port that runs Spanning Tree or MAC binding, or that is a trunk port or a member of a port aggregation group, until those conditions are removed.

Example: Enable 802.1X on the switch and on port Ethernet 1/0/12.

```
Switch(config)#dot1x enable
Switch(config)#interface ethernet 1/0/12
Switch(Config-If-Ethernet1/0/12)#dot1x enable
```

7.3.8 dot1x guest-vlan

Command: dot1x guest-vlan <vlanid>
no dot1x guest-vlan

Function: Configures the guest VLAN of the port. The **no dot1x guest-vlan** command deletes the guest VLAN.

Parameters: <vlanid>: The VLAN ID, ranging from 1 to 4094.

Command Mode: Port Mode.

Default: No 802.1X guest VLAN is configured on the port.

Usage Guidelines: If no supplicant on the port is authenticated within a certain time, for example because no dedicated supplicant software is installed or the supplicant version is too old, the access device adds the port to the guest VLAN.

In the guest VLAN, users can obtain 802.1X supplicant software, upgrade the supplicant, or update other applications (such as antivirus software or operating system patches). If a user on a port in the guest VLAN fails authentication, the port remains in the guest VLAN. If authentication succeeds, there are two possible results:

- The authentication server assigns an Auto VLAN; the port leaves the guest VLAN and joins the assigned Auto VLAN. When the user goes offline, the port returns to the guest VLAN.
- The authentication server does not assign an Auto VLAN; the port leaves the guest VLAN and joins the configured VLAN. When the user goes offline, the port returns to the guest VLAN.

Note:

- Different ports can have different guest VLANs, but each port can have only one guest VLAN.
- The guest VLAN takes effect only when the access control mode is port-based. If the access control mode of the port is MAC-based or user-based, the guest VLAN can be configured but does not take effect.

Example: Set the guest VLAN of port Ethernet 1/0/3 to VLAN 10.

```
Switch(Config-If-Ethernet1/0/3)#dot1xguest-vlan 10
```

7.3.9 dot1x macfilter enable

Command: dot1x macfilter enable
no dot1x macfilter enable

Function: Enables the 802.1X address filter function on the switch. The **no dot1x macfilter enable** command disables it.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: When the 802.1X address filter function is enabled, the switch filters authenticating users by MAC address; only authentication requests from users in the 802.1X address filter table are accepted.

Example: Enable the 802.1X address filter function on the switch.

```
Switch(config)#dot1x macfilter enable
```

7.3.10 dot1x macbased guest-vlan

Command: dot1x macbased guest-vlan <vlanid>
no dot1x macbased guest-vlan

Function: Configures the MAC-based guest VLAN of the port. The **no** form of this command deletes the guest VLAN.

Parameters: <vlanid>: The VLAN ID, ranging from 1 to 4094.

Command Mode: Port Mode.

Default: No MAC-based guest VLAN is configured.

Usage Guidelines: If no supplicant on the port is authenticated within a certain time, for example because no dedicated authentication client is installed or the client version is too old, the access device adds the user to the guest VLAN. In the guest VLAN, users can obtain the 802.1X client software, upgrade the client, or perform other updates (such as antivirus software or system patches). If a user on a port in the guest VLAN fails authentication, the port remains in the guest VLAN. If authentication succeeds, there are two possible results:

1. The authentication server assigns an Auto VLAN; the user leaves the guest VLAN and joins the Auto VLAN. When the user goes offline, the user is assigned to the configured guest VLAN again.

2. The authentication server does not assign a VLAN; the user leaves the guest VLAN and joins the configured native VLAN. When the user goes offline, the user is assigned to the configured guest VLAN again.

Note:

1. A MAC-based guest VLAN can be configured only on a port that uses MAC-based authentication and is in Hybrid mode.

2. Different ports can have different MAC-based guest VLANs, but each port can have only one.

Example: Set the MAC-based guest VLAN of Ethernet 1/0/3 to VLAN 10.

```
Switch(Config-If-Ethernet1/0/3)#dot1x macbased guest-vlan 10
```

7.3.11 dot1x macbased port-down-flush

Command: dot1x macbased port-down-flush
no dot1x macbased port-down-flush

Function: When a port using MAC-based 802.1X authentication goes down, deletes the users on that port that passed authentication. The **no** form of this command disables this behavior.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: When users authenticated by MAC address move between ports, they must be deleted so that they can authenticate again. Enable this command to delete such users.

Example: Delete the authenticated users on a port when the port using MAC-based 802.1X authentication goes down.

```
Switch(config)#dot1x macbased port-down-flush
```

7.3.12 dot1x max-req

Command: dot1x max-req <count>
no dot1x max-req

Function: Sets the number of times the switch sends EAP-Request/MD5 frames before it restarts authentication when the supplicant does not respond. The **no dot1x max-req** command restores the default.

Parameters: <count> is the number of EAP-Request/MD5 frame retransmissions, ranging from 1 to 10.

Command Mode: Global Mode.

Default: 2.

Usage Guidelines: Using the default number of EAP-Request/MD5 retransmissions is recommended.

Example: Set the maximum number of EAP-Request/MD5 retransmissions to 5.

```
Switch(config)#dot1x max-req 5
```

7.3.13 dot1x user allow-movement

Command: dot1x user allow-movement
no dot1x user allow-movement

Function: Allows users to authenticate again after moving to another port. The **no** form of this command disables this function.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: With this function enabled, the switch allows a user who has moved to another port to authenticate. Enable **dot1x user allow-movement** when the switch connects to a hub and users may move to other ports.

Example: Allow users to authenticate after moving to another port.

```
Switch(config)#dot1x user allow-movement
```

7.3.14 dot1x user free-resource

Command: dot1x user free-resource <prefix> <mask>
no dot1x user free-resource

Function: Configures the 802.1X free resource. The **no** form of this command disables this function.

Parameters: <prefix> is the network segment of the free resource, in dotted decimal notation.

<mask> is the mask of the free resource, in dotted decimal notation.

Command Mode: Global Mode.

Default: No free resource is configured.

Usage Guidelines: This command is available only with user-based access control. With user-based access control, it configures the limited resources that unauthenticated users can access. With port-based and MAC-based access control, users cannot access any network resources before authentication.

Note: Only one free resource can be configured for the whole network.

Example: Configure the free resource segment 1.1.1.0 with mask 255.255.255.0.

```
Switch(Config)#dot1x user free-resource 1.1.1.0 255.255.255.0
```

7.3.15 free-resource destination

Command: free-resource destination {ipv4 | ipv6]} <prefix>/<mask>
no free-resource destination [ipv4 | ipv6] <prefix>/<mask>

Function: Configures a global IPv4 or IPv6 free resource. The **no** form of this command deletes it.

Parameters: <prefix> is the network segment of the free resource: an IPv4 address in dotted decimal notation or an IPv6 address in colon-hexadecimal notation.

<mask> is the mask length of the free resource.

Command Mode: Global Mode.

Default: No free resource is configured.

Usage Guidelines: After a free resource is configured, users who have not passed 802.1X authentication can access it.

Example: Configure the free resource segment 100.1.1.0 with mask 255.255.255.0.

```
Switch (config): free-resource destination ipv4 100.1.1.0/24
```

7.3.16 dot1x max-user macbased

Command: dot1x max-user macbased <number>
no dot1x max-user macbased

Function: Sets the maximum number of users allowed on the port. The **no dot1x max-user macbased** command restores the default.

Parameters: <number> is the maximum number of users, ranging from 1 to 256.

Command Mode: Port Mode.

Default: 1.

Usage Guidelines: This command applies to ports that use MAC-based access control. When the number of authenticated MAC addresses reaches the limit, additional users cannot access the network.

Example: Allow five users on port Ethernet 1/0/3.

```
Switch(Config-If-Ethernet1/0/3)#dot1x max-user macbased 5
```

7.3.17 dot1x max-user userbased

Command: dot1x max-user userbased <number>
no dot1x max-user userbased

Function: Sets the maximum number of users allowed on the port in user-based access control mode. The **no** form of this command restores the default.

Parameters: <number> is the maximum number of users allowed to access the network, ranging from 1 to 256.

Command Mode: Port Mode.

Default: 10.

Usage Guidelines: This command takes effect only when the port uses user-based access control. When the number of authenticated users reaches the limit, additional users cannot access the network.

Example: Allow five users on port Ethernet 1/0/3.

```
Switch(Config-If-Ethernet1/0/3)#dot1x max-user userbased 5
```

7.3.18 dot1x portbased mode single-mode

Command: dot1x portbased mode single-mode
no dot1x portbased mode single-mode

Function: Enables single-user mode for port-based authentication. The **no** form of this command disables it.

Parameters: None.

Command Mode: Port Mode.

Default: Disabled.

Usage Guidelines: This command takes effect only when the access control mode of the port is port-based. If port-based access control (**dot1x port-method portbased**) is already enabled on the port and users are online when single-user mode is configured, the switch forces all users on the port offline. Afterward, only one user on the port can pass authentication and access the network; other users on the port are denied. When single-user mode is disabled, the switch also forces the authenticated user offline.

Example:

```
Switch(Config-If-Ethernet1/0/1)#dot1x portbased mode single-mode
```

7.3.19 dot1x port-control

Command: dot1x port-control {auto | force-authorized | force-unauthorized}
no dot1x port-control

Function: Sets the 802.1X authorization state of the port. The **no dot1x port-control** command restores the default.

Parameters: auto: Enables 802.1X authentication; the authorization state of the port is determined by the authentication exchange between the switch and the supplicant. **force-authorized**: Sets the port to the authorized state; unauthenticated data can pass through the port. **force-unauthorized**: Sets the port to the unauthorized state; the switch does not authenticate the supplicant and blocks data on the port.

Command Mode: Port Mode.

Default: When 802.1X is enabled on the port, the default is **auto**.

Usage Guidelines: If the port must authenticate users with 802.1X, set the port control mode to **auto**.

Example: Configure port Ethernet 1/0/1 to require 802.1X authentication.

```
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#dot1x port-control auto
```

7.3.20 dot1x port-method

Command: dot1x port-method {macbased | portbased | userbased {standard | advanced}}
no dot1x port-method

Function: Configures the access control method of the specified interface. The **no** form of this command restores the default access control method.

Parameters: macbased: MAC-based access control.

portbased: Port-based access control.

userbased: User-based access control, either **standard** or **advanced**.

Command Mode: Port Mode.

Default: Advanced user-based access control.

Usage Guidelines: This command configures the 802.1X access control method of the specified port. With port-based access control, only one host can authenticate through a port, and after authentication it can access all resources. With MAC-based access control, multiple hosts connected to one port can each access all network resources after authentication. With either method, unauthenticated hosts cannot access any network resources.

With user-based access control, unauthenticated users can access only limited network resources. User-based access control has two variants: standard and advanced. Standard user-based access control does not restrict access to the limited resources before the host is authenticated, whereas advanced user-based access control can control access to the limited resources before authentication.

Note: For standard user-based access control, the 802.1X free resource must be configured first, and the method must be used together with **dot1x privateclient enable**.

Example: Configure port-based access control on Ethernet 1/0/4.

```
Switch(Config-If-Ethernet1/0/4)#dot1x port-method portbased
```

7.3.21 dot1x re-authenticate

Command: dot1x re-authenticate [interface <interface-name>] | port-channel <interface-name>

Function: Re-authenticates 802.1X supplicants immediately (without waiting for the re-authentication timer) on all ports or the specified port.

Parameters: <interface-name> is the port. If omitted, all ports are re-authenticated.

Command Mode: Global Mode.

Usage Guidelines: This command is issued in Global Mode. It makes the switch re-authenticate the client immediately without waiting for the re-authentication timer to expire. The command no longer applies after authentication completes.

Example: Re-authenticate port Ethernet 1/0/8 immediately.

```
Switch(config)#dot1x re-authenticate interface ethernet 1/0/8
```

7.3.22 dot1x re-authentication

Command: dot1x re-authentication
no dot1x re-authentication

Function: Enables periodic re-authentication of supplicants. The **no dot1x re-authentication** command disables this function.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: When periodic re-authentication is enabled, the switch re-authenticates supplicants at regular intervals. This function is not recommended for general use.

Example: Enable periodic re-authentication of authenticated users.

```
Switch(config)#dot1x re-authentication
```

7.3.23 dot1x timeout quiet-period

Command: dot1x timeout quiet-period <seconds>
no dot1x timeout quiet-period

Function: Sets the quiet period after a supplicant fails authentication. The **no dot1x timeout quiet-period** command restores the default.

Parameters: <seconds> is the quiet period of the port, in seconds, ranging from 1 to 65535.

Command Mode: Global Mode.

Default: 10 seconds.

Usage Guidelines: Using the default value is recommended.

Example: Set the quiet period to 120 seconds.

```
Switch(config)#dot1x timeout quiet-period 120
```

7.3.24 dot1x timeout re-authperiod

Command: dot1x timeout re-authperiod <seconds>
no dot1x timeout re-authperiod

Function: Sets the supplicant re-authentication interval. The **no dot1x timeout re-authperiod** command restores the default.

Parameters: <seconds> is the re-authentication interval, in seconds, ranging from 1 to 65535.

Command Mode: Global Mode.

Default: 3600 seconds.

Usage Guidelines: dot1x re-authentication must be enabled before the re-authentication interval is changed; otherwise, the configured interval does not take effect.

Example: Set the re-authentication interval to 1200 seconds.

```
Switch(config)#dot1x timeout re-authperiod 1200
```

7.3.25 dot1x timeout tx-period

Command: dot1x timeout tx-period <seconds>
no dot1x timeout tx-period

Function: Sets the interval at which the switch retransmits EAP-Request/Identity frames to the supplicant. The **no dot1x timeout tx-period** command restores the default.

Parameters: <seconds> is the retransmission interval of EAP-Request frames, in seconds, ranging from 1 to 65535.

Command Mode: Global Mode.

Default: 30 seconds.

Usage Guidelines: Using the default value is recommended.

Example: Set the EAP-Request frame retransmission interval to 1200 seconds.

```
Switch(config)#dot1x timeout tx-period 1200
```

7.3.26 dot1x unicast enable

Command: dot1x unicast enable
no dot1x unicast enable

Function: Enables the 802.1X unicast pass-through function of the switch. The **no** form of this command disables it.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: Enable 802.1X unicast pass-through on the switch first, and then configure the 802.1X function.

Example: Enable 802.1X unicast pass-through on the switch and enable 802.1X on port Ethernet 1/0/1.

```
Switch(config)#dot1x enable
Switch(config)# dot1x unicast enable
Switch(config)#interface ethernet1/0/1
Switch(Config-If-Ethernet1/0/1)#dot1x enable
```

7.3.27 free-mac

Command: `free-mac <source mac><wildcard bits>`
`no free-mac <source mac><wildcard bits>`

Function: Adds an authentication-free MAC address for the switch. The **no** form of this command deletes it.

Parameters: <source mac> is the MAC address of the authentication-free user.

<wildcard bits> is the mask of the MAC address of the authentication-free user.

Command Mode: Global Mode.

Default: Not configured.

Usage Guidelines: Authentication-free MAC addresses allow specific users to access resources without authentication. To exempt a single user, specify the user's MAC address with mask ff-ff-ff-ff-ff-ff. To exempt multiple users, set the corresponding mask bits to 0.

Example: Configure 00-01-11-11-11-11 as an authentication-free MAC address.

```
Switch(config)# free-mac 00-01-11-11-11-11 ff-ff-ff-ff-ff-ff
```

7.3.28 show dot1x

Command: `show dot1x [interface <interface-list>]`

Function: Displays 802.1X parameters and status; if a port is specified, the 802.1X status of that port is displayed.

Parameters: <interface-list> is the port list. If omitted, information for all ports is displayed.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Use **show dot1x** to display 802.1X parameters and status.

Example:

Example 1: Display the global 802.1X parameters of the switch.

```
Switch#show dot1x
Global 802.1x Parameters
  reauth-enabled        no
  reauth-period         3600
  quiet-period          10
  tx-period             30
  max-req               2
  authenticator mode    passive
Mac Filter Disable
MacAccessList :
dot1x-EAPoR Enable
dot1x-privateclient Disable
dot1x-unicast Disable
802.1x is enabled on ethernet Ethernet1/0/1
Authentication Method:Port based
Max User Number:1
  Status                Authorized
  Port-control           Auto
  Supplicant            00-03-0F-FE-2E-D3
Authenticator State Machine
```

```
  State                  Authenticated
Backend State Machine
  State                  Idle
Reauthentication State Machine
  State                  Stop
```

Output	Description
Global 802.1x Parameters	Global 802.1X parameters
reauth-enabled	Whether re-authentication is enabled
reauth-period	Re-authentication interval
quiet-period	Quiet period
tx-period	EAP retransmission interval
max-req	Maximum number of EAP request retransmissions
authenticator mode	Authentication mode of the switch
Mac Filter	Whether the 802.1X address filter is enabled
MacAccessList	802.1X address filter table
dot1x-EAPoR	Authentication method used by the switch (EAP relay or EAP local termination)
dot1x-privateclient	Whether the switch supports the private client protocol
802.1x is enabled on ethernet Ethernet1/0/1	Whether 802.1X is enabled on the port
Authentication Method:	Port authentication method (MAC-based, port-based, or user-based)
Status	Port authentication status
Port-control	Port control mode
Supplicant	MAC address of the supplicant
Authenticator State Machine	Authenticator state machine status
Backend State Machine	Backend state machine status
Reauthentication State Machine	Re-authentication state machine status

7.3.29 show dot1x user

Command: `show dot1x user`

Function: Displays information about online users that have passed 802.1X authentication.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Users normally need only the online user information; the other information is for technical support in fault diagnosis and troubleshooting.

Example: Display information about online users that have passed 802.1X authentication.

```
Switch(config)# show dot1x user
------------------------ total authenticated users: 0
------------------------------
 UserName      Port      OnTime(sec)     MAC     UserIP     UserIPv6
-------------------------------------------------------------------------------
         -------------- total authenticated users: 0--------------
```

7.3.30 clear dot1x all

Command: `clear dot1x {all |interface <ethernet IFNAME | IFNAME>|mac WORD |user WORD }`

Function: Deletes online users that have passed 802.1X authentication.

Parameters: all: Deletes all 802.1X online users.

interface <IFNAME>: Deletes 802.1X online users on the specified port.

mac <WORD>: Deletes the 802.1X online user with the specified MAC address.

user <WORD>: Deletes the 802.1X online user with the specified user name.

Command Mode: Admin Mode.

Usage Guidelines: Use this command to delete 802.1X online users by MAC address, port, or user name, or to delete all of them.

Example: Delete all 802.1X online users.

```
Switch#clear dot1x all
```

7.4 Number Limitation of MAC and IP Addresses on Ports and VLANs

7.4.1 debug ip arp count

Command: debug ip arp count
no debug ip arp count

Function: Enables debugging of the ARP number limitation function in VLANs. When the number of dynamic ARP entries in a VLAN exceeds the allowed maximum, debugging information is displayed. The **no debug ip arp count** command disables this debugging.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Displays debugging information about the number of dynamic ARP entries in the VLAN.

Example:

```
Switch#debug vlan mac count
%Jun 14 16:04:40 2007 Current arp count 21 is more than or equal to the
maximum limit in vlan 1!!
%Jun 14 16:04:40 2007Arp learning will be stopped and some arp will be delete
!!
```

7.4.2 debug ipv6 nd count

Command: debug ipv6 nd count
no debug ipv6 nd count

Function: Enables debugging of the neighbor number limitation function in VLANs. When the number of dynamic neighbor entries in a VLAN exceeds the allowed maximum, debugging information is displayed. The **no debug ipv6 nd count** command disables this debugging.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Displays debugging information about the number of dynamic neighbor entries in the VLAN.

Example:

```
Switch#debug vlan mac count
%Jun 14 16:04:40 2007 Current neighbor count 21 is more than or equal to the
maximum limit in vlan 1!!
```

7.4.3 debug switchport arp count

Command: debug switchport arp count
no debug switchport arp count

Function: Enables debugging of the ARP number limitation function on ports. When the number of dynamic ARP entries on a port exceeds the allowed maximum, debugging information is displayed. The **no debug switchport arp count** command disables this debugging.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Displays debugging information about the number of dynamic ARP entries on the port.

Example:

```
Switch#debug switchport arp count
%Jun 14 16:04:40 2007 Current arp count 21 is more than or equal to the
maximum limit in port Ethernet1/0/1
!!%Jun 14 16:04:40 2007 Arp learning will be stopped and some mac will be
delete !!
```

7.4.4 debug switchport mac count

Command: debug switchport mac count
no debug switchport mac count

Function: Enables debugging of the MAC number limitation function on ports. When the number of dynamic MAC addresses on a port exceeds the allowed maximum, debugging information is displayed. The **no debug switchport mac count** command disables this debugging.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Displays debugging information about the number of dynamic MAC addresses on the port.

Example:

```
Switch#debug switchport mac count
%Jun 14 16:04:40 2007 Current mac count 21 is more than or equal to the
maximum limit in port Ethernet1/0/1
!!%Jun 14 16:04:40 2007 Mac learning will be stopped and some mac will be
delete !!
```

7.4.5 debug switchport nd count

Command: debug switchport nd count
no debug switchport nd count

Function: Enables debugging of the ND number limitation function on ports. When the number of dynamic ND entries on a port exceeds the allowed maximum, debugging information is displayed. The **no debug switchport nd count** command disables this debugging.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Displays debugging information about the number of dynamic ND entries on the port.

Example:

```
Switch#debug switchport arp count
%Jun 14 16:04:40 2007 Current neighbor count 21 is more than or equal to the
maximum limit in port  Ethernet1/0/1
!!%Jun 14 16:04:40 2007 Neighbor learning will be stopped and some mac will
be delete !!
```

7.4.6 debug vlan mac count

Command: `debug vlan mac count`
`no debug vlan mac count`

Function: Enables debugging of the MAC number limitation function in VLANs. When the number of dynamic MAC addresses in a VLAN exceeds the allowed maximum, debugging information is displayed. The **no debug vlan mac count** command disables this debugging.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Displays debugging information about the number of dynamic MAC addresses in the VLAN.

Example:

```
Switch#debug vlan mac count
%Jun 14 16:04:40 2007 Current mac count 21 is more than or equal to the
maximum limit in vlan 1!!
%Jun 14 16:04:40 2007 Mac learning will be stopped and some mac will be
delete !!
```

7.4.7 ip arp dynamic maximum

Command: `ip arp dynamic maximum <value>`
`no ip arp dynamic maximum`

Function: Sets the maximum number of dynamic ARP entries allowed in the VLAN and enables dynamic ARP number limitation in the VLAN. The **no ip arp dynamic maximum** command disables dynamic ARP number limitation in the VLAN.

Parameters: <value>: The maximum number of dynamic ARP entries in the VLAN, ranging from 1 to 4096.

Default: Disabled.

Command Mode: Interface Mode.

Usage Guidelines: If the number of dynamically learned ARP entries in the VLAN already exceeds the configured maximum, the excess dynamic ARP entries are deleted.

Example:

Enable dynamic ARP number limitation in VLAN 1 with a maximum of 50.

```
Switch(config)#interface ethernet
Switch(Config-if-Vlan1)# ip arp dynamic maximum 50
```

Disable dynamic ARP number limitation in VLAN 1.

```
Switch(Config-if-Vlan1)#no ip arp dynamic maximum
```

7.4.8 ipv6 nd dynamic maximum

Command: ipv6 nd dynamic maximum <value>
no ipv6 nd dynamic maximum

Function: Sets the maximum number of dynamic neighbor entries allowed in the VLAN and enables dynamic neighbor number limitation in the VLAN. The **no ipv6 nd dynamic maximum** command disables dynamic neighbor number limitation in the VLAN.

Parameters: <value>: The maximum number of dynamic neighbor entries in the VLAN, ranging from 1 to 4096.

Default: Disabled.

Command Mode: Interface Mode.

Usage Guidelines: If the number of dynamically learned neighbor entries in the VLAN already exceeds the configured maximum, the excess dynamic neighbor entries are deleted.

Example:

Enable dynamic neighbor number limitation in VLAN 1 with a maximum of 50.

```
Switch(config)#interface ethernet
Switch(Config-if-Vlan1)# ipv6 nd dynamic maximum 50
```

Disable dynamic neighbor number limitation in VLAN 1.

```
Switch(Config-if-Vlan1)#no ipv6 nd dynamic maximum
```

7.4.9 mac-address query timeout

Command: mac-address query timeout <seconds>

Function: Sets the timeout for querying dynamic MAC addresses.

Parameters: <seconds> is the timeout, in seconds, ranging from 30 to 300.

Default: 60 seconds.

Command Mode: Global Mode.

Usage Guidelines: After MAC number limitation is enabled, use this command to configure the timeout for querying dynamic MAC addresses. With heavy traffic, use a shorter timeout; otherwise, a longer one. Set it according to the actual situation.

Example:

Set the timeout for querying dynamic MAC addresses to 30 seconds.

```
Switch(config)#mac-address query timeout 30
```

7.4.10 show arp-dynamic count

Command: show arp-dynamic count {(vlan <1-4096>)| interface ethernet <portName>}

Function: Displays the number of dynamic ARP entries on the specified port or VLAN.

Parameters: <1-4096> is the VLAN ID.

<portName> is the Layer 2 port name.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the number of dynamic ARP entries on the specified port or VLAN.

Example: Display the number of dynamic ARP entries on a port and a VLAN configured with ARP number limitation.

```
Switch(config)# show arp-dynamic count interface ethernet 1/0/3
Port           MaxCount            CurrentCount
```

```
------------------------------------------------------------------------------
------------------------
 Ethernet1/0/3            5               1
------------------------------------------------------------------------------
------------------------
Switch(config)# show arp-dynamic count vlan 1
Vlan           MaxCount            CurrentCount
------------------------------------------------------------------------------
------------------------
 1                 55              15
------------------------------------------------------------------------------
------------------------
```

7.4.11 show mac-address dynamic count

Command: show mac-address dynamic count { (vlan <1-4096>)| interface ethernet <portName>}

Function: Displays the number of dynamic MAC addresses on the specified port or VLAN.

Parameters: <1-4096> is the VLAN ID.

<portName> is the Layer 2 port name.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the number of dynamic MAC addresses on the specified port or VLAN.

Example: Display the number of dynamic MAC addresses on a port and a VLAN configured with MAC number limitation.

```
Switch(config)# show mac-address dynamic count interface ethernet 1/0/3
Port           MaxCount            CurrentCount
------------------------------------------------------------------------------
------------------------
 Ethernet1/0/3            5               1
------------------------------------------------------------------------------
------------------------
Switch(config)# show mac-address dynamic count vlan 1
Vlan           MaxCount            CurrentCount
------------------------------------------------------------------------------
------------------------
 1                 55              15
------------------------------------------------------------------------------
------------------------
```

7.4.12 show nd-dynamic count

Command: show nd-dynamic count {(vlan <1-4096>)| interface ethernet <portName>}

Function: Displays the number of dynamic ND entries on the specified port or VLAN.

Parameters: <1-4096> is the VLAN ID. **<portName>** is the Layer 2 port name.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the number of dynamic ND entries on the specified port or VLAN.

Example: Display the number of dynamic ND entries on a port and a VLAN configured with ND number limitation.

```
Switch(config)# show nd-dynamic count interface ethernet 1/0/3
Port           MaxCount            CurrentCount
------------------------------------------------------------------------------
------------------------
 Ethernet1/0/3            5               1
```

```
------------------------------------------------------------------------------
------------------------
Switch(config)# show nd-dynamic count vlan 1
Vlan           MaxCount            CurrentCount
------------------------------------------------------------------------------
------------------------
 1                 55               15
------------------------------------------------------------------------------
------------------------
```

7.4.13 switchport arp dynamic maximum

Command: `switchport arp dynamic maximum <value>`
`no switchport arp dynamic maximum`

Function: Sets the maximum number of dynamic ARP entries allowed on the port and enables dynamic ARP number limitation on the port. The **no switchport arp dynamic maximum** command disables dynamic ARP number limitation on the port.

Parameters: <value>: The maximum number of dynamic ARP entries on the port, ranging from 1 to 4096.

Default: Disabled.

Command Mode: Port Mode.

Usage Guidelines: If the number of dynamically learned ARP entries on the port already exceeds the configured maximum, the excess dynamic ARP entries are deleted. Trunk ports do not support this function.

Example:

Enable dynamic ARP number limitation on port Ethernet 1/0/2 with a maximum of 20.

```
Switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)# switchport arp dynamic maximum 20
```

Disable dynamic ARP number limitation on port Ethernet 1/0/2.

```
Switch(Config-If-Ethernet1/0/2)#no switchport arp dynamic maximum
```

7.4.14 switchport mac-address dynamic maximum

Command: `switchport mac-address dynamic maximum <value>`
`no switchport mac-address dynamic maximum`

Function: Sets the maximum number of dynamic MAC addresses allowed on the port and enables dynamic MAC number limitation on the port. The **no switchport mac-address dynamic maximum** command disables dynamic MAC number limitation on the port.

Parameters: <value>: The maximum number of dynamic MAC addresses on the port, ranging from 1 to 4096.

Default: Disabled.

Command Mode: Port Mode.

Usage Guidelines: If the number of dynamically learned MAC addresses on the port already exceeds the configured maximum, the excess dynamic MAC addresses are deleted. This function is mutually exclusive with functions such as 802.1X and MAC binding; it cannot be enabled on a port where 802.1X, MAC binding, or trunk mode is enabled.

Example:

Enable dynamic MAC number limitation on port Ethernet 1/0/2 with a maximum of 20.

```
Switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)# switchport mac-address dynamic maximum 20
```

Disable dynamic MAC number limitation on port Ethernet 1/0/2.

```
Switch(Config-If-Ethernet1/0/2)#no switchport mac-address dynamic maximum
```

7.4.15 switchport mac-address violation

Command: switchport mac-address violation {protect | shutdown} [recovery <5-3600>]
no switchport mac-address violation

Function: Sets the violation mode of the port. The **no** form of this command restores protect mode.

Parameters: protect: Protect mode.

shutdown: Shutdown mode.

recovery: Configures the port to recover automatically after it is shut down by the shutdown violation mode.

<5-3600>: The recovery time in seconds. By default, the port does not recover automatically.

Command Mode: Port Mode.

Default: Protect mode.

Usage Guidelines: The violation mode applies only after MAC number limitation is enabled on the port. In protect mode, the port only stops learning dynamic MAC addresses when the number of MAC addresses exceeds the limit. In shutdown mode, the port is disabled when the number of MAC addresses exceeds the limit; it can be re-enabled manually with **no shutdown** or automatically when the recovery time expires.

Example: Set the violation mode of port Ethernet 1/0/1 to shutdown with a recovery time of 60 seconds.

```
Switch(config)#interface Ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#switchport mac-address violation shutdown
recovery 60
```

7.4.16 switchport nd dynamic maximum

Command: switchport nd dynamic maximum <value>
no switchport nd dynamic maximum

Function: Sets the maximum number of dynamic neighbor entries allowed on the port and enables dynamic neighbor number limitation on the port. The **no switchport nd dynamic maximum** command disables dynamic neighbor number limitation on the port.

Parameters: <value>: The maximum number of dynamic neighbor entries on the port, ranging from 1 to 4096.

Default: Disabled.

Command Mode: Port Mode.

Usage Guidelines: If the number of dynamically learned neighbor entries on the port already exceeds the configured maximum, the excess dynamic neighbor entries are deleted. Trunk ports do not support this function.

Example:

Enable dynamic neighbor number limitation on port Ethernet 1/0/2 with a maximum of 20.

```
Switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)# switchport nd dynamic maximum 20
```

Disable dynamic neighbor number limitation on port Ethernet 1/0/2.

```
Switch(Config-If-Ethernet1/0/2)#no switchport nd dynamic maximum
```

7.4.17 vlan mac-address dynamic maximum

Command: `vlan mac-address dynamic maximum <value>`
`no vlan mac-address dynamic maximum`

Function: Sets the maximum number of dynamic MAC addresses allowed in the VLAN and enables dynamic MAC number limitation in the VLAN. The **no vlan mac-address dynamic maximum** command disables dynamic MAC number limitation in the VLAN.

Parameters: <value>: The maximum number of MAC addresses in the VLAN, ranging from 1 to 4096.

Default: Disabled.

Command Mode: VLAN Mode.

Usage Guidelines: If the number of dynamically learned MAC addresses in the VLAN already exceeds the configured maximum, the excess dynamic MAC addresses are deleted. After dynamic MAC number limitation is enabled in the VLAN, the limit applies only to ordinary access ports; MAC addresses on trunk ports and on ports with 802.1X or MAC binding enabled are neither limited nor counted.

Example: Enable dynamic MAC number limitation in VLAN 1 with a maximum of 50.

```
Switch(config)#vlan1
Switch(Config-if-Vlan1)#vlan mac-address dynamic maximum 50
```

Disable dynamic MAC number limitation in VLAN 1.

```
Switch(Config-if-Vlan1)#no vlan mac-address dynamic maximum
```

7.5 AM

7.5.1 am enable

Command: `am enable`
`no am enable`

Function: Enables or disables AM globally.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: None.

Example: Enable AM on the switch.

```
Switch(config)#am enable
```

Disable AM on the switch.

```
Switch(config)#no am enable
```

7.5.2 am port

Command: `am iport`
`no am port`

Function: Enables or disables AM on the port.

Parameters: None.

Default: AM is disabled on all ports.

Command Mode: Port Mode.

Example: Enable AM on interface Ethernet 1/0/3.

```
Switch(Config-If-Ethernet 1/0/3)#am port
```

Disable AM on interface Ethernet 1/0/3.

```
Switch(Config-If-Ethernet 1/0/3)#no am port
```

7.5.3 am ip-pool

Command: `am ip-pool <ip-address> <num>`
`no am ip-pool <ip-address> <num>`

Function: Configures an AM IP address range on the interface, which allows IP or ARP packets with source IP addresses in the range to be forwarded through the interface.

Parameters: <ip-address> is the first address of the range in the IP address pool. **<num>** is the number of consecutive addresses starting from ip-address, up to 32.

Default: The IP address pool is empty.

Command Mode: Port Mode.

Usage Guidelines: None.

Example: Configure interface Ethernet 1/0/3 to forward packets from the 10 consecutive IP addresses starting at 10.10.10.1.

```
Switch(Config-If-Ethernet 1/0/3)#am ip-pool 10.10.10.1 10
```

7.5.4 am mac-ip-pool

Command: `am mac-ip-pool <mac-address> <ip-address>`
`no am mac-ip-pool <mac-address> <ip-address>`

Function: Configures an AM MAC-IP address binding on the interface, which allows IP or ARP packets with the specified source MAC and IP address to be forwarded through the interface.

Parameters: <mac-address> is the source MAC address. **<ip-address>** is the source IP address of the packets, in dotted decimal notation.

Default: The MAC-IP address pool is empty.

Command Mode: Port Mode.

Usage Guidelines: None.

Example: Configure interface Ethernet 1/0/3 to forward packets with source MAC address 11-22-22-11-11-11 and source IP address 10.10.10.1.

```
Switch(Config-If-Ethernet1/0/3)#am mac-ip-pool 11-22-22-11-11-11 10.10.10.1
```

7.5.5 no am all

Command: `no am all [ip-pool | mac-ip-pool]`

Function: Deletes all configured MAC-IP address pools, IP address pools, or both.

Parameters: ip-pool: The IP address pool. **mac-ip-pool**: The MAC-IP address pool. If no parameter is specified, both pools are deleted.

Default: Both address pools are empty.

Command Mode: Global Mode.

Usage Guidelines: None.

Example: Delete all configured IP address pools.

```
Switch(config)#no am all ip-pool
```

7.5.6 show am

Command: `show am [interface <interface-name>]`

Function: Displays the configured AM entries.

Parameters: <interface-name> is the interface whose configuration is displayed. If omitted, the AM configuration of all interfaces is displayed.

Command Mode: Admin Mode and Configuration Mode.

Example: Display all configured AM entries.

```
Switch#show am
AM is enabled
Interface Ethernet1/0/3
    am interface
    am ip-pool 30.10.10.1  20
Interface Ethernet1/0/5
    am port
    am ip-pool 50.10.10.1  30
    am mac-ip-pool  00-02-04-06-08-09 20.10.10.5
    am ip-pool 50.20.10.1  20
Interface Ethernet1/0/6
    am port
Interface Ethernet1/0/1
    am interface
    am ip-pool 10.10.10.1  20
    am ip-pool 10.20.10.1  20
```

Display the AM configuration entries of Ethernet 1/0/5.

```
Switch#show am interface ethernet 1/0/5
AM is enabled
Interface Etherne1/0/5
    am interface
    am ip-pool 50.10.10.1  30
    am mac-ip-pool  00-02-04-06-08-09 20.10.10.5
am ip-pool 50.20.10.1  20
```

7.6 Security Feature

7.6.1 dosattack-check srcip-equal-dstip enable

Command: `[no] dosattack-check srcip-equal-dstip enable`

Function: Enables checking of whether the source IP address equals the destination IP address. The **no** form of this command disables this function.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: With this function enabled, packets whose source IP address equals the destination IP address are dropped.

Example: Drop packets whose source IP address equals the destination IP address.

```
Switch(config)# dosattack-check srcip-equal-dstip enable
```

7.6.2 dosattack-check tcp-flags enable

Command: `[no] dosattack-check tcp-flags enable`

Function: Enables checking for invalid TCP flags. The **no** form of this command disables this function.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: With this function enabled, the switch drops the following four types of packets with invalid TCP flags: SYN = 1 with a source port lower than 1024; all TCP flags 0 with sequence number 0; FIN = 1, URG = 1, and PSH = 1 with sequence number 0; and SYN = 1 with FIN = 1.

Example: Drop one or more of the four packet types above.

```
Switch(config)#dosattack-check tcp-flags enable
```

7.6.3 dosattack-check srcport-equal-dstport enable

Command: `dosattack-check srcport-equal-dstport enable`
`no dosattack-check srcport-equal-dstport enable`

Function: Enables checking of whether the source port equals the destination port. The **no** form of this command disables this function.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: With this function enabled, the switch drops TCP and UDP packets whose destination port equals the source port.

Example: Drop non-fragmented TCP and UDP packets whose destination port equals the source port.

```
Switch(config)#dosattack-check srcport-equal-dstport enable
```

7.6.4 dosattack-check icmp-attacking enable

Command: `[no] dosattack-check icmp-attacking enable`

Function: Enables ICMP fragment attack checking. The **no** form of this command disables this function.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: With this function enabled, the switch is protected against ICMP fragment attacks by dropping fragmented ICMPv4/v6 packets whose payload length is less than the specified value.

Example: Enable ICMP fragment attack checking.

```
Switch(config)#dosattack-check icmp-attacking enable
```

7.6.5 invalid-dip-drop

Command: `invalid-dip-drop {enable|disable}`

Function: Checks IPv4 destination addresses for invalid values. Packets with invalid destination IP addresses are dropped and sent to the CPU, where the information is recorded.

Parameters: enable: Enables the function. **disable**: Disables the function.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Invalid destination IP addresses include X.X.X.0, 127.X.X.X, and 240.0.0.0 to 255.255.255.254.

Example: Enable the function.

```
Switch(config)#invalid-dip-drop enable
```

7.7 TACACS+

7.7.1 tacacs-server authentication host

Command: **tacacs-server authentication host {{vrf <vrf-name>| } <ip-address>} [port <port-number>] [timeout <seconds>] [key {0 | 7} <string>] [primary]**

no tacacs-server authentication host <ip-address>

Function: Configures the IP address, listening port, timeout, and key of a TACACS+ server. The **no** form of this command deletes the TACACS+ authentication server.

Parameters: **<vrf-name>** is the VRF name. **<ip-address>** is the IP address of the server. **<port-number>** is the listening port of the server, ranging from 0 to 65535; 0 means the server is not used for authentication. **<seconds>** is the TACACS+ authentication timeout, in seconds, ranging from 1 to 60. **<string>** is the key: with key option 0, the key is unencrypted; with key option 7, the key is encrypted. In both cases, it can be up to 64 characters long. **primary** specifies the primary server.

Command Mode: Global Mode.

Default: No TACACS+ authentication server is configured.

Usage Guidelines: Specifies the IP address, port number, timeout, and key of the TACACS+ server used to authenticate users of the switch. The port must match the authentication port of the TACACS+ server, which is 49 by default. The key and timeout parameters configure a server-specific key and timeout; if they are not configured, the switch uses the global values configured with **tacacs-server timeout <seconds>** and **tacacs-server key <string>**. Several TACACS+ servers can be configured; they are used for authentication in the order in which they are configured. If **primary** is configured on a TACACS+ server, that server is the primary server.

Example: Set the TACACS+ authentication server address to 192.168.1.2 and use the global key.

```
Switch(config)#tacacs-server authentication host 192.168.1.2
```

7.7.2 tacacs-server key

Command: **tacacs-server key {0 | 7} <string>**

no tacacs-server key

Function: Configures the TACACS+ server key. The **no tacacs-server key** command deletes the key.

Parameters: **<string>** is the key of the TACACS+ server. With key option 0, the key is unencrypted; with key option 7, the key is encrypted. In both cases, it can be up to 64 characters long.

Command Mode: Global Mode.

Usage Guidelines: The key is used to encrypt communication between the switch and the TACACS+ server. It must match the key configured on the TACACS+ server; otherwise, TACACS+ authentication fails. Configuring the key is recommended to ensure data security.

Example: Set the TACACS+ server key to test.

```
Switch(config)#tacacs-server key 0 test
```

7.7.3 tacacs-server nas-ipv4

Command: `tacacs-server nas-ipv4 <ip-address>`
`no tacacs-server nas-ipv4`

Function: Configures the source IP address of TACACS+ packets sent by the switch. The **no tacacs-server nas-ipv4** command deletes the configuration.

Parameters: <ip-address> is the source IP address of TACACS+ packets, in dotted decimal notation. It must be a valid unicast IP address.

Default: No source IP address is configured; the address of the interface that sends the TACACS+ packets is used.

Command Mode: Global Mode.

Usage Guidelines: The source IP address must belong to an IP interface of the switch; otherwise, an address binding failure message is returned when the switch sends TACACS+ packets. Using the loopback interface address as the source address is recommended, so that packets from the TACACS+ server are not dropped when an interface link goes down.

Example: Set the source IP address of TACACS+ packets to 192.168.2.254.

```
Switch#tacacs-server nas-ipv4 192.168.2.254
```

7.7.4 tacacs-server timeout

Command: `tacacs-server timeout <seconds>`
`no tacacs-server timeout`

Function: Configures the TACACS+ server authentication timeout. The **no tacacs-server timeout** command restores the default.

Parameters: <seconds> is the TACACS+ authentication timeout, in seconds, ranging from 1 to 60.

Command Mode: Global Mode.

Default: 3 seconds.

Usage Guidelines: Specifies how long the switch waits for authentication through the TACACS+ server. After sending an authentication request to the TACACS+ server, the switch waits for a response; if no response is received within this time, authentication fails.

Example: Set the TACACS+ server timeout to 30 seconds.

```
Switch(config)#tacacs-server timeout 30
```

7.7.5 debug tacacs-server

Command: `debug tacacs-server`
`no debug tacacs-server`

Function: Enables TACACS+ debugging. The **no debug tacacs-server** command disables it.

Command Mode: Admin Mode.

Parameters: None.

Usage Guidelines: TACACS+ debugging shows the TACACS+ protocol negotiation process, which can help diagnose faults.

Example: Enable TACACS+ debugging.

```
Switch#debug tacacs-server
```

7.8 RADIUS

7.8.1 aaa enable

Command: `aaa enable`
`no aaa enable`

Function: Enables AAA authentication on the switch. The **no aaa enable** command disables AAA authentication.

Command Mode: Global Mode.

Parameters: None.

Default: Disabled.

Usage Guidelines: AAA authentication must be enabled on the switch before IEEE 802.1X authentication can be enabled.

Example: Enable AAA on the switch.

```
Switch(config)#aaa enable
```

7.8.2 aaa-accounting enable

Command: `aaa-accounting enable`
`no aaa-accounting enable`

Function: Enables AAA accounting on the switch. The **no aaa-accounting enable** command disables AAA accounting.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: When accounting is enabled, the switch performs accounting based on the traffic or online time of the port used by the authenticated user. The switch sends an Accounting-Start message to the RADIUS accounting server when accounting starts, sends accounting packets for online users to the RADIUS accounting server every five seconds, and sends an Accounting-Stop message when accounting ends. Note: The switch sends the user-offline message to the RADIUS accounting server only when accounting is enabled; the message is not sent to the RADIUS authentication server.

Example: Enable AAA accounting on the switch.

```
Switch(config)#aaa-accounting enable
```

7.8.3 aaa-accounting update

Command: `aaa-accounting update {enable | disable}`

Function: Enables or disables AAA interim accounting updates.

Command Mode: Global Mode.

Default: Enabled.

Usage Guidelines: When interim accounting updates are enabled, the switch periodically sends accounting messages for each online user.

Example: Disable AAA interim accounting updates on the switch.

```
Switch(config)#aaa-accounting update disable
```

7.8.4 debug aaa packet

Command: debug aaa packet {send | receive | all} interface {ethernet <interface-number> | <interface-name>}
no debug aaa packet {send | receive | all} interface {ethernet <interface-number> | <interface-name>}

Function: Enables AAA packet debugging for sent and received packets. The **no** form of this command disables this debugging.

Parameters: send: Debugging of packets sent by AAA.

receive: Debugging of packets received by AAA.

all: Debugging of packets sent and received by AAA.

<interface-number>: The interface number.

<interface-name>: The interface name.

Command Mode: Admin Mode.

Usage Guidelines: AAA packet debugging shows the RADIUS messages sent and received, which can help diagnose faults.

Example: Enable AAA packet debugging for sent and received packets on interface Ethernet 1/0/1.

```
Switch#debug aaa packet all interface Ethernet 1/0/1
```

7.8.5 debug aaa detail attribute

Command: debug aaa detail attribute interface {ethernet <interface-number> | <interface-name>}
no debug aaa detail attribute interface {ethernet <interface-number> | <interface-name>}

Function: Enables debugging of AAA RADIUS attribute details. The **no** form of this command disables this debugging.

Parameters: <interface-number>: The interface number.

<interface-name>: The interface name.

Command Mode: Admin Mode.

Usage Guidelines: This debugging shows the attribute details of RADIUS messages, which can help diagnose faults.

Example: Enable debugging of AAA RADIUS attribute details on interface Ethernet 1/0/1.

```
Switch#debug aaa detail attribute interface Ethernet 1/0/1
```

7.8.6 debug aaa detail connection

Command: debug aaa detail connection
no debug aaa detail connection

Function: Enables debugging of AAA connection details. The **no** form of this command disables this debugging.

Parameters: None.

Command Mode: Admin Mode.

Usage Guidelines: This debugging shows AAA connection details, which can help diagnose faults.

Example: Enable debugging of AAA connection details.

```
Switch#debug aaa detail connection
```

7.8.7 debug aaa detail event

Command: **`debug aaa detail event`**
`no debug detail event`

Function: Enables debugging of AAA events. The **no** form of this command disables this debugging.

Parameters: None.

Command Mode: Admin Mode.

Usage Guidelines: This debugging shows the events generated during RADIUS protocol operation, which can help diagnose faults.

Example: Enable debugging of AAA events.

```
Switch#debug aaa detail event
```

7.8.8 debug aaa error

Command: **`debug aaa error`**
`no debug error`

Function: Enables debugging of AAA errors. The **no** form of this command disables this debugging.

Parameters: None.

Command Mode: Admin Mode.

Usage Guidelines: This debugging shows the errors that occur during RADIUS protocol operation, which can help diagnose faults.

Example: Enable debugging of AAA errors.

```
Switch#debug aaa error
```

7.8.9 radius nas-ipv4

Command: **`radius nas-ipv4 <ip-address>`**
`no radius nas-ipv4`

Function: Configures the source IP address of RADIUS packets sent by the switch. The **no radius nas-ipv4** command deletes the configuration.

Parameters: **<ip-address>** is the source IP address of RADIUS packets, in dotted decimal notation. It must be a valid unicast IP address.

Default: No source IP address is configured; the address of the interface that sends the RADIUS packets is used.

Command Mode: Global Mode.

Usage Guidelines: The source IP address must belong to an IP interface of the switch; otherwise, an address binding failure message is returned when the switch sends RADIUS packets. Using the loopback interface address as the source address is recommended, so that packets from the RADIUS server are not dropped when an interface link goes down.

Example: Set the source IP address of RADIUS packets to 192.168.2.254.

```
Switch#radius nas-ipv4 192.168.2.254
```

7.8.10 radius nas-ipv6

Command: **`radius nas-ipv6 <ipv6-address>`**
`no radius nas-ipv6`

Function: Configures the source IPv6 address of RADIUS packets sent by the switch. The **no** form of this command deletes the configuration.

Parameters: <ipv6-address> is the source IPv6 address of RADIUS packets. It must be a valid unicast IPv6 address.

Default: No source IPv6 address is configured; the IPv6 address of the interface that sends the RADIUS packets is used.

Command Mode: Global Mode.

Usage Guidelines: The source IPv6 address must belong to an IPv6 interface of the switch; otherwise, an address binding failure message is returned when the switch sends RADIUS packets. Using the loopback interface address as the source address is recommended, so that packets from the RADIUS server are not dropped when an interface link goes down.

Example: Set the source IPv6 address of RADIUS packets to 2001:da8:456::1.

```
Switch#radius nas-ipv6 2001:da8:456::1
```

7.8.11 radius-server accounting host

Command: radius-server accounting host (vrf <vrfname>){<ipv4-address> | <ipv6-address>} [port <port-number>] [key {0 | 7} <string>] [primary]
no radius-server accounting host {<ipv4-address> | <ipv6-address>}

Function: Specifies the IPv4/IPv6 address and port number of a RADIUS accounting server and whether it is the primary server. The **no** form of this command deletes the RADIUS accounting server.

Parameters: <ipv4-address> | <ipv6-address>: The IPv4 or IPv6 address of the server.

<port-number>: The listening port of the server, ranging from 0 to 65535.

<vrfname>: The VRF instance name.

<string>: The key. With key option 0, the key is unencrypted; with key option 7, the key is encrypted. In both cases, it can be up to 64 characters long.

primary: Specifies the primary server. Multiple RADIUS servers can be configured. If no primary server is configured, RADIUS servers are used in the order in which they are configured; otherwise, the primary server is used first.

Command Mode: Global Mode.

Default: No RADIUS accounting server is configured.

Usage Guidelines: Specifies the IPv4/IPv6 address and port number of a RADIUS server used for switch accounting; the command can be configured multiple times. The **<port-number>** parameter specifies the accounting port, which must match the accounting port on the RADIUS server; the default is 1813. If the port is set to 0, a random accounting port is generated, which can make the configuration invalid. When several RADIUS servers are configured, the switch sends accounting packets to all of them, and they back each other up. If **primary** is specified, the server is the primary server. Only one primary RADIUS server can be configured, whether it uses an IPv4 or IPv6 address.

Example: Set the RADIUS accounting server to IPv6 address 2004:1:2:3::2, as the primary server, with accounting port 3000.

```
Switch(config)#radius-server accounting host 2004:1:2:3::2 port 3000 primary
```

7.8.12 radius-server authentication host

Command: **radius-server authentication host {{vrf <vrf-name>| }<ipv4-address> | <ipv6-address>} [port <port-number>] [key {0 | 7} <string>] [primary] [access-mode {dot1x | telnet}]**

no radius-server authentication host {<ipv4-address> | <ipv6-address>}

Function: Specifies the IPv4 or IPv6 address, listening port, key, primary status, and access mode of a RADIUS authentication server. The **no** form of this command deletes the RADIUS authentication server.

Parameters: **<vrf-name>**: The VRF name.

<ipv4-address> | <ipv6-address>: The IPv4 or IPv6 address of the server.

<port-number>: The listening port, ranging from 0 to 65535; 0 means the server is not used for authentication.

<string>: The key. With key option 0, the key is unencrypted; with key option 7, the key is encrypted. In both cases, it can be up to 64 characters long.

primary: Specifies the primary server. Multiple RADIUS servers can be configured. If no primary server is configured, RADIUS servers are used in the order in which they are configured; otherwise, the primary server is used first.

access-mode {dot1x | telnet}: Restricts the RADIUS server to 802.1X authentication or Telnet authentication only. By default, all services can use the RADIUS server.

Command Mode: Global Mode.

Default: No RADIUS authentication server is configured.

Usage Guidelines: Specifies the IPv4 or IPv6 address, port number, key, and access mode of a RADIUS server used for switch authentication; the command can be configured multiple times. The port must match the authentication port on the RADIUS server; the default is 1812. If the port is set to 0, the server is not used for authentication. When several RADIUS servers are configured, the configuration order is the priority order of the authentication servers. Once a server responds (whether authentication succeeds or fails), the switch does not send the request to the next server. If **primary** is specified, the server is the primary server. If no key is configured for the server, the global key configured with **radius-server key <string>** is used. The **access-mode** option restricts the server to 802.1X or Telnet authentication; if it is not configured, all services can use the server.

Example: Set the RADIUS authentication server address to 2004:1:2:3::2.

```
Switch(config)#radius-server authentication host 2004:1:2:3::2
```

7.8.13 radius-server dead-time

Command: **radius-server dead-time <minutes>**

no radius-server dead-time

Function: Configures how long a RADIUS server is considered down before it is restored. The **no radius-server dead-time** command restores the default.

Parameters: **<minutes>** is the restore time of the RADIUS server, in minutes, ranging from 1 to 255.

Command Mode: Global Mode.

Default: 5 minutes.

Usage Guidelines: Specifies how long to wait before an unreachable RADIUS server is considered reachable again. When the switch determines that a server is unreachable, it marks the server as invalid; after the interval specified by this command, the server is marked valid again.

Example: Set the RADIUS server restore time to 3 minutes.

```
Switch(config)#radius-server dead-time 3
```

7.8.14 radius-server key

Command: `radius-server key {0 | 7} <string>`
`no radius-server key`

Function: Specifies the key for RADIUS servers (authentication and accounting). The **no radius-server key** command deletes the key.

Parameters: <string> is the RADIUS server key. With key option 0, the key is unencrypted; with key option 7, the key is encrypted. In both cases, it can be up to 64 characters long.

Command Mode: Global Mode.

Usage Guidelines: The key is used to encrypt communication between the switch and the RADIUS server. It must match the key configured on the RADIUS server; otherwise, RADIUS authentication and accounting do not work properly.

Example: Set the RADIUS key to test.

```
Switch(config)#radius-server key 0 test
```

7.8.15 radius-server retransmit

Command: `radius-server retransmit <retries>`
`no radius-server retransmit`

Function: Configures the number of retransmissions of RADIUS authentication packets. The **no radius-server retransmit** command restores the default.

Parameters: <retries> is the number of retransmissions, ranging from 0 to 100.

Command Mode: Global Mode.

Default: 3.

Usage Guidelines: Specifies how many times a packet is retransmitted when the RADIUS server does not respond. If the authentication server does not respond, the AAA authentication request is retransmitted. If the number of retransmissions reaches the limit without a response, the server is considered down and marked invalid.

Example: Set the number of RADIUS authentication packet retransmissions to 5.

```
Switch(config)#radius-server retransmit 5
```

7.8.16 radius-server timeout

Command: `radius-server timeout <seconds>`
`no radius-server timeout`

Function: Configures the RADIUS server timeout. The **no radius-server timeout** command restores the default.

Parameters: <seconds> is the RADIUS server timeout, in seconds, ranging from 1 to 1000.

Command Mode: Global Mode.

Default: 3 seconds.

Usage Guidelines: Specifies how long the switch waits for a RADIUS server response. After sending a request to the RADIUS server, the switch waits for the response; if no response arrives within this time, the switch resends the request or marks the server invalid, depending on the conditions.

Example: Set the RADIUS server timeout to 30 seconds.

```
Switch(config)#radius-server timeout 30
```

7.8.17 radius-server accounting-interim-update timeout

Command: `radius-server accounting-interim-update timeout <seconds>`
`no radius-server accounting-interim-update timeout`

Function: Sets the interval at which accounting update (interim update) messages are sent. The **no** form of this command restores the default.

Parameters: <seconds> is the interval between accounting update messages, in seconds, ranging from 60 to 3600.

Command Mode: Global Mode.

Default: 300 seconds.

Usage Guidelines: Sets the interval at which the NAS sends accounting update messages. To support real-time accounting, the NAS sends an accounting update message for each user to the RADIUS server at this interval, starting when the user comes online.

The accounting update interval is related to the maximum number of users supported by the NAS: the shorter the interval, the fewer users the NAS supports; the longer the interval, the more users it supports. The recommended intervals for different maximum numbers of users are as follows:

Recommended accounting update intervals by maximum number of NAS users

Maximum number of users	Accounting update interval (seconds)
1-299	300 (default)
300-599	600
600-1199	1200
1200-1799	1800
≥1800	3600

Example: The NAS supports a maximum of 700 users; set the accounting update interval to 1200 seconds.

```
Switch(config)#radius-server accounting-interim-update timeout 1200
```

7.8.18 show aaa authenticated-user

Command: `show aaa authenticated-user`

Function: Displays the authenticated online users.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Administrators normally need only the online user information; the other information is for troubleshooting by technical support.

Example:

```
Switch#show aaa authenticated-user
------------------------- authenticated users ------------------------------
 UserName  Retry RadID Port EapID ChapID OnTime    UserIP         MAC
--------------------------------------------------------------------------------
         -------------- total: 0 ---------------
```

7.8.19 show aaa authenticating-user

Command: `show aaa authenticating-user`

Function: Displays the users being authenticated.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Administrators normally need only the information about users being authenticated; the other information is for troubleshooting by technical support.

Example:

```
Switch#show aaa authenticating-user
```

```
------------------------ authenticating users -----------------------------
   User-name   Retry-time  Radius-ID   Port  Eap-ID Chap-ID Mem-Addr   State
--------------------------------------------------------------------------------
          -------------- total: 0 --------------
```

7.8.20 show aaa config

Command: `show aaa config`

Function: Displays the RADIUS client configuration of the switch.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays whether AAA authentication and accounting are enabled, the key, and the configured authentication and accounting servers.

Example: In the output, Boolean values are shown as 1 (TRUE) and 0 (FALSE). The text after each colon is an explanatory annotation, not device output.

```
Switch#show aaa config
----------------- AAA config data ------------------
    Is Aaa Enabled = 1     :1 means AAA authentication is enabled; 0 means it
is not enabled
    Is Account Enabled= 1   :1 means AAA accounting is enabled; 0 means it is
not enabled
    MD5 Server Key = yangshifeng   :Authentication key
    authentication server sum = 2     :Number of configured authentication
servers
    authentication server[0].sock_addr = 2:100.100.100.60.1812  :Address
family, IP address, and port of the first authentication server
                              .Is Primary = 1     :Whether the server is the
primary server
                              .Is Server Dead = 0  :Whether the server is down
                              .Socket No = 0  :Local socket number used for
this server
    authentication server[1].sock_addr = 10:2004:1:2::2.1812
                              .Is Primary = 0
                              .Is Server Dead = 0
                              .Socket No = 0
    accounting server sum = 2  :Number of configured accounting servers
    accounting server[0].sock_addr = 2:100.100.100.65.1813  :Address family,
IP address, and port of the accounting server
                               .Is Primary = 1    :Whether the server is the
primary server
                               .Is Server Dead = 0  :Whether the server is
down
                               .Socket No = 0   :Local socket number used for
this server
accounting server[1].sock_addr = 10:2004::7.1813
                              .Is Primary = 1
                              .Is Server Dead = 0
                              .Socket No = 0
    Time Out = 5s  :Response timeout after a request packet is sent
    Retransmit = 3  :Number of retransmissions
    Dead Time = 5min  :Restore interval of a down server
Account Time Interval = 0min  :Accounting interval
```

7.8.21 show radius authenticated-user count

Command: `show radius authenticated-user count`

Function: Displays the number of online users that have passed authentication.

Parameters: None.

Command Mode: Admin Mode and Configuration Mode.

Default: None.

Usage Guidelines: None.

Example:

```
Switch#show radius authenticated-user count
The authenticated online user num is:     105
```

7.8.22 show radius authenticating-user count

Command: `show radius authenticating-user count`

Function: Displays the number of users being authenticated.

Parameters: None.

Command Mode: Admin Mode and Configuration Mode.

Default: None.

Usage Guidelines: None.

Example:

```
Switch#show radius authenticating-user count
The authenticating user num is:       10
```

7.8.23 show radius count

Command: `show radius {authenticated-user|authenticating-user} count`

Function: Displays RADIUS authentication user statistics.

Parameters: authenticated-user: Displays the authenticated online users. **authenticating-user**: Displays the users being authenticated.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Use **show radius count** to display RADIUS authentication user statistics.

Example:

Example 1: Display statistics for RADIUS authenticated users.

```
Switch#show radius authenticated-user count
The authenticated online user num is:     0
```

Example 2: Display statistics for RADIUS users being authenticated.

```
Switch#show radius authenticating-user count
```

7.8.24 Radius Escaping

7.8.24.1 radius-server escape { enable | disable}

Command: `radius-server escape enable`
`radius-server escape disable`

Function: Enables or disables the AAA RADIUS server escape function.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: With RADIUS server escape enabled, traffic from 802.1X or portal authentication clients is allowed when the RADIUS server configured for them is unreachable. When the authentication server becomes reachable again, the rule that allows the traffic is deleted.

Example: Enable RADIUS server escape.

```
Switch (Config)# radius-server escape enable
```

7.8.24.2 radius-server escape detection-interval

Command: `radius-server escape detection-interval {default| < second >)}`

Function: Configures the detection interval for RADIUS server escape.

Parameters: default: The default interval, 3 minutes.

<second>: The interval, ranging from 1 to 1800 seconds.

Default: 180 seconds.

Command Mode: Global Mode.

Usage Guidelines: The shorter the interval, the more responsive the RADIUS server escape function. The interval must be longer than (Retransmit + 1) × Time Out.

Example: Set the RADIUS server escape detection interval to 120 seconds.

```
Switch(config)#radius-server escape detection-interval 120
```

7.9 SSL

7.9.1 ip http secure-server

Command: `ip http secure-server`
`no ip http secure-server`

Function: Enables or disables SSL.

Parameters: None.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: Enables or disables SSL. With SSL enabled, users access the switch through an HTTPS client, and the switch and client establish a secure SSL channel. All application-layer data is then encrypted, ensuring the privacy of the communication.

Example: Enable SSL.

```
Switch(config)#ip http secure-server
```

7.9.2 ip http secure-port

Command: `ip http secure-port <port-number>`
`no ip http secure-port`

Function: Configures or deletes the port number used by SSL.

Parameters: <port-number> is the port number, ranging from 1025 to 65535. The default is 443.

Command Mode: Global Mode.

Default: Not configured (port 443 is used).

Usage Guidelines: If a port number is configured with this command, the switch listens on that port. If the HTTPS port is changed, users must specify the new port when connecting over HTTPS, for example, https://device:port_number. SSL must be restarted after each change.

Example: Set the port number to 1028.

```
Switch(config)#ip http secure-port 1028
```

7.9.3 ip http secure- ciphersuite

Command: ip http secure-ciphersuite {aes128-gcm-sha256|aes128-sha|aes128-sha256|aes256-sha|aes256-sha256|ecdhe-rsa-aes128-gcm-sha256|ecdhe-rsa-aes128-sha|ecdhe-rsa-aes256-sha}
no ip http secure-ciphersuite

Function: Configures or deletes the cipher suite used by SSL.

Parameters: aes128-gcm-sha256: Encryption algorithm AES128-GCM with hash algorithm SHA256.

aes128-sha: Encryption algorithm AES128 with hash algorithm SHA.

aes128-sha256: Encryption algorithm AES128 with hash algorithm SHA256.

aes256-sha: Encryption algorithm AES256 with hash algorithm SHA.

aes256-sha256: Encryption algorithm AES256 with hash algorithm SHA256.

ecdhe-rsa-aes128-gcm-sha256: Encryption algorithm ECDHE-RSA-AES128-GCM with hash algorithm SHA256.

ecdhe-rsa-aes128-sha: Encryption algorithm ECDHE-RSA-AES128 with hash algorithm SHA.

ecdhe-rsa-aes256-sha: Encryption algorithm ECDHE-RSA-AES256 with hash algorithm SHA.

Command Mode: Global Mode.

Default: Not configured.

Usage Guidelines: If a cipher suite is configured with this command, the specified encryption method is used. SSL must be restarted for configuration changes to take effect. When des-cbc-sha is configured, Internet Explorer 7.0 or later is required.

Example: Set the cipher suite to rc4-128-sha.

```
Switch(config)# ip http secure- ciphersuite rc4-128-sha
```

7.9.4 show ip http secure-server status

Command: show ip http secure-server status

Function: Displays the SSL configuration status.

Parameters: None.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch# show ip http secure-server status
HTTP secure server status: Enabled
HTTP secure server port: 1028
HTTP secure server ciphersuite: rc4-128-sha
```

7.9.5 debug ssl

Command: debug ssl
no debug ssl

Function: Enables SSL debugging. The **no** form of this command disables it.

Parameters: None.

Command Mode: Admin Mode.

Example:

```
Switch# debug ssl
%Jan 01 01:02:05 2006 ssl will to connect to web server 127.0.0.1:9998
%Jan 01 01:02:05 2006 connect to http security server success!
```

7.10 VLAN-ACL

7.10.1 clear vacl statistic vlan

Command: `clear vacl [in | out] statistic vlan [<1-4094>]`

Function: Clears VACL statistics.

Parameters: in | out: Clears the ingress or egress traffic statistics.

vlan <1-4094>: The VLAN whose VACL statistics are cleared. If no VLAN ID is specified, the statistics of all VLANs are cleared.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: None.

Example:

Clear the VACL statistics of VLAN 1.

```
Switch#clear vacl statistic vlan 1
```

7.10.2 show vacl vlan

Command: `show vacl [in | out] vlan [<1-4094>] | [begin | include | exclude <regular-expression>]`

Function: Displays the VACL configuration and statistics.

Parameters: in | out: Displays the ingress or egress configuration and statistics.

vlan <1-4094>: The VLAN whose VACL configuration and statistics are displayed. If no VLAN ID is specified, the information for all VLANs is displayed.

begin | include | exclude <regular-expression>: Filters the output with a regular expression:

. matches any character except a line feed.

^ matches the beginning of a line.

$ matches the end of a line.

| matches the string on either side of the vertical bar.

[0-9] matches the digits 0 through 9.

[a-z] matches the lowercase letters a through z.

[aeiou] matches any of the letters a, e, i, o, and u.

\ is the escape character, used to match special characters; for example, \$ matches the $ character rather than the end of the string.

\w matches a letter, digit, or underscore.

\b matches the beginning or end of a word.

\W matches any character other than a letter, digit, or underscore.

\B matches a position that is not the beginning or end of a word.

[^x] matches any character except x.

[^aeiou] matches any character except a, e, i, o, and u.

* repeats zero or more times.

+ repeats one or more times.

(n) repeats n times.

(n,) repeats n or more times.

(n, m) repeats n to m times.

The following regular expression syntax is currently not supported:

\s matches a whitespace character.

\d matches a digit.

\S matches any non-whitespace character.

\D matches any non-digit character.

? repeats zero or one time.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: None.

Example:

```
Switch (config)#show vacl vlan 2
Vlan 2:
IP Ingress access-list used is 100, traffic-statistics Disable.
Switch (config)# show vacl vlan 3
Vlan 3:
IP Ingress access-list used is myacl, packet(s) number is 5.
```

Output	Description
Vlan 2	VLAN name
100, myacl	VACL name
traffic-statistics Disable	VACL statistics are disabled.
packet(s) number is 5	Number of packets that matched this VACL

7.10.3 vacl ip access-group

Command: vacl ip access-group {<1-299> | WORD} {in | out} [traffic-statistic] vlan WORD

no vacl ip access-group {<1-299> | WORD} {in | out} vlan WORD

Function: Configures an IP VACL on the specified VLANs.

Parameters: <1-299> | WORD: A numbered IP ACL (standard ACL 1 to 99, extended ACL 100 to 299) or a named ACL.

in | out: Filters ingress or egress traffic.

traffic-statistic: Enables statistics of matched packets.

vlan WORD: The VLANs to which the VACL is bound.

Command Mode: Global Mode.

Default: None.

Usage Guidelines: Use ";" or "-" to enter one or more VLANs; up to 128 VLANs can be entered, and the command line cannot exceed 80 characters. Currently, IP ACLs that match TCP/UDP port ranges cannot be bound to the egress direction of a VLAN.

Example: Bind numbered IP ACL 1 with statistics enabled to VLANs 1-5, 6, and 7-9.

```
Switch(config)#vacl ip access-group 1 in traffic-statistic vlan 1-5; 6; 7-9
```

7.10.4 vacl ipv6 access-group

Command: vacl ipv6 access-group (<500-699> | WORD) {in | out} (traffic-statistic|) vlan WORD

no ipv6 access-group {<500-699> | WORD} {in | out} vlan WORD

Function: Configures an IPv6 VACL on the specified VLANs.

Parameters: <500-699> | WORD: A numbered IPv6 ACL (standard ACL 500 to 599, extended ACL 600 to 699) or a named ACL.

in | out: Filters ingress or egress traffic.

traffic-statistic: Enables statistics of matched packets.

vlan WORD: The VLANs to which the VACL is bound.

Command Mode: Global Mode.

Default: None.

Usage Guidelines: Use ";" or "-" to enter one or more VLANs; up to 128 VLANs can be entered, and the command line cannot exceed 80 characters. Currently, IPv6 ACLs that match the flow label cannot be bound to the egress direction of a VLAN.

Example: Bind numbered IPv6 ACL 600 to VLAN 5.

```
Switch(config)#vacl ipv6 access-group 600 in traffic-statistic vlan 5
```

7.10.5 vacl mac access-group

Command: vacl mac access-group {<700-1199> | WORD} {in | out} [traffic-statistic] vlan WORD
no vacl mac access-group {<700-1199> | WORD} {in | out} vlan WORD

Function: Configures a MAC VACL on the specified VLANs.

Parameters: <700-1199> | WORD: A numbered MAC ACL (standard MAC ACL 700 to 799, extended MAC ACL 1100 to 1199) or a named ACL.

in | out: Filters ingress or egress traffic.

traffic-statistic: Enables statistics of matched packets.

vlan WORD: The VLANs to which the VACL is bound.

Command Mode: Global Mode.

Default: None.

Usage Guidelines: Use ";" or "-" to enter one or more VLANs; up to 128 VLANs can be entered, and the command line cannot exceed 80 characters.

Example: Bind numbered MAC ACL 700 to VLANs 1-5.

```
Switch(config)#vacl mac access-group 700 in traffic-statistic vlan 1-5
```

7.10.6 vacl mac-ip access-group

Command: vacl mac-ip access-group {<3100-3299> | WORD} {in | out} [traffic-statistic] vlan WORD
no vacl mac-ip access-group {<3100-3299> | WORD} {in | out} vlan WORD

Function: Configures a MAC-IP VACL on the specified VLANs.

Parameters: <3100-3299> | WORD: A numbered MAC-IP ACL or a named ACL.

in | out: Filters ingress or egress traffic.

traffic-statistic: Enables statistics of matched packets.

vlan WORD: The VLANs to which the VACL is bound.

Command Mode: Global Mode.

Default: None.

Usage Guidelines: Use ";" or "-" to enter one or more VLANs; up to 128 VLANs can be entered, and the command line cannot exceed 80 characters. Currently, MAC-IP ACLs that match TCP/UDP port ranges cannot be bound to the egress direction of a VLAN.

Example: Bind numbered MAC-IP ACL 3100 to VLANs 1, 2, and 5.

```
Switch(config)#vacl mac-ip access-group 3100 in traffic-statistic vlan 1;2;5
```

7.11 Captive Portal Authentication

7.11.1 Authentication

7.11.1.1 ac-name

Command: `ac-name <word>`
`no ac-name`

Function: Configures the acname parameter in the redirect URL. The **no** form of this command deletes it.

Parameters: <word>: The acname value, up to 32 characters.

Command Mode: Captive Portal Instance Mode.

Default: None.

Usage Guidelines: Some portal servers allow authentication only with a specific acname; configure this parameter as required by the portal server.

Example: Set the acname in the redirect URL to 0100.0010.010.00 as required by a mobile operator portal server, in the format ACN.CTY.PRO.OPE.

```
Switch(config-cp-instance)#ac-name 0100.0010.010.00
```

7.11.1.2 captive-portal

Command: `captive-portal`

Function: Enters Captive Portal Configuration Mode.

Parameters: None.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: Use this command to enter Captive Portal Configuration Mode.

Example: Enter Captive Portal Configuration Mode.

```
Switch(config)#captive-portal
```

7.11.1.3 captive-portal client deauthenticate

Command: `captive-portal client deauthenticate {<1-10> | <FF-FF-FF-FF-FF-FF> { ipv4 | ipv6} <ip-addr>}`

Function: Deauthenticates the specified Captive Portal clients.

Parameters: <1-10> is the Captive Portal configuration ID.

<FF-FF-FF-FF-FF-FF> is the MAC address of the client.

ipv4 specifies an IPv4 user address.

ipv6 specifies an IPv6 user address.

<ip-addr> is the user address: an IPv4 address in dotted decimal notation or an IPv6 address in X:X::X:X format.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Deauthenticates the client with the specified MAC address, all users of the specified Captive Portal configuration, or all users. If no parameter is specified, all users are deauthenticated.

Example: Deauthenticate Captive Portal clients.

```
Switch #captive-portal client deauthenticate    (forces all portal users on
this switch offline)
The specified clients will be deauthenticated. Are you sure you want to
deauthenticated clients?  [Y/N]
Switch #captive-portal client deauthenticate 1    (forces all users of
configuration 1 offline)
Switch #captive-portal client deauthenticate 34-08-04-30-07-ca ipv4 100.1.1.1
(forces one user offline)
```

7.11.1.4 captive-portal client keep-alive flow-detection enable

Command: `captive-portal client keep-alive flow-detection enable`
`no captive-portal client keep-alive flow-detection enable`

Function: Enables user keepalive detection. The **no** form of this command disables this function.

Parameters: None.

Default: Disabled.

Command Mode: Captive Portal Mode.

Usage Guidelines: With this function enabled, the switch keeps online users alive based on traffic detection.

Example: Enable user keepalive detection in Captive Portal Mode.

```
Switch (config-cp)#captive-portal client keep-alive flow-detection enable
```

7.11.1.5 captive-portal client keep-alive flow-detection interval

Command: `captive-portal client keep-alive flow-detection interval <3-120>`
`no captive-portal client keep-alive flow-detection interval`

Function: Configures the user keepalive query interval. The **no** form of this command restores the default.

Parameters: <3-120>: The interval, ranging from 3 to 120 minutes.

Default: 5 minutes.

Command Mode: Captive Portal Mode.

Usage Guidelines: After this command is configured, the keepalive timer queries the online status of users at the configured interval.

Example: Set the user keepalive query interval in Captive Portal Mode.

```
Switch (config-cp)# captive-portal client keep-alive flow-detection interval
3
```

7.11.1.6 captive-portal client keep-alive flow-detection number

Command: `captive-portal client keep-alive flow-detection number <1-10>`
`no captive-portal client keep-alive flow-detection number`

Function: Configures how many consecutive failed queries the keepalive timer allows. The **no** form of this command restores the default.

Parameters: <1-10>: The number of queries, ranging from 1 to 10.

Default: 3 times.

Command Mode: Captive Portal Mode.

Usage Guidelines: The keepalive timer queries the user's online status the configured number of times. If the user is offline in all queries, the user is considered offline; if the user is online in any query, the user is considered online and the count restarts.

Example: Set the number of allowed failed keepalive queries in Captive Portal Mode.

```
Switch (config-cp)# captive-portal client keep-alive flow-detection interval
3
```

7.11.1.7 configuration

Command: `configuration <cp-id>`
`no configuration <cp-id>`

Function: Enters Captive Portal Instance Mode. The **no** form of this command deletes the Captive Portal instance configuration.

Parameters: <cp-id> is the Captive Portal instance number, ranging from 1 to 10.

Default: None.

Command Mode: Captive Portal Mode.

Usage Guidelines: Configures Captive Portal instances. Each instance represents a class of users; users in the same instance share the same traffic and rate settings. The **no** form deletes a Captive Portal configuration; it is rejected if an interface is associated with the instance.

Example: Configure Captive Portal instance 4.

```
Switch(config-cp)#configuration 4
```

7.11.1.8 debug captive-portal packet

Command: `debug captive-portal packet {send|receive|dump|all}`
`no debug captive-portal packet {send|receive|dump|all}`

Function: Enables Captive Portal packet debugging. The **no** form of this command disables it.

Parameters: send: Debugging of packets sent by Captive Portal.

receive: Debugging of packets received by Captive Portal.

dump: Packet parsing (dump) debugging of Captive Portal.

all: Debugging of packets sent, received, and dumped by Captive Portal.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: Enables Captive Portal packet debugging.

Example: Enable all Captive Portal packet debugging.

```
Switch#debug captive-portal packet all
```

7.11.1.9 debug captive-portal trace

Command: `debug captive-portal trace`
`no debug captive-portal trace`

Function: Enables Captive Portal trace debugging. The **no** form of this command disables it.

Parameters: None.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: Enables Captive Portal trace debugging.

Example: Enable Captive Portal trace debugging.

```
Switch#debug captive-portal trace
```

7.11.1.10 debug captive-portal error

Command: debug captive-portal error
no debug captive-portal error

Function: Enables Captive Portal error debugging. The **no** form of this command disables it.

Parameters: None.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: Enables Captive Portal error debugging.

Example: Enable Captive Portal error debugging.

```
Switch#debug captive-portal error
```

7.11.1.11 enable (global)

Command: enable
disable

Function: Enables Captive Portal globally on the switch. The **disable** command disables Captive Portal globally.

Parameters: None.

Default: Disabled.

Command Mode: Captive Portal Mode.

Usage Guidelines: Use this command to enable Captive Portal globally on the switch.

Example: Enable Captive Portal globally on the switch.

```
Switch(config-cp)#enable
```

7.11.1.12 enable (instance)

Command: enable
disable

Function: Enables the Captive Portal configuration (instance). The **disable** command disables it.

Parameters: None.

Default: Enabled.

Command Mode: Captive Portal Instance Mode.

Usage Guidelines: The **disable** command disables the Captive Portal instance; portal users of the instance are then forced offline.

Example: Enable the Captive Portal instance.

```
Switch(config-cp-instance)#enable
```

7.11.1.13 external portal-server server-name

Command: external portal-server server-name <name> {ipv4 | ipv6} <ipaddr> [port <1-65535>]
no external portal-server {ipv4 | ipv6}server-name <name>

Function: Configures an external portal server. The redirect page is provided by this server; after the user enters the correct user name and password, authentication succeeds and the client can access the external network.

Parameters: <name> is the name of the external portal server.

<ipaddr> is the IP address of the external portal server.

ipv4: The portal server address is an IPv4 address.

ipv6: The portal server address is an IPv6 address.

<1-65535> is the port number of the portal server.

Default: None.

Command Mode: Captive Portal Mode.

Usage Guidelines: Up to 10 external portal servers can be configured. Each Captive Portal configuration can be bound to one portal server.

Example: Configure an external portal server.

```
Switch(config-cp)# external portal-server server-name x1 ipv4 1.0.0.1 port
11111
```

7.11.1.14 http-redirect-filter <1-32>

Command: `http-redirect-filter <1-32>`
`no http-redirect-filter <1-32>`

Function: Binds a redirect filter rule to a Captive Portal instance. The **no** form of this command deletes the binding.

Parameters: <1-32>: The rule ID (index).

Default: Not configured.

Command Mode: Captive Portal Instance Mode.

Usage Guidelines: Binds a rule to a Captive Portal instance.

Example: Bind rule 1 to the instance.

```
Switch (config-cp-instance)# http-redirect-filter 1
```

7.11.1.15 name

Command: `name <cp-name>`
`no name`

Function: Defines the name of the Captive Portal configuration.

Parameters: <cp-name>: The name of the Captive Portal configuration, up to 32 characters (letters and digits).

Default: None.

Command Mode: Captive Portal Instance Mode.

Usage Guidelines: Defines the name of the Captive Portal configuration.

Example: Set the name of the Captive Portal configuration to abc123.

```
Switch(config-cp-instance)#name abc123
```

7.11.1.16 nas-ipv4

Command: `nas-ipv4 < A.B.C.D>`
`no nas-ipv4 < A.B.C.D>`

Function: Defines the Captive Portal NAS IPv4 address.

Parameters: <A.B.C.D>: The IPv4 address of the NAS.

Default: None.

Command Mode: Captive Portal Mode.

Usage Guidelines: Defines the Captive Portal NAS IPv4 address.

Example: Set the Captive Portal NAS IPv4 address to 10.1.1.1.

```
Switch (config-cp)#nas-ip 10.1.1.1
```

7.11.1.17 nas-ipv6

Command: **`nas-ipv6 <ipv6-address>`**
`no nas-ipv6`

Function: Defines the Captive Portal NAS IPv6 address.

Parameters: <ipv6-address>: The IPv6 address of the NAS.

Default: None.

Command Mode: Captive Portal Mode.

Usage Guidelines: Defines the Captive Portal NAS IPv6 address.

Example: Set the Captive Portal NAS IPv6 address to 2000::1.

```
Switch (config-cp)#nas-ipv6 2000::1
```

7.11.1.18 portal-server

Command: **`portal-server {ipv4 | ipv6} <name>`**
`no portal-server {ipv4 | ipv6}`

Function: Binds an external portal server to the Captive Portal configuration. All networks under this configuration are redirected to this portal server for authentication.

Parameters: <name>: The name of the portal server to bind.

ipv4: The bound portal server address is an IPv4 address.

ipv6: The bound portal server address is an IPv6 address.

Default: None.

Command Mode: Captive Portal Instance Mode.

Usage Guidelines: Use this command to bind an external portal server to the Captive Portal configuration; the **no** form removes the binding.

Example: Bind an external portal server to the Captive Portal configuration.

```
Switch(config-cp -instance)#portal-server ipv4 x1
```

7.11.1.19 radius accounting

Command: **`radius accounting`**
`no radius accounting`

Function: Enables accounting for the Captive Portal instance. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Captive Portal Instance Mode.

Usage Guidelines: Enables accounting for the Captive Portal instance.

Example: Enable accounting for the Captive Portal instance.

```
Switch (config-cp-instance)#radius accounting
```

7.11.1.20 radius-accounting update interval

Command: **`radius-accounting update interval <60-3600>`**
`no radius-accounting update interval`

Function: Configures the interval at which the switch sends accounting updates for portal users to the RADIUS server. The **no** form of this command restores the default.

Parameters: <60-3600> is the interval, in seconds.

Default: 300 seconds.

Command Mode: Captive Portal Instance Mode.

Usage Guidelines: Configures the accounting update interval for portal users.

Example: Set the accounting update interval for portal users to 60 seconds.

```
Switch (config-cp-instance)# radius-accounting update interval 60
```

7.11.1.21 radius-acct-server

Command: `radius-acct-server <server-name>`
`no radius-acct-server`

Function: Defines the RADIUS accounting server of the Captive Portal instance. The **no** form of this command deletes it.

Parameters: <server-name>: The name of the RADIUS accounting server.

Default: None.

Command Mode: Captive Portal Instance Mode.

Usage Guidelines: Defines the RADIUS accounting server of the Captive Portal instance.

Example: Set the RADIUS accounting server of the Captive Portal instance to radius_aaa_1.

```
Switch (config-cp-instance)#radius-acct-server radius_aaa_1
```

7.11.1.22 radius-auth-server

Command: `radius-auth-server <server-name>`
`no radius-auth-server`

Function: Defines the RADIUS authentication server of the Captive Portal configuration. The **no** form of this command deletes the configuration.

Parameters: <server-name>: The name of the RADIUS authentication server.

Default: None.

Command Mode: Captive Portal Instance Mode.

Usage Guidelines: Defines the RADIUS authentication server of the Captive Portal configuration.

Example: Set the RADIUS authentication server of the Captive Portal configuration to radius_aaa_1.

```
Switch(config-cp-instance)#radius-auth-server radius_aaa_1
```

7.11.1.23 redirect url-head <word>

Command: `redirect url-head <word>`
`no redirect url-head`

Function: Configures the redirect URL head, including the protocol, host name, port, and path. The **no** form of this command deletes it.

Parameters: <word>: The redirect URL head, such as https://200.101.13.4:8080/index.jsp or http://www.portal.com/index.jsp, up to 128 characters.

Command Mode: Captive Portal Instance Mode.

Default: None.

Usage Guidelines: Configures the redirect URL head, including the protocol, host name, port, and path, according to the redirect URL of the portal server. The protocol, host name, port, and path must match those of the portal server.

Example: Set the redirect URL head to http://17.16.1.26/control.

```
Switch(config-cp-instance)#redirect url-head http://17.16.1.26/control
```

7.11.1.24 redirect attribute ssid enable

Command: `redirect attribute ssid enable`
`no redirect attribute ssid enable`

Function: Configures the redirect URL to carry the SSID parameter. The **no** form of this command disables this function.

Parameters: None.

Command Mode: Captive Portal Instance Mode.

Default: Disabled.

Usage Guidelines: With this command enabled, the redirect URL carries the SSID associated with the client when the client is redirected.

Example: Configure the redirect URL to carry the SSID parameter.

```
Switch(config-cp-instance)#redirect attribute ssid enable
```

7.11.1.25 redirect attribute ssid name

Command: `redirect attribute ssid name <word>`
`no redirect attribute ssid name`

Function: Configures the name of the SSID parameter carried in the redirect URL. The **no** form of this command restores the default.

Parameters: <word>: The parameter name, up to 32 characters.

Command Mode: Captive Portal Instance Mode.

Default: ssid.

Usage Guidelines: Configures the name of the SSID parameter carried in the redirect URL.

Example: Set the name of the SSID parameter carried in the redirect URL to ssid.

```
Switch(config-cp-instance)#redirect attribute ssid name ssid
```

7.11.1.26 redirect attribute nas-ip enable

Command: `redirect attribute nas-ip enable`
`no redirect attribute nas-ip enable`

Function: Configures the redirect URL to carry the NAS IP parameter. The **no** form of this command disables this function.

Parameters: None.

Command Mode: Captive Portal Instance Mode.

Default: Disabled.

Usage Guidelines: With this command enabled, the redirect URL carries the IP address of the switch associated with the client when the client is redirected.

Example: Configure the redirect URL to carry the NAS IP parameter.

```
Switch(config-cp-instance)#redirect attribute nas-ip enable
```

7.11.1.27 redirect attribute nas-ip name

Command: `redirect attribute nas-ip name <word>`
`no redirect attribute nas-ip name`

Function: Configures the name of the NAS IP parameter carried in the redirect URL. The **no** form of this command restores the default.

Parameters: <word>: The parameter name, up to 32 characters.

Command Mode: Captive Portal Instance Mode.

Default: acname.

Usage Guidelines: Configures the name of the NAS IP parameter carried in the redirect URL.

Example: Set the name of the NAS IP parameter carried in the redirect URL to nasip.

```
Switch(config-cp-instance)#redirect attribute nas-ip name nasip
```

7.11.1.28 session-timeout

Command: `session-timeout <0-86400>`
`no session-timeout`

Function: Defines the Captive Portal session timeout. The **no** form of this command disables this function.

Parameters: <0-86400>: The session timeout, in seconds. 0 disables the timeout.

Default: 86400 seconds.

Command Mode: Captive Portal Instance Mode.

Usage Guidelines: Defines the Captive Portal session timeout.

Example: Set the Captive Portal session timeout to 100 seconds.

```
Switch (config-cp-instance)# session-timeout 100
```

7.11.1.29 show captive-portal

Command: `show captive-portal`

Function: Displays the Captive Portal status.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays the Captive Portal status parameters of the switch.

Example: Display the Captive Portal status when it is enabled and when it is disabled.

Captive Portal enabled:

```
Switch#show captive-portal
Administrative Mode.......................... Enable
Operational Status........................... Enabled
CP IP Address................................ 101.1.1.3
```

Captive Portal disabled:

```
Switch#show captive-portal
Administrative Mode.......................... Disable
Operational Status........................... Disabled
Disable Reason............................... Administrator Disabled
CP IP Address................................ 0.0.0.0
```

7.11.1.30 show captive-portal status

Command: `show captive-portal status`

Function: Displays the status of all Captive Portal instances in the system.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays the Captive Portal configuration and supported parameters of the switch.

Example: Display the Captive Portal status of the switch.

```
Switch#show captive-portal status
Peer Switch Statistics Reporting Interval..... 120
Authentication Timeout..................... 300
Authentication Type........................ External
Supported Captive Portals.................. 10
Configured Captive Portals................. 9
Active Captive Portals..................... 0
Local Supported Users...................... 128
Configured Local Users..................... 0
System Supported Users..................... 1024
Authenticated Users........................ 0
```

7.11.1.31 show captive-portal configuration

Command: `show captive-portal configuration <cp-id>`

Function: Displays the status of the Captive Portal configuration.

Parameters: <cp-id> is the Captive Portal ID, ranging from 1 to 10.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays the configured parameters of the portal instance.

Example: Display Captive Portal configuration 1.

```
Switch#show captive-portal configuration 1
CP ID...................................... 1
CP Name.................................... default
Operational Status......................... Enabled
Block Status............................... Not Blocked
Configured Locales......................... 1
Authenticated Users........................ 0
Permit-all Status.......................... Disabled
```

7.11.1.32 show captive-portal configuration interface

Command: `show captive-portal configuration <cp-id> interface <IFNAME or ethernet>`

Function: Displays the interfaces assigned to the Captive Portal configuration.

Parameters: <cp-id>: The Captive Portal ID.

IFNAME: The interface name or number.

ethernet: Ethernet port.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays the interface status of a portal instance.

Example: Display the interfaces of Captive Portal configuration 1.

```
Switch # show captive-portal configuration 1 interface e1/0/1
CP ID...................................... 1
CP Name.................................... Default
Interface.................................. 1
Interface Description...................... Ethernet1/0/1
Operational Status......................... Enabled
Block Status............................... Not Blocked
Authenticated Users........................ 0
```

7.11.1.33 show captive-portal configuration status

Command: show captive-portal configuration [<cp-id>] status

Function: Displays the configuration of all or a specific Captive Portal.

Parameters: <cp-id>: The Captive Portal ID. With this parameter, the configuration of the specified instance is displayed; without it, the parameters of all configured instances are displayed.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays detailed configuration parameters of portal instances.

Example: Display all Captive Portal configurations.

Display the status of all instances:

```
Switch # show captive-portal configuration status
CP ID       CP Name          Mode   Protocol Verification
----- -------------------- ------- -------- ------------
1     Default              Enable  HTTP     RADIUS
2     Default              Enable  HTTP     RADIUS
```

7.11.1.34 show captive-portal client status

Command: show captive-portal client [<FF-FF-FF-FF-FF-FF> { ipv4 | ipv6} <ip-addr>] status

Function: Displays detailed connection information for a user, or an overview of all users connected to Captive Portal.

Parameters: <FF-FF-FF-FF-FF-FF> is the MAC address of the user.

ipv4: The user address is an IPv4 address.

ipv6: The user address is an IPv6 address.

<ip-addr> is the user address: an IPv4 address in dotted decimal notation or an IPv6 address in X:X::X:X format.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays the status of all portal users or of a single user.

Example: Display information about users connected to Captive Portal.

```
Switch # show captive-portal client status
MAC Address    IP Address        User Name  Protocol  Mode  Session Time
20-6a-8a-65-0d-17 66.1.1.2          user1       HTTP    RADIUS 0d:00:00:47
```

7.11.1.35 show captive-portal configuration client

Command: show captive-portal configuration [<cp-id>] client status

Function: Displays the clients that have passed portal authentication on the interfaces of a Captive Portal configuration.

Parameters: <cp-id>: The Captive Portal ID.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays the user parameters of a portal instance.

Example: Display the authenticated clients of Captive Portal configuration 1.

```
Switch #show captive-portal configuration 1 client status
CP ID..................................... 1
CP Name................................... Default
  Client MAC Address   Client IP Address  Interface    Interface Description
```

```
   00-24-8c-00-99-27    10.1.1.51          1922      Port-Channel2
```

7.11.1.36 show captive-portal ext-portal-server status

Command: show captive-portal ext-portal-server status

Function: Displays the status of external portal servers.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays the status of external portal servers.

Example: Display the status of external portal servers.

```
Switch #show captive-portal ext-portal-server status
Server Name            Server IP Address           port     SocketNo
-------------------- ------------------------------------ --------
--------
x1             100.1.1.2                        7749               0
x2             100.1.1.1                        7749               0
```

7.11.1.37 show captive-portal interface configuration status

Command: show captive-portal interface configuration [<cp-id>] status

Function: Displays the interface information of all Captive Portal configurations or a specific configuration.

Parameters: <cp-id>: The Captive Portal ID.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays the bindings between all or specific portal instances and interfaces.

Example: Display the interface information of all Captive Portal configurations.

```
Switch #show captive-portal interface configuration status
CP ID    CP Name       Interface        Interface Description          Type
----- ----------------- --------- ----------------------------------
-------------------------------------------
1      Default            1             Ethernet1/0/1
Physical
```

7.11.2 Free-resource

7.11.2.1 free-resource

Command: free-resource destination { ipv4 | ipv6} <ip-addr><netmask> }
no free-resource destination { ipv4 | ipv6} <ip-addr><netmask> }

Function: Configures free-resource rules. Clients whose source IP addresses match a rule can access the destination resources in the rule directly, without redirection or portal authentication.

Parameters: ipv4: The free resource address is an IPv4 address.

ipv6: The free resource address is an IPv6 address.

<ip-addr>: The IP address of the free resource.

<netmask>: The mask of the free resource address.

Default: None.

Command Mode: Captive Portal Mode.

Usage Guidelines: Configures the client address range (visitors) that can access free resources and the address range of the free resources.

Example: Configure free-resource rules.

```
Switch (config-cp)# free-resource 1 source any
```

7.11.3 Automatic Page Pushing after Successful Authentication

7.11.3.1 redirect attribute url-after-login enable

Command: `redirect attribute url-after-login enable`
`no redirect attribute url-after-login enable`

Function: Configures the redirect URL to carry the URL to be pushed after successful authentication. The **no** form of this command disables this function.

Parameters: None.

Command Mode: Captive Portal Instance Mode.

Default: Disabled.

Usage Guidelines: With this command enabled, the redirect URL pushed by the switch carries the URL to be pushed after successful authentication. If the url-value of **redirect attribute url-after-login value** is empty, the carried URL is the page the user requested before authentication; otherwise, it is the URL configured by url-value.

Example: Configure the redirect URL to carry the URL to be pushed after successful authentication.

```
Switch(config-cp-instance)#redirect attribute url-after-login enable
```

7.11.3.2 redirect attribute url-after-login name

Command: `redirect attribute url-after-login name <name>`
`no redirect attribute url-after-login name`

Function: Configures the name of the attribute that carries the post-authentication URL in the redirect URL. The **no** form of this command restores the default.

Parameters: <name>: The attribute name, up to 32 characters.

Command Mode: Captive Portal Instance Mode.

Default: srcurl.

Usage Guidelines: Configures the name of the attribute that carries the post-authentication URL in the redirect URL.

Example: Set the name of the attribute that carries the post-authentication URL in the redirect URL to redirect.

```
Switch(config-cp-instance)#redirect attribute url-after-login name redirect
```

7.11.3.3 redirect attribute url-after-login encode

Command: `redirect attribute url-after-login encode {plain-text|base64}`

Function: Configures the encoding of the post-authentication URL carried in the redirect URL.

Parameters: plain-text: Plain text.

base64: Base64 encoding.

Command Mode: Captive Portal Instance Mode.

Default: plain-text.

Usage Guidelines: Configures the encoding of the post-authentication URL carried in the redirect URL, according to the encodings supported by the portal server.

Example: Set the encoding of the post-authentication URL carried in the redirect URL to Base64.

```
Switch(config-cp-instance)#redirect attribute url-after-login encode base64
```

7.11.3.4 redirect attribute url-after-login value

Command: `redirect attribute url-after-login value <url-value>`
`no redirect attribute url-after-login value`

Function: Configures the URL that is displayed after successful authentication. The **no** form of this command deletes it.

Parameters: <url-value>: The URL, up to 512 characters.

Command Mode: Captive Portal Instance Mode.

Default: None.

Usage Guidelines: Configures the URL that is displayed after successful authentication. If the redirect URL is configured to carry the post-authentication URL, it carries the URL specified by <url-value>.

Example: Set the URL displayed after successful authentication to http://www.test.com.

```
Switch(config-cp-instance)#redirect attribute url-after-login value
http://www.test.com
```

7.11.4 Portal Escaping

7.11.4.1 show captive-portal ext-portal-server server-name <name> status

Command: `show captive-portal ext-portal-server server-name <name> status`

Function: Displays the portal server status, including the server address and whether portal escape is enabled.

Parameters: <name> is the portal server name, a case-sensitive string of 1 to 32 characters.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Checking the server status is an important troubleshooting method. If portal escape does not take effect, the configuration may be wrong; this command helps the administrator find and correct the fault. Without <name>, the status of all servers is displayed; with <name>, detailed status information for that server is displayed.

Example: Display the status of external portal servers.

Display the detailed status of the server named Portaltest.

```
Switch (config-cp)#show captive-portal ext-portal-server server-name
Portaltest status
Server Name..................................... portaltest
Server IP....................................... 101.1.1.6
Server Port..................................... 7749
Server Key.....................................
Detect Mode..................................... Enable
Detect Interval................................. 20
Detect Retries.................................. 3
Detect Trap Mode................................ Disable
Detect Log Mode................................. Disable
Detect Permit-all Mode.......................... Enable
Detect Operational Mode......................... Enable
Detect Operational Status....................... Down
Detect Operational Fails........................ 1
Detect Operational Time......................... 0d:00:00:11
```

7.12 MAB

7.12.1 authentication mab

Command: `authentication mab {radius|local} (none|)`
`no authentication mab`

Function: Configures the authentication method and priority of MAC address authentication. The **no** form of this command restores the default method.

Parameters: radius: RADIUS authentication. **local**: Local authentication. **none**: No authentication.

Default: RADIUS authentication.

Command Mode: Global Mode.

Usage Guidelines: The **none** option provides the escape function for MAC address authentication: if none of the configured RADIUS servers respond, the switch uses no authentication and lets MAC authentication users access the network directly. The **local** option authenticates MAC addresses locally with a local user name and password. With **authentication mab radius local none**, when the RADIUS server does not respond, the switch checks whether a local user name and password for MAB are configured; if they are, local authentication is used; otherwise, the backup **none** method is used.

Example: Configure local authentication and the escape function for MAC address authentication.

```
Switch(config)#authentication mab radius local none
```

7.12.2 clear mac-authentication-bypass binding

Command: `clear mac-authentication-bypass binding {mac WORD | interface (ethernet IFNAME | IFNAME) | all}`

Function: Clears MAB bindings.

Parameters: mac WORD: Deletes the MAB binding of the specified MAC address.

interface IFNAME: Deletes the MAB bindings of the specified port.

all: Deletes all MAB bindings.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: None.

Example: Delete all MAB bindings.

```
Switch#clear mac-authentication-bypass binding all
```

7.12.3 debug mac-authentication-bypass

Command: `debug mac-authentication-bypass {packet | event | binding}`

Function: Enables debugging of MAB packets, events, or bindings.

Parameters: packet: Debugging of MAB packets.

event: Debugging of MAB events.

binding: Debugging of MAB bindings.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: None.

Example: Enable debugging of MAB packets.

```
Switch#debug mac-authentication-bypass packet
```

7.12.4 mac-authentication-bypass binding-limit

Command: `mac-authentication-bypass binding-limit <1-100>`
`no mac-authentication-bypass binding-limit`

Function: Sets the maximum number of MAB bindings. The **no** form of this command restores the default of 3.

Parameters: <1-100>: The maximum number of MAB bindings, ranging from 1 to 100.

Command Mode: Port Mode.

Default: 3.

Usage Guidelines: Sets the maximum number of MAB bindings. When the limit is reached, the port stops creating bindings. If the configured limit is less than the current number of bindings on the port, the configuration fails.

Example: Set the maximum number of MAB bindings to 10.

```
Switch(Config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#mac-authentication-bypass binding-limit 10
```

7.12.5 mac-authentication-bypass enable

Command: `mac-authentication-bypass enable`
`no mac-authentication-bypass enable`

Function: Enables MAB globally and on ports. The **no** form of this command disables MAB.

Parameters: None.

Command Mode: Global Mode and Port Mode.

Default: MAB is disabled globally and on ports.

Usage Guidelines: To perform MAB authentication on a port, first enable MAB globally and then on the port.

Example: Enable MAB globally and on port Ethernet 1/0/1.

```
Switch(Config)#mac-authentication-bypass enable
Switch(Config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#mac-authentication-bypass enable
```

7.12.6 mac-authentication-bypass guest-vlan

Command: `mac-authentication-bypass guest-vlan <1-4094>`
`no mac-authentication-bypass guest-vlan`

Function: Configures the MAB guest VLAN. The **no** form of this command deletes the guest VLAN.

Parameters: <1-4094>: The guest VLAN ID, ranging from 1 to 4094.

Command Mode: Port Mode.

Default: None.

Usage Guidelines: Configures the MAB guest VLAN. This command applies only to Hybrid ports and does not take effect on Access ports. If MAB authentication fails and a guest VLAN is configured on the port connected to the MAB user, the user joins and can access the guest VLAN.

Example: Configure the MAB guest VLAN of port Ethernet 1/0/1.

```
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)#mac-authentication-bypass guest-vlan 10
```

7.12.7 mac-authentication-bypass timeout linkup-period

Command: `mac-authentication-bypass timeout linkup-period <0-30>`
`no mac-authentication-bypass timeout linkup-period`

Function: Sets the down/up interval used when the VLAN binding of a port changes, so that the user can obtain an IP address again.

Parameters: <0-30>: The time, in seconds, after which an automatically shut-down port is brought up again. 0 means no down/up operation is performed.

Command Mode: Global Mode.

Default: 0.

Usage Guidelines: After successful MAB authentication, the user is placed in a VLAN according to the auto VLAN setting; after failed authentication, according to the guest VLAN setting. With linkup-period set, when the VLAN binding of a port changes, the port is shut down automatically and brought up again after the linkup period, so that the client can obtain an IP address.

Example: Set the down/up time to 12 seconds.

```
Switch(Config)#mac-authentication-bypass timeout linkup-period 12
```

7.12.8 mac-authentication-bypass timeout offline-detect

Command: `mac-authentication-bypass timeout offline-detect (0 | <60-7200>)`
`no mac-authentication-bypass timeout offline-detect`

Function: Configures the offline detection time. The **no** form of this command restores the default.

Parameters: 0 | <60-7200>: The offline detection time, 0 or 60 to 7200 seconds.

Command Mode: Global Mode.

Default: 180 seconds.

Usage Guidelines: When the offline detection time is 0, the switch does not monitor MAB bindings. When it is 60 to 7200 seconds, the switch periodically checks the traffic of each MAB binding; if no traffic is seen within the offline detection time, the binding is deleted and the traffic is blocked.

Example: Set the offline detection time to 200 seconds.

```
Switch(Config)#mac-authentication-bypass timeout offline-detect 200
```

7.12.9 mac-authentication-bypass timeout quiet-period

Command: `mac-authentication-bypass timeout quiet-period <1-60>`
`no mac-authentication-bypass timeout quiet-period`

Function: Sets the MAB quiet period. The **no** form of this command restores the default.

Parameters: <1-60>: The quiet period, ranging from 1 to 60 seconds.

Command Mode: Global Mode.

Default: 30 seconds.

Usage Guidelines: If MAB authentication fails, the switch does not respond to authentication requests from that MAC address during the quiet period; after the quiet period, it responds again.

Example: Set the MAB quiet period to 60 seconds.

```
Switch(Config)#mac-authentication-bypass timeout quiet-period 60
```

7.12.10 mac-authentication-bypass timeout reauth-period

Command: `mac-authentication-bypass timeout reauth-period <1-3600>`
`no mac-authentication-bypass timeout reauth-period`

Function: Sets the re-authentication interval in the authentication-failed state. The **no** form of this command restores the default.

Parameters: <1-3600>: The re-authentication interval, ranging from 1 to 3600 seconds.

Command Mode: Global Mode.

Default: 30 seconds.

Usage Guidelines: In the authentication-failed state, the user is re-authenticated periodically until authentication succeeds; after successful authentication, the user can access network resources.

Example: Set the re-authentication interval to 20 seconds.

```
Switch(Config)#mac-authentication-bypass timeout reauth-period 20
```

7.12.11 mac-authentication-bypass timeout stale-period

Command: `mac-authentication-bypass timeout stale-period <0-60>`
`no mac-authentication-bypass timeout stale-period`

Function: Sets how long after an MAB port goes down its user bindings are deleted. The **no** form of this command restores the default.

Parameters: <0-60>: The delay before bindings are deleted, ranging from 0 to 60 seconds.

Command Mode: Global Mode.

Default: 30 seconds.

Usage Guidelines: If the delay is 0, all user bindings of the port are deleted as soon as the MAB port goes down; if it is greater than 0, the bindings are deleted after the delay.

Example: Set the binding deletion delay to 40 seconds.

```
Switch(Config)#mac-authentication-bypass timeout stale-period 40
```

7.12.12 mac-authentication-bypass username-format

Command: `mac-authentication-bypass username-format {mac-address | {fixed username WORD password WORD}}`

Function: Sets the user name format for MAB authentication.

Parameters: mac-address: Uses the MAC address of the MAB user as the user name and password.

fixed username WORD password WORD: Uses the specified user name and password, each 1 to 32 characters long.

Command Mode: Global Mode.

Default: The MAC address of the MAB user is used as the user name and password.

Usage Guidelines: MAB authentication uses either the MAC address of the MAB user as the user name and password, or a specified user name and password. If no user name and password are specified, the device uses the MAC address by default.

Example: Configure all MAB users to authenticate with user name mab-user and password mab-pwd.

```
Switch(Config)#mac-authentication-bypass username-format fixed username mab-
user password mab-pwd
```

7.12.13 show mac-authentication-bypass

Command: show mac-authentication-bypass {interface {ethernet IFNAME | IFNAME) |}

Function: Displays MAB binding information.

Parameters: interface {ethernet IFNAME | IFNAME}: The port name.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: None.

Example: Display the binding information of all MAB users.

```
Switch#show mac-authentication-bypass
The Number of all binding is 5
MAC                  Interface       Vlan ID    State
------------------------------------------------------------------------------
----------------------------
05-0a-eb-6a-7f-88    Ethernet1/0/1   1          MAB_QUIET
04-0a-eb-6a-7f-88    Ethernet1/0/1   1          MAB_QUIET
03-0a-eb-6a-7f-88    Ethernet1/0/1   1          MAB_QUIET
02-0a-eb-6a-7f-88    Ethernet1/0/1   1          MAB_AUTHENTICATED
00-0a-eb-6a-7f-8e    Ethernet1/0/1   1          MAB_AUTHENTICATED
```

Output	Description
The Number of all binding	Number of bindings of all MAB users, including successfully authenticated users and users in the quiet period after failed authentication
MAC	MAC address
Interface	Bound port
Vlan	VLAN to which the MAB user belongs
State	Authentication state

```
Switch(config)#show mac-authentication-bypass int e1/0/1
Interface Ethernet1/0/1 user config:
MAB enable: Enable
Binding info: 1
------------------------------------------------------
MAB Binding built at SUN JAN 01 01:14:48 2006
        VID 1, Port: Ethernet1/0/1
        Client MAC: 00-0a-eb-6a-7f-8e
        Binding State: MAB_AUTHENTICATED
        Binding State Lease: 164 seconds left
```

Output	Description
MAB enable	Whether MAB is enabled
Binding info	Number of MAB bindings on the specified port
MAB Binding built at	Time when the user binding was created
VID	VLAN to which the MAB user belongs
Port	Bound port
Client MAC	MAC address
Binding State	Authentication state
Binding State Lease	Remaining time before the binding is released

7.13 PPPoE Intermediate Agent

7.13.1 debug pppoe packet {receive | send} interface ethernet <interface-name>

Command: debug pppoe packet (receive | send|) interface ethernet <interface-name>
no debug pppoe packet (receive | send|) interface ethernet <interface-name>

Function: Enables PPPoE packet debugging on the specified port. The **no** form of this command disables it.

Parameters: receive: Debugging of received PPPoE packets.

send: Debugging of sent PPPoE packets.

ethernet: Physical port.

<interface-name>: The port name.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: Enables PPPoE packet debugging on the specified port to display the PPPoE packets received and sent on the port.

Example: Enable PPPoE packet debugging on port Ethernet 1/0/2.

```
Switch#debug pppoe intermediate send interface ethernet 1/0/2
```

7.13.2 pppoe intermediate-agent

Command: pppoe intermediate-agent
no pppoe intermediate-agent

Function: Enables PPPoE intermediate agent globally. The **no** form of this command disables it globally.

Parameters: None.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: After PPPoE intermediate agent (IA) is enabled globally, PPPoE discovery-stage packets are processed according to the related configuration.

Example: Enable PPPoE intermediate agent globally.

```
Switch(config)#pppoe intermediate agent
```

7.13.3 pppoe intermediate-agent (Port)

Command: pppoe intermediate-agent
no pppoe intermediate-agent

Function: Enables PPPoE intermediate agent on the port. The **no** form of this command disables it on the port.

Parameters: None.

Command Mode: Port Mode.

Default: Disabled.

Usage Guidelines: After PPPoE IA is enabled on the port, a vendor tag is added to PPPoE packets on the port.

Note: 1. PPPoE intermediate agent must be enabled globally.

2. At least one port must be connected to the PPPoE server and configured as a trusted port.

Example: Enable PPPoE intermediate agent on port Ethernet 1/0/2.

```
Switch(config-if-ethernet1/0/2)#pppoe intermediate agent
```

7.13.4 pppoe intermediate-agent circuit-id

Command: pppoe intermediate-agent circuit-id <string>
no pppoe intermediate-agent circuit-id <string>

Function: Configures the circuit ID of the port. The **no** form of this command cancels the configuration.

Parameters: <string>: The circuit ID, up to 63 bytes.

Command Mode: Port Mode.

Default: Not configured.

Usage Guidelines: Configures a circuit ID for each port individually; it takes precedence over the **pppoe intermediate-agent identifier-string** command.

Example: Set the circuit ID of port Ethernet 1/0/3 in VLAN 3 to abcd/efgh.

```
Switch(config-if-ethernet1/0/3)#pppoe intermediate-agent circuit-id abcd/efgh
```

When port Ethernet 1/0/3 in VLAN 3 receives a PPPoE packet, the circuit ID in the added vendor tag is "abcd/efgh".

7.13.5 pppoe intermediate-agent delimiter

Command: pppoe intermediate-agent delimiter <WORD>
no pppoe intermediate-agent delimiter

Function: Configures the delimiter between fields in the circuit ID and remote ID. The **no** form of this command cancels the configuration.

Parameters: <WORD>: The delimiter: #, ., ,, ;, :, /, or space.

Command Mode: Global Mode.

Default: Fields are separated by '\0'.

Usage Guidelines: After the delimiter is configured, the fields added to the circuit ID and remote ID are separated by it. Note: Global PPPoE intermediate agent must be enabled.

Example: Set the delimiter to a space.

```
Switch(config)#pppoe intermediate-agent delimiter space
```

7.13.6 pppoe intermediate-agent format

Command: pppoe intermediate-agent format (circuit-id | remote-id) (hex | ascii)
no pppoe intermediate-agent format (circuit-id | remote-id)

Function: Configures hexadecimal or ASCII format for the circuit ID and remote ID. The **no** form of this command cancels the configuration.

Parameters: hex: Hexadecimal.

ascii: ASCII.

Command Mode: Global Mode.

Default: Not configured.

Usage Guidelines: Encodes the circuit ID and remote ID in the vendor tag in hexadecimal or ASCII format. Note: Global PPPoE intermediate agent must be enabled.

Example: Set the remote ID format to ASCII.

```
Switch(config)#pppoe intermediate-agent format remote-id ascii
```

7.13.7 pppoe intermediate-agent remote-id

Command: pppoe intermediate-agent remote-id <string>
no pppoe intermediate-agent remote-id <string>

Function: Configures the remote ID of the port. The **no** form of this command cancels the configuration.

Parameters: <string>: The remote ID, up to 63 bytes.

Command Mode: Port Mode.

Default: Not configured.

Usage Guidelines: Configures the remote ID of each port. If it is not configured, the MAC address of the switch is used as the remote ID.

Example: Set the remote ID of port Ethernet 1/0/2 to abcd.

```
Switch(config-if-ethernet1/0/2)# pppoe intermediate-agent remote-id abcd
```

7.13.8 pppoe intermediate-agent trust

Command: pppoe intermediate-agent trust
no pppoe intermediate-agent trust

Function: Configures the port as a trusted port. The **no** form of this command configures it as an untrusted port.

Parameters: None.

Command Mode: Port Mode.

Default: Untrusted.

Usage Guidelines: Ports connected to the server must be configured as trusted ports. Note: At least one trusted port must be connected to the PPPoE server.

Example: Configure port Ethernet 1/0/1 as a trusted port.

```
Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent trust
```

7.13.9 pppoe intermediate-agent type self-defined circuit-id

Command: pppoe intermediate-agent type self-defined circuit-id {vlan | port | id (switch-id (mac | hostname) | remote-mac) | string WORD}
no pppoe intermediate-agent type self-defined circuit-id

Function: Configures a self-defined circuit ID. The **no** form of this command cancels the configuration.

Parameters: vlan: The VLAN ID.

port: The port ID.

id switch-id mac: The local MAC address.

id switch-id hostname: The local host name.

id remote-mac: The remote MAC address.

string WORD: The specified string.

Command Mode: Global Mode.

Default: Not configured.

Usage Guidelines: This configuration and **type tr-101 circuit-id** are mutually exclusive; configuring this command clears the **type tr-101 circuit-id** configuration.

Example: Configure the self-defined circuit ID as vlan, port, and id switch-id hostname.

```
Switch(config)#pppoe intermediate-agent type self-defined circuit-id vlan
port id switch-id hostname
```

7.13.10 pppoe intermediate-agent type self-defined remoteid

Command: pppoe intermediate-agent type self-defined remoteid {mac | vlan-mac | hostname | string WORD}

no pppoe intermediate-agent type self-defined remote-id

Function: Configures a self-defined remote ID. The **no** form of this command cancels the configuration.

Parameters: mac: The MAC address of the Ethernet port.

vlan-mac: The MAC address of the IP interface.

hostname: The local host name.

string WORD: The specified string.

Command Mode: Global Mode.

Default: Not configured.

Usage Guidelines: The fields in the remote ID appear in the order in which they are configured in this command.

Example: Configure the self-defined remote ID as string abcd, mac, and hostname.

```
Switch(config)#pppoe intermediate-agent type self-defined remoteid string
abcd mac hostname
```

7.13.11 pppoe intermediate-agent type tr-101 circuit-id access-node-id

Command: pppoe intermediate-agent type tr-101 circuit-id access-node-id <string>

no pppoe intermediate-agent type tr-101 circuit-id access-node-id

Function: Configures the access-node-id field of the circuit ID in the vendor tag added in TR-101 format.

Parameters: <string>: The access node ID, up to 47 bytes.

Command Mode: Global Mode.

Default: The MAC address of the switch.

Usage Guidelines: Use this command to configure the access-node-id of the circuit ID in the vendor tag. The circuit ID is access-node-id + " eth " + Slot ID + delimiter + Port Index + delimiter + VLAN ID. The access-node-id occupies n bytes (n < 48); " eth " (space, e, t, h, space) occupies 5 bytes; Slot ID occupies 2 bytes; Port Index occupies 3 bytes; VLAN ID occupies 4 bytes; and each delimiter occupies 1 byte. By default, the access-node-id of the circuit ID is the MAC address of the switch (6 bytes). For example, if the MAC address is "0a0b0c0d0e0f", the Slot ID is 12, the Port Index is 34, and the VLAN ID is 567, the default circuit ID is "0a0b0c0d0e0f eth 12/034:0567".

Example: Set the access-node-id of the circuit ID in the vendor tag to abcd.

```
Switch(config)#pppoe intermediate-agent access-node-id abcd
```

When port Ethernet 1/0/3 in VLAN 3 receives PPPoE packets, the circuit ID in the added vendor tag is "abcd eth 01/003:0003".

7.13.12 pppoe intermediate-agent type tr-101 circuit-id identifier-string option delimiter

Command: pppoe intermediate-agent type tr-101 circuit-id identifier-string <string> option {sp | sv | pv | spv} delimiter <WORD> [delimiter <WORD>]

no pppoe intermediate-agent type tr-101 circuit-id identifier-string option delimiter

Function: Configures the circuit ID of the vendor tag added in TR-101 format. The **no** form of this command deletes the configuration.

Parameters: <string>: The identifier string, up to 47 bytes.

{sp | sv | pv | spv}: The combination of slot, port, and VLAN: **sp** = slot and port, **sv** = slot and VLAN, **pv** = port and VLAN, **spv** = slot, port, and VLAN.

<WORD>: The delimiter between slot, port, and VLAN: #, ., ,, ;, :, /, or space. Note: In spv mode, there are two delimiters: the first between slot and port, and the second between port and VLAN.

Command Mode: Global Mode.

Default: Not configured.

Usage Guidelines: Configures the global circuit ID; it takes precedence over the **pppoe intermediate-agent access-node-id** command. The circuit ID is access-node-id + " eth " + Slot ID + delimiter + Port Index + delimiter + VLAN ID. The access-node-id occupies n bytes (n < 48); " eth " (space, e, t, h, space) occupies 5 bytes; Slot ID occupies 2 bytes; Port Index occupies 3 bytes; VLAN ID occupies 4 bytes; and each delimiter occupies 1 byte.

Example: Set the identifier string to xyz, use the spv combination, use "#" between the Slot ID and Port ID, and use "/" between the Port ID and VLAN ID.

```
Switch(config)#pppoe intermediate-agent identifier-string xyz option spv
delimiter # delimiter /
Switch# show pppoe intermediate-agent identifier-string option delimiter
config identifier string is : xyz
config option is : slot , port and vlan
the first delimiter is :  "# "
the second delimiter is :  "/ "
```

When port Ethernet 1/0/3 in VLAN 3 receives PPPoE packets, the circuit ID in the added vendor tag is "xyz eth 01#003/0003".

7.13.13 pppoe intermediate-agent vendor-tag strip

Command: pppoe intermediate-agent vendor-tag strip

no pppoe intermediate-agent vendor-tag strip

Function: Enables vendor tag stripping on the port. The **no** form of this command disables it.

Parameters: None.

Command Mode: Port Mode.

Default: Disabled.

Usage Guidelines: If a packet from the server to the client contains a vendor tag, the vendor tag is stripped.

Note: 1. Global PPPoE intermediate agent must be enabled.

2. This command must be configured on a trusted port.

Example: Enable vendor tag stripping on trusted port Ethernet 1/0/1.

```
Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent trust
Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent vendor-tag strip
```

7.13.14 show pppoe intermediate-agent access-node-id

Command: show pppoe intermediate-agent access-node-id

Function: Displays the configured access node ID.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Displays the access-node-id configured by the user.

Example: Display the access-node-id configuration.

```
Switch#pppoe intermediate-agent access-node-id abcd
Switch#show pppoe intermediate-agent access-node-id
pppoe intermediate-agent access-node-id is : abcd
```

7.13.15 show pppoe intermediate-agent identifier-string option delimiter

Command: show pppoe intermediate-agent identifier-string option delimiter

Function: Displays the configured identifier string, slot/port/VLAN combination, and delimiters.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Displays the configured identifier string, slot/port/VLAN combination, and delimiters.

Example: Display the PPPoE intermediate agent identifier string configuration.

```
Switch#pppoe intermediate-agent identifier-string abcd option spv delimiter #
delimiter /
Switch# show pppoe intermediate-agent identifier-string option delimiter
config identifier string is : abcd
config option is : slot , port and vlan
the first delimiter is :  "# "
the second delimiter is :  "/ "
```

7.13.16 show pppoe intermediate-agent info

Command: show pppoe intermediate-agent info [interface ethernet <interface-name>]

Function: Displays the PPPoE IA configuration of all ports or the specified port.

Parameters: ethernet: Physical port.

<interface-name>: The port name.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Displays the configuration of the port: whether it is a trusted port, whether vendor tag stripping and rate limiting are enabled, and the configured circuit ID and remote ID.

Example: Display the PPPoE intermediate agent configuration of port Ethernet 1/0/2.

```
Switch# show pppoe intermediate-agent info interface ethernet 1/0/2
Interface    IA    Trusted  vendor Strip  Rate limit  circuit id remote id
----------  ------  ------  -----------   -------     ---------  ----------
Ethernet1/0/2  yes      no       no           no       test1/port1   host1
```

7.14 QoS

7.14.1 accounting

Command: `accounting`
`no accounting`

Function: Enables statistics for the classified traffic.

Parameters: None.

Command Mode: Policy Class Map Mode.

Default: Statistics are disabled.

Usage Guidelines: With this function enabled, statistics are collected for the traffic of the policy class map. In single-bucket mode, packets passing the policer are either red or green; in the output, in-profile means green and out-profile means red. In dual-bucket mode, packets have three colors; in the output, in-profile means green and out-profile means red and yellow.

Example: Count the packets that match class c1.

```
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#accounting
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
```

7.14.2 class

Command: `class <class-map-name> [insert-before <class-map-name>]`
`no class <class-map-name>`

Function: Associates a class with a policy map and enters Policy Class Map Mode. The **no** form of this command deletes the specified class.

Parameters: <class-map-name> is the name of the class map used by the class.

insert-before <class-map-name>: Inserts the new class before an existing class, giving the new class a higher priority.

Default: No policy class is configured.

Command Mode: Policy Map Configuration Mode.

Usage Guidelines: Before configuring a policy class, create a policy map and enter Policy Map Mode. In Policy Map Mode, actions can be configured for traffic classified by the class map.

Example: Add policy class c1 to the policy map, and then add policy class c2 before c1.

```
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#class c2 insert-before c1
Switch(Config-PolicyMap-p1-Class-c2)#exit
```

7.14.3 class-map

Command: `class-map <class-map-name>`
`no class-map <class-map-name>`

Function: Creates a class map and enters Class Map Mode. The **no** form of this command deletes the specified class map.

Parameters: <class-map-name> is the class map name.

Default: No class map is configured.

Command Mode: Global Mode.

Usage Guidelines: None.

Example: Create and then delete a class map named c1.

```
Switch(config)#class-map c1
Switch(Config-ClassMap-c1)#exit
Switch(config)#no class-map c1
```

7.14.4 clear mls qos statistics

Command: clear mls qos statistics [in | out] {interface <interface-name> | vlan <vlan-id>}

Function: Clears the inbound or outbound statistics of the policy map applied to the specified port or VLAN.

Parameters: in | out: The inbound or outbound direction of the port or VLAN.

<vlan-id>: The VLAN ID.

<interface-name>: The interface name.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Clears the inbound or outbound statistics of the policy map applied to the specified port or VLAN.

Example: Clear the policy map statistics of VLAN 100.

```
Switch#Clear mls qos statistics vlan 100
```

7.14.5 drop

Command: drop
no drop

Function: Drops packets that match the class. The **no** form of this command cancels the action.

Parameters: None.

Default: No action.

Command Mode: Policy Class Map Mode.

Usage Guidelines: After this command is configured, matching packets are dropped.

Example: Drop packets that match class c1.

```
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#drop
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
```

7.14.6 match

Command: match {access-group <acl-index-or-name> | ip dscp <dscp-list> | ip precedence <ip-precedence-list> | ipv6 access-group <acl-index-or-name> | ipv6 dscp <dscp-list> | ipv6 flowlabel <flowlabel-list> | vlan <vlan-list> | cos <cos-list>}
no match {access-group | ip dscp | ip precedence| ipv6 access-group| ipv6 dscp | ipv6 flowlabel | vlan | cos}

Function: Configures the match criterion of the class map. The **no** form of this command deletes the specified match criterion.

Parameters: access-group <acl-index-or-name>: Matches the specified IP ACL, MAC ACL, or IPv6 standard ACL, specified by number or name.

ip dscp <dscp-list> and **ipv6 dscp <dscp-list>**: Match the specified DSCP values. The list can contain up to 8 DSCP values, ranging from 0 to 63.

ip precedence <ip-precedence-list>: Matches the specified IP precedence values. The list can contain up to 8 values, ranging from 0 to 7.

ipv6 access-group <acl-index-or-name>: Matches the specified IPv6 ACL, specified by number or name.

ipv6 flowlabel <flowlabel-list>: Matches the specified IPv6 flow label values, ranging from 0 to 1048575.

vlan <vlan-list>: Matches the specified VLAN IDs. The list can contain up to 8 VLAN IDs, ranging from 1 to 4094.

cos <cos-list>: Matches the specified CoS values. The list can contain up to 8 values, ranging from 0 to 7.

Default: No match criterion is configured.

Command Mode: Class Map Mode.

Usage Guidelines: Only one match criterion can be configured in a class map. When an ACL is matched, permit rules select the traffic to which the policy map actions apply, and deny rules exclude traffic from the policy map actions. (Deny rules are not supported in PBR; avoid using them there.) Configuring a different match criterion after one is configured fails, but configuring the same criterion again overwrites the previous one.

Example: Create class map c1 and configure it to match packets with IP precedence 0.

```
Switch(config)#class-map c1
Switch(Config-ClassMap-c1)#match ip precedence 0
Switch(Config-ClassMap-c1)#exit
```

7.14.7 mls qos aggregate-policy

Command:

Single Bucket Mode:

mls qos aggregate-policy <policer_name> <bits_per_second> <normal_burst_bytes> [{conform-action ACTION | exceed-action ACTION }]

Dual Bucket Mode:

mls qos aggregate-policy <policer_name> <bits_per_second> <normal_burst_bytes> (pir <peak_rate_bps> | <maximum_burst_bytes>) ({conform-action ACTION | exceed-action ACTION | violate-action ACTION)

ACTION definition:

drop | transmit | set-internal-priority <intp_value> | set-cos-transmit <new-cos> | set-dscp-transmit <new-dscp> | set-prec-transmit <ip-precedence> | set-drop-precedence < new-drop-priority>

[no] mls qos aggregate-policy <policer_name>

Function: Defines an aggregate policer, sets the token bucket mode (single-rate single-bucket, single-rate dual-bucket, or dual-rate dual-bucket), and sets the actions for packets of each color. The **no** form of this command deletes the configuration.

Parameters: <policer_name>: The name of the aggregate policer.

<bits_per_second>: The committed information rate (CIR), in kbps, ranging from 1 to 10000000.

<normal_burst_bytes>: The committed burst size (CBS), in KB, ranging from 1 to 1000000. If the configured CBS exceeds the chip limit, the hardware is configured with the maximum value supported by the chip, without a CLI prompt.

<maximum_burst_bytes>: The peak burst size (PBS), in KB, ranging from 1 to 1000000. If the configured PBS exceeds the chip limit, the hardware is configured with the maximum value supported by the chip, without a CLI prompt. Note: This parameter exists only in dual-bucket mode.

pir <peak_rate_bps>: The peak information rate (PIR), in kbps, ranging from 1 to 10000000. If PIR is not configured, the policer works in single-rate dual-bucket mode; otherwise, in dual-rate dual-bucket mode. Note: This parameter exists only in dual-bucket mode.

conform-action: The action for green packets, which do not exceed the CIR. The default is transmit.

exceed-action: The action for yellow packets, which exceed the CIR but not the PIR. The default is drop.

violate-action: The action for red packets, which exceed the PIR. The default is drop.

ACTION:

drop / **transmit**: Drops or transmits the packets.

set-internal-priority <intp_value>: Changes the internal priority of the packets.

set-cos-transmit <new-cos>: Changes the Layer 2 CoS value of the packets.

set-drop-precedence <new-drop-priority>: Changes the drop precedence of the packets.

set-dscp-transmit <new-dscp>: Changes the DSCP value.

set-prec-transmit <ip-precedence>: Changes the IP precedence (ToS).

Default: No aggregate policer is defined. The default action for both exceed-action and violate-action is drop.

Command Mode: Global Mode.

Usage Guidelines: The CLI supports both single-bucket and dual-bucket configuration, determined by whether PIR or PBS is configured. If an action is configured directly after the CBS, the mode is single-rate single-bucket; if only PBS is configured, the mode is single-rate dual-bucket three-color; if both PIR and PBS are configured, the mode is dual-rate dual-bucket three-color. Set actions and policer actions in the policy map have the same effect; the policer action overrides the set action. In addition, if both exceed-action and violate-action are set-internal-priority, the <intp_value> must be the same.

Example: Configure dual-bucket mode with CIR 1000, CBS 1000, PIR 20000, and PBS 10000, and transmit yellow packets (those that exceed the CIR but not the PIR).

```
Switch(config)#mls qos aggregate-policy color 10000 1000 pir 20000 10000
exceed-action transmit
```

7.14.8 mls qos cos

Command: `mls qos cos {<default-cos>}`
`no mls qos cos`

Function: Configures the default CoS value of the port. The **no mls qos cos** command restores the default.

Parameters: <default-cos> is the default CoS value of the port, ranging from 0 to 7.

Default: 0.

Command Mode: Port Mode.

Usage Guidelines: Configures the default CoS value of the switch port. Untagged packets received on the port are assigned the default CoS value.

Example: Set the default CoS value of port Ethernet 1/0/1 to 7; packets received on this port without a CoS value are assigned CoS 7.

```
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#mls qos cos 7
```

7.14.9 mls qos internal-priority

Command: mls qos internal-priority {<default-intp> }
no mls qos internal-priority

Function: Configures the default internal priority of the port. The **no** form of this command restores the default.

Parameters: <default-intp>: The default internal priority of the port, ranging from 0 to 119.

Default: 0.

Command Mode: Port Mode.

Usage Guidelines: Configures the default internal priority of the port. If a packet received on the port has no trusted DSCP or CoS field, it is assigned the default internal priority. The internal priority may be changed by the configured QoS policy.

Example: Set the default internal priority of port Ethernet 1/0/1 to 40.

```
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#mls qos internal-priority 40
```

7.14.10 mls qos map

Command: mls qos map (cos-intp < in-cos list > | dscp-dscp <in-dscp list> to <out-dscp> | dscp-intp <in-dscp list> to <intp> | intp-exp <exp1。。。exp8>|exp-intp <intp>| intp-cos <intp> to <in-cos list>| intp-dp <intp> to <dp1…dp8> |intp-dscp <intp> to <in-dscp list| intp-quene <intp> to <quene>)
no mls qos map (cos-intp | dscp-dscp | dscp-intp | dscp-dp| intp-exp | exp-intp| intp-cos|intp-dp|intp-dscp|intp-quene)
mls qos map intp-exp <exp1。。。exp8>no mls qos map intp-exp

Function: Configures QoS priority mapping. The **no** form of this command restores the default mapping.

Parameters: cos-dp <dp1...dp8>: Defines the mapping from CoS to drop precedence (DP). <dp1...dp8> are eight DP values corresponding to CoS values 0 to 7, separated by spaces, each ranging from 0 to 2.

cos-intp <in-cos list>: Defines the mapping from ingress Layer 2 CoS values to internal priority. <in-cos list> is eight internal priority values corresponding to CoS values 0 to 7, separated by spaces, each ranging from 0 to 7.

dscp-dscp: Defines the mapping from ingress DSCP to egress DSCP. <in-dscp list> is up to eight ingress DSCP values separated by spaces, each ranging from 0 to 63; <out-dscp> is the egress DSCP value, ranging from 0 to 63.

dscp-intp: Defines the mapping from DSCP to internal priority.

dscp-dp: Defines the mapping from DSCP to drop precedence.

intp-exp <exp1...exp8>: Defines the mapping from internal priority to EXP. <exp1...exp8> are eight EXP values corresponding to internal priorities 0 to 7, separated by spaces, each ranging from 0 to 7.

Default: The default mappings are as follows:

```
Ingress COS-TO-Drop-Precedence map:
COS:  0   1   2   3   4   5   6   7
 ----------------------------------------
```

```
DP:   0   0   0   0   0   0   0   0
Ingress COS-TO-Internal-Priority map:
COS:  0   1   2   3   4   5   6   7
 ----------------------------------------
INTP: 0   1   2   3   4   5   6   7
Ingress DSCP-TO-Internal-Priority map:
d1 : d2  0   1   2   3   4   5   6   7   8   9
0:       0   0   0   0   0   0   0   0   1   1
1:       1   1   1   1   1   1   2   2   2   2
2:       2   2   2   2   3   3   3   3   3   3
3:       3   3   4   4   4   4   4   4   4   4
4:       5   5   5   5   5   5   5   5   6   6
5:       6   6   6   6   6   6   7   7   7   7
6:       7   7   7   7
Ingress DSCP-TO-DSCP map:
d1 : d2  0   1   2   3   4   5   6   7   8   9
0:       0   0   0   0   0   0   0   0   8   8
1:       8   8   8   8   8   8  16  16  16  16
2:      16  16  16  16  24  24  24  24  24  24
3:      24  24  32  32  32  32  32  32  32  32
4:      40  40  40  40  40  40  40  40  48  48
5:      48  48  48  48  48  48  56  56  56  56
6:      56  56  56  56
Ingress DSCP-TO-Drop-Precedence map:
d1 : d2  0   1   2   3   4   5   6   7   8   9
0:       0   0   0   0   0   0   0   0   0   0
1:       0   0   0   0   0   0   0   0   0   0
2:       0   0   0   0   0   0   0   0   0   0
3:       0   0   0   0   0   0   0   0   0   0
4:       0   0   0   0   0   0   0   0   0   0
5:       0   0   0   0   0   0   0   0   0   0
6:       0   0   0   0
Egress Internal-Priority-TO-EXP map:
INTP: 0   1   2   3   4   5   6   7
 ----------------------------------------
EXP:  0   1   2   3   4   5   6   7
```

Command Mode: Global Mode.

Usage Guidelines: INTP is the internal priority of the chip, and DP is the drop precedence. Because there are 64 DSCP values but only 8 internal priorities, every 8 consecutive DSCP values map to the same INTP or DP.

Example: 1. Change the CoS-to-DP mapping from the default to 1 1 1 1 1 1 1 1.

```
Switch(config)#mls qos map cos-dp 1 1 1 1 1 1 1 1
```

2. Map DSCP 1 to DP 2.

```
Switch(config)#mls qos map dscp-dp 1 to 2
```

7.14.11 mls qos queue weight

Command: `mls qos queue weight <weight0..weight7>`
`no mls qos queue weight`

Function: Sets the queue weights.

Parameters: <weight0..weight7>: The queue weights, each ranging from 0 to 255. They take effect for the WDRR algorithm but not for the SP algorithm. Only the relative values matter; WDRR allocates bandwidth according to the eight weights.

Default: 1 1 1 1 1 1 1 0; the weight of the eighth queue can be configured by the user.

Command Mode: Global Mode.

Usage Guidelines: A queue with weight 0 is scheduled by SP; a queue with a nonzero weight is scheduled by WDRR, giving SP+WDRR scheduling. Within the WDRR group, queues are selected by the WDRR algorithm; the WDRR group and the SP queues are scheduled in strict priority order.

Example: Set the queue weights to 1 2 3 4 5 6 7 8.

```
Switch(config)#mls qos queue weight 1 2 3 4 5 6 7 8
```

7.14.12 mls qos trust

Command: `mls qos trust {cos | dscp|exp}`
`no mls qos trust {cos | dscp|exp}`

Function: Configures the trust mode of the port. The **no** form of this command disables the current trust mode of the port.

Parameters: cos: Trusts the CoS value. **dscp**: Trusts the DSCP value. **exp**: Trusts the EXP value.

Default: Trust CoS.

Command Mode: Port Mode.

Usage Guidelines:

In trust DSCP mode, the internal priority is set according to the DSCP-to-INTP mapping, the drop precedence according to the DSCP-to-DP mapping, and the DSCP value according to the DSCP-to-DSCP mapping.

Example:

```
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0)# mls qos trust dscp
```

7.14.13 pass-through-cos

Command: `pass-through-cos`
`no pass-through-cos`

Function: Prevents the Layer 2 CoS value from being rewritten when packets egress.

Parameters: None.

Default: The Layer 2 CoS value can be rewritten at egress.

Command Mode: Port Mode.

Usage Guidelines:

By default, the Layer 2 CoS value can be rewritten when packets egress. When pass-through-cos is configured on the ingress port, the Layer 2 CoS value is not rewritten on the egress port. This command can be used with other QoS commands, such as **mls qos trust**: after other QoS actions take effect, the CoS value carried at ingress is retained at egress.

Example: Trust DSCP on port Ethernet 1/0/1, so that packets are classified by DSCP, but keep the CoS value of the packets unchanged.

```
switch(config-if-ethernet1/0/1)#pass-through-cos
```

7.14.14 pass-through-dscp-exp

Command: `pass-through-dscp`
`no pass-through-dscp`

Function: Prevents the DSCP value of packets from being rewritten at egress.

Parameters: None.

Default: The DSCP value of packets can be rewritten at egress.

Command Mode: Port Mode.

Usage Guidelines: When pass-through-dscp is configured on the ingress port, the DSCP value is not rewritten at egress. This command can be used with other QoS commands, such as **mls qos trust**: after the QoS actions take effect, the original DSCP value is retained at egress.

Example: Trust CoS on port Ethernet 1/0/1 (classify packets by CoS) and keep the original DSCP value at egress.

```
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#mls qos trust cos
Switch(config-if-ethernet1/0/1)#pass-through-dscp
```

7.14.15 policy

Command:

Single Bucket Mode:

policy <bits_per_second> <normal_burst_bytes> ({conform-action ACTION | exceed-action ACTION})

Dual Bucket Mode:

policy <bits_per_second> <normal_burst_bytes> [pir <peak_rate_bps>] | <maximum_burst_bytes> [{conform-action ACTION | exceed-action ACTION | violate-action ACTION }]

ACTION definition:

drop | transmit | set-dscp-transmit <dscp_value> | set-prec-transmit <ip_precedence_value> | set-cos-transmit <cos_value> | set-internal-priority <inp_value> | set-Drop-Precedence <dp_value>

no policy

Function: Configures a non-aggregate three-color policer: sets the token bucket mode (single-rate single-bucket, single-rate dual-bucket, or dual-rate dual-bucket) and the actions for packets of each color. The **no** form of this command deletes the configuration.

Parameters: <bits_per_second>: The committed information rate (CIR), in kbps, ranging from 1 to 10000000.

<normal_burst_bytes>: The committed burst size (CBS), in bytes, ranging from 1 to 1000000. If the configured CBS exceeds the chip limit, the hardware is configured with the maximum value supported by the chip, without a CLI prompt.

<maximum_burst_bytes>: The peak burst size (PBS), in bytes, ranging from 1 to 10000000. If the configured PBS exceeds the chip limit, the hardware is configured with the maximum value supported by the chip, without a CLI prompt. Note: This parameter exists only in dual-bucket mode.

pir <peak_rate_bps>: The peak information rate (PIR), in kbps, ranging from 1 to 10000000. If PIR is not configured, the policer works in single-rate dual-bucket mode; otherwise, in dual-rate dual-bucket mode. Note: This parameter exists only in dual-bucket mode.

violate-action: The action for red packets, which exceed the PIR. The default is drop.

conform-action: The action for green packets, which do not exceed the CIR. The default is transmit.

exceed-action: The action for yellow packets, which exceed the CIR but not the PIR. The default is drop.

ACTION includes:

drop / **transmit**: Drops or transmits the packets.

set-dscp-transmit: Sets the DSCP value; applies to IPv4 and IPv6 packets. Only one of set-dscp-transmit and set-prec-transmit can be selected.

set-prec-transmit: Sets the IP precedence (ToS). Only one of set-prec-transmit and set-dscp-transmit can be selected.

set-internal-priority: Sets the internal priority of the packets.

set-Drop-Precedence: Sets the drop precedence of the packets.

set-cos-transmit: Sets the Layer 2 CoS value of the packets.

Default: No policer action. The default conform-action is transmit; the default exceed-action and violate-action are drop.

Command Mode: Policy Class Map Mode.

Usage Guidelines:

The CLI supports both single-bucket and dual-bucket configuration, determined by whether PIR or PBS is configured. If an action is configured directly after the CBS, the mode is single-bucket two-color; if only PBS is configured, the mode is single-rate dual-bucket three-color; if both PIR and PBS are configured, the mode is dual-rate dual-bucket three-color. If both **set** and **policy** (or **policy aggregate**) are configured in a policy map with the same action, the **policy** action overrides the **set** action.

Example: In Policy Class Map Mode, set the CIR to 1000 and the CBS to 2000; for packets that do not exceed the CIR, change the DSCP to 23 and transmit them; transmit packets that exceed the CIR unchanged.

```
Switch(config)#class-map cm
Switch(config-classmap-cm)#match cos 0
Switch(config-classmap-cm)#exit
Switch(config)#policy-map 1
Switch(config-policymap-1)#class cm
Switch(config-policymap-1-class-cm)#policy 1000 2000 conform-action set-dscp-
transmit 23
```

7.14.16 policy aggregate

Command: policy aggregate <aggregate-policy-name>
no policy aggregate <aggregate-policy-name>

Function: Applies an aggregate policer to the classified traffic in the policy map. The **no** form of this command deletes the aggregate policer.

Parameters: <aggregate-policy-name> is the name of the aggregate policer.

Default: No aggregate policer is applied.

Command Mode: Policy Class Map Mode.

Usage Guidelines: The same aggregate policer can be referenced by different policy class maps.

Example: Create class map cm to match CoS 0, create policy map 1, enter Policy Class Map Mode, and apply aggregate policer color.

```
Switch(config)#class-map cm
Switch(config-classmap-cm)#match cos 0
Switch(config-classmap-cm)#exit
Switch(config)#policy-map 1
Switch(config-policymap-1)#class cm
Switch(config-policymap-1-class-cm)#policy aggregate color
```

7.14.17 policy-map

Command: policy-map <policy-map-name>
no policy-map <policy-map-name>

Function: Creates a policy map and enters Policy Map Mode. The **no policy-map <policy-map-name>** command deletes the policy map.

Parameters: <policy-map-name> is the policy map name.

Default: No policy map is configured.

Command Mode: Global Mode.

Usage Guidelines: PBR classification and next-hop marking can be configured in Policy Map Mode.

Example: Create and delete a policy map named p1.

```
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#exit
Switch(config)#no policy-map p1
```

7.14.18 service-policy input

Command: service-policy input <policy-map-name>
no service-policy input {<policy-map-name>}

Function: Applies a policy map to the specified port. The **no** form of this command deletes the specified policy map from the port, or all policy maps applied in the ingress direction of the port.

Parameters: input <policy-map-name>: Applies the specified policy map to the ingress direction of the switch port.

If no policy map name is specified in the **no** form, all policy maps applied in the ingress direction of the port are deleted.

Default: No policy map is bound to the port.

Command Mode: Port Mode.

Usage Guidelines: Only one policy map can be applied to each direction of a port or VLAN interface. Applying policy maps to a VLAN and to ports in that VLAN at the same time is not recommended.

Example:

Bind policy map p1 to the ingress direction of port Ethernet 1/0/1.

```
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#service-policy input p1
```

Bind policy map p1 to the ingress direction of interface VLAN 1.

```
Switch(config)#interface vlan 1
Switch(Config-If-vlan1)#service-policy input p1
```

7.14.19 service-policy input vlan

Command: service-policy input <policy-map-name> vlan <vlan-list>
no service-policy input {<policy-map-name>} vlan < vlan-list>

Function: Applies a policy map to the specified VLANs. The **no** form of this command deletes the specified policy map from the VLANs, or all policy maps applied in the ingress direction of the VLANs.

Parameters: input <policy-map-name>: Applies the specified policy map to the ingress direction of the VLANs.

vlan <vlan-list>: The list of VLANs to which the policy map is bound.

If no policy map name is specified in the **no** form, all policy maps applied in the ingress direction of the VLANs are deleted.

Default: No policy map is bound to the VLAN.

Command Mode: Global Mode.

Usage Guidelines: Only one policy map can be applied to each direction of a port or VLAN interface. Applying policy maps to a VLAN and to ports in that VLAN at the same time is not recommended.

Example:

Bind policy map p1 to the ingress direction of VLANs 2, 3, 4, and 6.

```
Switch(config)# service-policy input p1 vlan 2-4;6
```

7.14.20 set

Command: set {ip dscp <new-dscp> | internal priority <new-inp> | ip [default] nexthop [vrf <vrf>] <ip-address> | ipv6 [default] nexthop [vrf <vrf>] <nexthop-ip> | cos <new-cos>}

no set {ip dscp | internal priority | ip nexthop | ipv6 nexthop | cos}

Function: Assigns new values (DSCP, internal priority, next hop, or CoS) to the classified traffic. The **no** form of this command cancels the assignment.

Parameters: ip dscp <new-dscp>: The new DSCP value; applies to both IPv4 and IPv6.

ipv6 flowlabel <new-flowlabel>: The new IPv6 flow label value.

ip [default] nexthop [vrf <vrf>] <ip-address>: The next-hop IP address for PBR. **default** specifies a route with the lowest priority, lower than route maps and neighbor maps. **vrf** specifies the VRF.

ipv6 [default] nexthop [vrf <vrf>] <nexthop-ip>: The next-hop IPv6 address for IPv6 PBR. **default** specifies a route with the lowest priority, lower than route maps and neighbor maps. **vrf** specifies the VRF.

cos <new-cos>: The new CoS value.

Default: No values are assigned.

Command Mode: Policy Class Map Mode.

Usage Guidelines: Only classified traffic that matches the match criterion is assigned the new values.

Example: Set the IP DSCP of packets that match class c1 to 3.

```
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#set ip dscp 3
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
```

7.14.21 show class-map

Command: show class-map [<class-map-name>]

Function: Displays QoS class maps.

Parameters: <class-map-name> is the class map name.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays all configured class maps or the specified class map.

Example:

```
Switch # show class-map
Class map name:c1, used by 1 times
  match acl name:1
```

Output	Description
Class map name:c1	Name of the class map
used by 1 times	Number of times the class map is used
match acl name:1	Classification rule of the class map

7.14.22 show policy-map

Command: show policy-map [<policy-map-name>]

Function: Displays QoS policy maps.

Parameters: <policy-map-name> is the policy map name.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays all configured policy maps or the specified policy map.

Example:

```
Switch#show policy -map
Policy Map p1, used by 0 port
  Class Map name: c1
    policy CIR: 1000 CBS: 1000  PIR: 200 PBS: 3000
    conform-action:
     transmit
    exceed-action:
     drop
    violate-action:
     drop
```

Output	Description
Policy Map p1	Name of the policy map
Class map name:c1	Name of the class map referenced
policy CIR: 1000 CBS: 1000 PIR: 200 PBS: 3000 conform-action: transmit exceed-action: drop violate-action: drop	Policer configuration applied

7.14.23 show mls qos interface

Command: show mls qos {interface [<interface-id>] [policy | queuing] | vlan <vlan-id>} | [begin | include | exclude <regular-expression>]

Function: Displays the QoS configuration of a port or VLAN.

Parameters: <interface-id> is the port ID. **<vlan-id>** is the VLAN ID. **policy** displays the policy settings of the port. **queuing** displays the queue settings of the port.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: In single-rate single-bucket mode, packets passing the policer are either red or green; in the output, in-profile means green and out-profile means red. In dual-bucket mode, packets have three colors, but the counters count only two kinds: red and yellow packets are both counted as out-profile. Statistics are available only for ingress policies.

Example:

```
Switch#show mls qos interface ethernet 1/0/2
Ethernet 1/0/2
Default COS: 0
Trust: COS DSCP EXP
Attached Policy Map for Ingress: p1
Classmap    classified    in-profile    out-profile (in packets)
    c1          20             10             10
  c2          NA            NA             NA
```

(NA is displayed if accounting is not configured for the class map.)

```
Internal-Priority-TO-Queue map:
INTP      0     1     2     3     4     5     6     7
-------------------------------------------------------------------------------
-
Queue     0     1     2     3     4     5     6     7
Queue Algorithm: WRR
Queue weights:
Queue      0     1     2     3     4     5     6     7
-------------------------------------------------------------------------------
----------------------------
weight     1     2     3     4     5     6     7     8
Bandwidth Guarantee Configuration:
Queue      0     1     2     3     4     5     6     7
-------------------------------------------------------------------------------
----------------------------
MinBW(K)   128       0        0     0     0    0        0     0
  MaxBW(K)  256   0  0     0     0    0        0     0
```

Output	Description
Ethernet1/0/2	Port name
default cos:0	Default CoS value of the port
Trust: COS DSCP EXP	Trust state of the port
Attached Policy Map for Ingress: p1	Policy map bound to the port
ClassMap	Class map name
classified	Total packets that match the class map; NA is displayed if accounting is not configured for the class map.
in-profile	Total in-profile packets that match the class map; NA is displayed if accounting is not configured for the class map.
out-profile	Total out-profile packets that match the class map; NA is displayed if accounting is not configured for the class map.
Internal-Priority-TO-Queue map::	Mapping from internal priority to queue
Queue Algorithm:	Queue scheduling method (WRR or PQ)
Queue weights	Queue weight configuration
Bandwidth Guarantee Configuration	Bandwidth guarantee configuration

```
Switch(config)#show mls qos interface ethernet1/0/2 queuing
Ethernet1/0/2:
Internal-Priority-TO-Queue map:
INTP  0     1     2     3     4     5     6     7
-------------------------------------------------------------------------------
-
Queue   0     1     2     3     4     5     6     7
Queue Algorithm: WRR
Queue weights:
Queue      0     1     2     3     4     5     6     7
-------------------------------------------------------------------------------
----------------------------
weight     1     2     3     4     5     6     7     8
Bandwidth Guarantee Configuration:
Queue      0     1     2     3     4     5     6     7
-------------------------------------------------------------------------------
----------------------------
MinBW(K)   128       0        0     0     0    0        0     0
```

```
MaxBW(K)  256    0     0     0     0    0        0     0
```

Output	Description
Internal-Priority-TO-Queue map::	Mapping from internal priority to queue
Queue Algorithm:	Queue scheduling method (WRR or PQ)
Queue weights	Queue weight configuration
Bandwidth Guarantee Configuration	Bandwidth guarantee configuration

```
Switch # show mls qos interface ethernet 1/0/2 policy
Ethernet1/0/2:
Attached Policy Map for Ingress: p1
Accounting: ON
Classmap    classified    in-profile    out-profile (in packets)
  c1          0             0             0
```

Output	Description
Ethernet1/0/2	Port name
Attached Policy Map for Ingress: p1	Policy map bound to the port
ClassMap	Class map name
classified	Total packets that match the class map
in-profile	Total in-profile packets that match the class map
out-profile	Total out-profile packets that match the class map

```
Switch #show mls qos vlan 100
Vlan 100:
Attached Policy Map for Ingress: p1
Classmap    classified    in-profile    out-profile (in packets)
    c1          20            10            10
  c2          NA            NA            NA
```

7.14.24 show mls qos in {interface <interface-name> policy | vlan <vlan-id>

Command: show mls qos in {interface <interface-name> policy | vlan <vlan-id>

Function: Displays the inbound policy configuration of a port or VLAN.

Parameters: <interface-name>: The port name. **<vlan-id>**: The VLAN ID.

Command Mode: Admin Mode and Configuration Mode.

Default: None.

Usage Guidelines: Displays the inbound policy configuration.

Example: Display the inbound policy configuration.

```
Switch#show mls qos in interface ethernet1/0 policy
Ethernet1/0:
Attached Policy Map for Ingress: p
```

7.14.25 show mls qos maps

Command: show mls qos maps [cos-dp| cos-intp | dscp-dscp | dscp-intp | dscp-dp |intp-exp] | [begin | include | exclude <regular-expression>]

Function: Displays the QoS mapping configuration.

Parameters: cos-dp: Mapping from ingress Layer 2 CoS to drop precedence.

cos-intp: Mapping from ingress Layer 2 CoS to internal priority.

dscp-dscp: Mapping from ingress DSCP to DSCP.

dscp-intp: Mapping from ingress DSCP to internal priority.

dscp-dp: Mapping from ingress DSCP to drop precedence.

intp-exp: Mapping from internal priority to EXP.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the QoS mapping configuration.

Example: Display the mapping tables.

```
Switch (config)#show mls qos maps
Ingress COS-TO-Internal-Priority map:
COS:  0   1   2   3   4   5   6   7
 ----------------------------------------
INTP: 0   1   2   3   4   5   6   7
Ingress DSCP-TO-Internal-Priority map:
d1 : d2  0   1   2   3   4   5   6   7   8   9
0:       0   0   0   0   0   0   0   0   1   1
1:       1   1   1   1   1   1   2   2   2   2
2:       2   2   2   2   3   3   3   3   3   3
3:       3   3   4   4   4   4   4   4   4   4
4:       5   5   5   5   5   5   5   5   6   6
5:       6   6   6   6   6   6   7   7   7   7
6:       7   7   7   7
Ingress COS-TO-Drop-Precedence map:
COS:  0   1   2   3   4   5   6   7
 ----------------------------------------
DP:   0   0   0   0   0   0   0   0
Ingress DSCP-TO-DSCP map:
d1 : d2  0   1   2   3   4   5   6   7   8   9
0:       0   0   0   0   0   0   0   0   8   8
1:       8   8   8   8   8   8  16  16  16  16
2:      16  16  16  16  24  24  24  24  24  24
3:      24  24  32  32  32  32  32  32  32  32
4:      40  40  40  40  40  40  40  40  48  48
5:      48  48  48  48  48  48  56  56  56  56
6:      56  56  56  56
Ingress DSCP-TO-Drop-Precedence map:
d1 : d2  0   1   2   3   4   5   6   7   8   9
0:       0   0   0   0   0   0   0   0   0   0
1:       0   0   0   0   0   0   0   0   0   0
2:       0   0   0   0   0   0   0   0   0   0
3:       0   0   0   0   0   0   0   0   0   0
4:       0   0   0   0   0   0   0   0   0   0
5:       0   0   0   0   0   0   0   0   0   0
6:       0   0   0   0
Ingress EXP-TO-Internal-Priority map:
EXP:  0   1   2   3   4   5   6   7
 ----------------------------------------
INTP: 0   1   2   3   4   5   6   7
Ingress EXP-TO-Drop-Precedence map:
EXP:  0   1   2   3   4   5   6   7
 ----------------------------------------
DP:   0   0   0   0   0   0   0   0
Egress Internal-Priority-TO-EXP map:
INTP: 0   1   2   3   4   5   6   7
 ----------------------------------------
EXP:  0   1   2   3   4   5   6   7
```

7.14.26 show mls qos vlan

Command: show mls qos vlan <v-id>

Function: Displays the QoS configuration of the VLAN.

Parameters: <v-id>: The VLAN ID, ranging from 1 to 4094.

Command Mode: Admin Mode.

Default: None.

Example:

```
Switch#show mls qos vlan 1
```

7.14.27 show mls qos aggregate-policy

Command: show mls qos aggregate-policy [<aggregate-policy-name>]

Function: Displays the aggregate policer configuration.

Parameters: <aggregate-policy-name>: The aggregate policer name.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the aggregate policer configuration.

Example:

```
Switch#show mls qos aggregate-policy
aggregate policy p
CIR: 1    CBS: 1    PBS: 1
 conform-action:
  transmit
    exceed-action:
     drop
    violate-action:
     drop
 Not used by any policy map
```

7.14.28 transmit

Command: transmit
no transmit

Function: Transmits packets that match the class. The **no** form of this command cancels the action.

Parameters: None.

Default: No action.

Command Mode: Policy Class Map Mode.

Usage Guidelines: After this command is configured, matching packets are transmitted directly.

Example: Transmit packets that match class c1.

```
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#transmit
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
```

7.15 Flow-based Redirection

7.15.1 access-group redirect to interface ethernet

Command: access-group <aclname> redirect to interface [ethernet <IFNAME> | <IFNAME>]
no access-group <aclname> redirect

Function: Configures flow-based redirection. The **no access-group <aclname> redirect** command deletes the flow-based redirection.

Parameters: <aclname>: The name of the flow (ACL). Only numbered standard IP ACLs, numbered extended IP ACLs, named standard IP ACLs, named extended IP ACLs, numbered standard IPv6 ACLs, and named standard IPv6 ACLs are supported. The ACL cannot contain time range or port range parameters, and its rules must be permit rules. **<IFNAME>**: The destination port of the redirection.

Command Mode: Port Mode.

Usage Guidelines: Flow-based redirection forwards data frames that meet specific conditions to another specified port. The **no access-group <aclname> redirect** command deletes the flow-based redirection.

Example: Redirect frames with source IP address 192.168.1.111 received on port 1 to port 6.

```
Switch(config)#access-list 1 permit host 192.168.1.111
Switch(config)# interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)# access-group 1 redirect to interface
ethernet 1/0/6
```

7.15.2 match vlan <1-4096> redirect interface (ethernet|) IFNAME

Command: match vlan <1-4096> redirect interface (ethernet|) IFNAME
no match vlan <1-4096> redirect

Command Mode: Port Mode.

Function: Configures VLAN redirection on the port.

Parameters: vlan <1-4096>: The VLAN ID.

IFNAME: The port name.

Usage Guidelines: Redirects traffic of the specified VLAN received on this port to another port.

Example: Redirect traffic of VLAN 1 received on port Ethernet 1/0/1 to port Ethernet 1/0/2.

```
(config-if-ethernet1/0/1)#match vlan 1 redirect interface ethernet 1/0/2
```

7.15.3 port-redirect match vlan <1-4094> source-port interface (ethernet|) IFNAME destination-port interface (ethernet|) IFNAME

Command: port-redirect match vlan <1-4094> source-port interface (ethernet|) IFNAME destination-port interface (ethernet|) IFNAME
no port-redirect match vlan <1-4094> source-port interface (ethernet|) IFNAME destination-port interface (ethernet|) IFNAME

Function: Configures VLAN redirection between ports.

Parameters: vlan <1-4094>: The VLAN ID.

IFNAME: The port name.

Command Mode: Global Mode.

Usage Guidelines: Redirects traffic of the specified VLAN from the source port to the destination port. The source and destination ports must be trunk ports.

Example: Redirect traffic of VLAN 1 from port Ethernet 1/0/1 to port Ethernet 1/0/2.

```
(config)#port-redirect match vlan 1 source-port interface ethernet 1/0/1
destination-port interface ethernet 1/0/2
```

7.15.4 show flow-based-redirect

Command: show flow-based-redirect {interface [ethernet <IFNAME> | <IFNAME>]}

Function: Displays the current flow-based redirection configuration of the system or of ports.

Parameters: If no port is specified, all flow-based redirection configuration in the system is displayed.

If ports are specified in **<IFNAME>**, the flow-based redirection configured on those ports is displayed.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the current flow-based redirection configuration of the system or of ports.

Example:

```
Switch(config)# show flow-based-redirect
Flow-based-redirect config on interface ethernet 1/0/1:
         RX flow (access-list 1) is redirected to interface Ethernet1/0/6
```

7.15.5 vlan-port-redirect vlan maximum <1-1000>

Command: vlan-port-redirect vlan maximum <1-1000>
no vlan-port-redirect vlan maximum

Command Mode: Global Mode.

Function: Configures the maximum number of redirected VLANs on each port.

Default: 500.

Parameters: maximum <1-1000>: The maximum number of VLANs.

Usage Guidelines: Configures the maximum number of redirected VLANs on each port.

Example: Set the maximum number of redirected VLANs per port to 600.

```
(config)# vlan-port-redirect vlan maximum 600
```

7.16 Egress QoS

7.16.1 mls qos egress green remark

Command: [no] mls qos egress green remark

Function: Enables egress QoS remarking for green packets. The **no** form of this command disables remarking for green packets.

Parameters: None.

Default: Green packets are not remarked.

Command Mode: Global Mode.

Usage Guidelines: After this global configuration is enabled, the QoS attributes of green packets are changed according to the remark tables.

Example: Enable egress remarking for green packets.

```
Switch(config)#mls qos egress green remark
```

7.16.2 mls qos map

Command: `mls qos map cos-cos <color> <cos1…cos8>`
`mls qos map cos-dscp <color> <dscp1…dscp8>`
`mls qos map dscp-cos <color> <dscp list> to <cos>`
`mls qos map dscp-dscp <color> <dscp list> to <dscp>`
`no mls qos map (cos-cos | cos-dscp | dscp-cos | dscp-dscp) <color>`

Function: Configures the egress QoS remark mapping tables. The **no** form of this command restores the default.

Parameters: cos-cos: Sets the CoS-to-CoS mapping of the egress CoS remark table.

cos-dscp: Sets the CoS-to-DSCP mapping of the egress CoS remark table.

dscp-cos: Sets the DSCP-to-CoS mapping of the egress DSCP remark table.

dscp-dscp: Sets the DSCP-to-DSCP mapping of the egress DSCP remark table.

<color>: The packet color: green, yellow, or red.

<cos>: The CoS value, ranging from 0 to 7.

<dscp>: The DSCP value, ranging from 0 to 63.

<dscp list>: One to eight DSCP values.

Default: The default mappings are as follows:

```
COS-TO-COS-GREEN map:
COS:  0   1   2   3   4   5   6   7
 ----------------------------------------
COS: 0   1   2   3   4   5   6   7
COS-TO-COS-YELLOW map:
COS:  0   1   2   3   4   5   6   7
 ----------------------------------------
COS: 0   1   2   3   4   5   6   7
COS-TO-COS-RED map:
COS:  0   1   2   3   4   5   6   7
 ----------------------------------------
COS: 0   1   2   3   4   5   6   7
COS-TO-DSCP-GREEN map:
COS:  0   1   2   3   4   5   6   7
 ----------------------------------------
DSCP: 0   8   16  24  32  40  48  56
COS-TO-DSCP-YELLOW map:
COS:  0   1   2   3   4   5   6   7
 ----------------------------------------
DSCP: 0   8   16  24  32  40  48  56
COS-TO-DSCP-RED map:
COS:  0   1   2   3   4   5   6   7
 ----------------------------------------
DSCP: 0   8   16  24  32  40  48  56
DSCP-TO-COS-GREEN map:
d1 : d2  0   1   2   3   4   5   6   7   8   9
0:       0   0   0   0   0   0   0   0   1   1
1:       1   1   1   1   1   1   2   2   2   2
2:       2   2   2   2   3   3   3   3   3   3
3:       3   3   4   4   4   4   4   4   4   4
4:       5   5   5   5   5   5   5   5   6   6
5:       6   6   6   6   6   6   7   7   7   7
6:       7   7   7   7
DSCP-TO-COS-YELLOW map:
d1 : d2  0   1   2   3   4   5   6   7   8   9
0:       0   0   0   0   0   0   0   0   1   1
1:       1   1   1   1   1   1   2   2   2   2
2:       2   2   2   2   3   3   3   3   3   3
3:       3   3   4   4   4   4   4   4   4   4
```

```
4:       5   5   5   5   5   5   5   5   6   6
5:       6   6   6   6   6   6   7   7   7   7
6:       7   7   7   7
DSCP-TO-COS-RED map:
d1 : d2  0   1   2   3   4   5   6   7   8   9
0:       0   0   0   0   0   0   0   0   1   1
1:       1   1   1   1   1   1   2   2   2   2
2:       2   2   2   2   3   3   3   3   3   3
3:       3   3   4   4   4   4   4   4   4   4
4:       5   5   5   5   5   5   5   5   6   6
5:       6   6   6   6   6   6   7   7   7   7
6:       7   7   7   7
DSCP-TO-DSCP-GREEN map:
d1 : d2  0   1   2   3   4   5   6   7   8   9
0:       0  10   2   3   4   5   6   7   8   9
1:      10  11  12  13  14  15  16  17  18  19
2:      20  21  22  23  24  25  26  27  28  29
3:      30  31  32  33  34  35  36  37  38  39
4:      40  41  42  43  44  45  46  47  48  49
5:      50  51  52  53  54  55  56  57  58  59
6:      60  61  62  63
DSCP-TO-DSCP-YELLOW map:
d1 : d2  0   1   2   3   4   5   6   7   8   9
0:       0   9   2   3   4   5   6   7   8   9
1:      10  11  12  13  14  15  16  17  18  19
2:      20  21  22  23  24  25  26  27  28  29
3:      30  31  32  33  34  35  36  37  38  39
4:      40  41  42  43  44  45  46  47  48  49
5:      50  51  52  53  54  55  56  57  58  59
6:      60  61  62  63
DSCP-TO-DSCP-RED map:
d1 : d2  0   1   2   3   4   5   6   7   8   9
0:       0   1   2   3   4   5   6   7   8   9
1:      10  11  12  13  14  15  16  17  18  19
2:      20  21  22  23  24  25  26  27  28  29
3:      30  31  32  33  34  35  36  37  38  39
4:      40  41  42  43  44  45  46  47  48  49
5:      50  51  52  53  54  55  56  57  58  59
6:      60  61  62  63
```

Command Mode: Global Mode.

Usage Guidelines: The egress remark mapping tables are global; they define how the QoS attributes of packets of different colors are changed.

Example: Change the DSCP value 0 of yellow packets to 3.

```
Switch(config)#mls qos map dscp-dscp yellow 0 to 3
```

7.16.3 service-policy output

Command: `service-policy output <policy-map-name>`
`no service-policy output {<policy-map-name>}`

Function: Applies a policy map to the egress direction of the port. The **no** form of this command deletes the specified policy map from the port, or all policy maps applied in the egress direction of the port.

Parameters: output <policy-map-name>: Applies the specified policy map to the egress direction of the port.

If no policy map name is specified in the **no** form, all policy maps in the egress direction of the port are deleted.

Default: No policy map is bound to the port.

Command Mode: Port Mode.

Usage Guidelines: Only one policy map can be applied to each direction of a port. A policy map that uses rules or actions not supported by the egress filter processor (EFP) may fail to bind to the port.

Example: Bind policy map p1 to the egress direction of port Ethernet 1/0/1.

```
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#service-policy output p1
```

7.16.4 service-policy output vlan

Command: service-policy output <policy-map-name> vlan <vlan-list>
no service-policy output {<policy-map-name>} vlan <vlan-list>

Function: Applies a policy map to the specified VLANs. The **no** form of this command deletes the specified policy map from the VLANs, or all policy maps applied in the egress direction of the VLANs.

Parameters: output <policy-map-name>: Applies the specified policy map to the egress direction of the VLANs.

If no policy map name is specified in the **no** form, all policy maps in the egress direction of the VLANs are deleted.

Default: No policy map is bound to the VLAN.

Command Mode: Global Mode.

Usage Guidelines: Only one policy map can be applied to each direction of a VLAN. A policy map that uses rules or actions not supported by the EFP may fail to bind.

Example: Bind policy map p1 to the egress direction of VLAN 1.

```
Switch(config)#service-policy output p1 vlan 1
```

7.16.5 set

Command: set {ip dscp <new-dscp> | ip precedence <new-precedence> | cos <new-cos> | c-vid <new-c-vid> | s-vid <new-s-vid> | s-tpid <new-s-tpid>}
no set {ip dscp | ip precedence | cos | c-vid | s-vid | s-tpid}

Function: Assigns new values (DSCP, IP precedence, CoS, C-VID, S-VID, or S-TPID) to the classified traffic. The **no** form of this command cancels the assignment.

Parameters: ip dscp <new-dscp>: The new DSCP value of IPv4 and IPv6 packets.

ip precedence <new-precedence>: The new IPv4 precedence. Only one of IP precedence and IP DSCP can be selected.

cos <new-cos>: The new CoS value.

c-vid <new-c-vid>: The new C-VID value.

s-vid <new-s-vid>: The new S-VID value.

s-tpid <new-s-tpid>: The new S-TPID value.

Default: No values are assigned.

Command Mode: Policy Class Map Mode.

Usage Guidelines: Only classified traffic that matches the match criterion is assigned the new values.

Example: Set the IP precedence of packets that match class c1 to 3.

```
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#set ip precedence 3
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
```

7.16.6 show mls qos egress green remark

Command: show mls qos egress green remark

Function: Displays whether egress remarking applies to green packets.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays whether the egress remark mapping applies to green packets.

Example: Display whether egress remarking applies to green packets.

```
Switch(config)#show mls qos egress green remark
Green remarking: Disable.
```

7.16.7 show mls qos maps

Command: show mls qos maps (cos-cos | cos-dscp | dscp-cos | dscp-dscp) <color>

Function: Displays the egress remark mapping.

Parameters: cos-cos: The CoS-to-CoS mapping of the egress CoS remark table.

cos-dscp: The CoS-to-DSCP mapping of the egress CoS remark table.

dscp-cos: The DSCP-to-CoS mapping of the egress DSCP remark table.

dscp-dscp: The DSCP-to-DSCP mapping of the egress DSCP remark table.

<color>: The packet color: green, yellow, or red.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the egress remark mapping tables.

Example: Display the CoS-to-CoS mapping for green packets.

```
Switch(config)#show mls qos maps cos-cos green
COS-TO-COS-GREEN map:
COS:  0   1   2   3   4   5   6   7
 ----------------------------------------
COS: 0   1   2   3   4   5   6   7
Green remarking: Disable.
```

7.17 Flexible QinQ

7.17.1 Add

Command: add s-vid <new-vid>
no add s-vid

Function: Adds an outer VLAN tag to packets that match the class map. The **no** form of this command cancels the operation.

Parameters: s-vid <new-vid>: The VID of the outer VLAN tag.

Default: No tag is added.

Command Mode: Policy Class Map Mode.

Usage Guidelines: After this command is configured, an outer tag is added to packets that match the class map.

Example: Add an outer VLAN tag with VID 2 to packets that match class c1.

```
Switch(config)#policy-map p1
```

```
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#add s-vid 2
```

7.17.2 Match

Command: match {access-group <acl-index-or-name> | ip dscp <dscp-list>| ip precedence <ip-precedence-list>| ipv6 access-group <acl-index-or-name>| ipv6 dscp <dscp-list> | ipv6 flowlabel <flowlabel-list> | vlan <vlan-list> | cos <cos-list>}

no match {access-group | ip dscp | ip precedence | ipv6 access-group | ipv6 dscp | ipv6 flowlabel | vlan | cos}

Function: Configures the match criterion of the class map. The **no** form of this command deletes the specified match criterion.

Parameters: access-group <acl-index-or-name>: Matches the specified IP ACL or MAC ACL, specified by number or name.

ip dscp <dscp-list> and **ipv6 dscp <dscp-list>**: Match the specified DSCP values. The list can contain up to 8 DSCP values, ranging from 0 to 63.

ip precedence <ip-precedence-list>: Matches the specified IP precedence values. The list can contain up to 8 values, ranging from 0 to 7.

ipv6 access-group <acl-index-or-name>: Matches the specified IPv6 ACL, specified by number or name.

ipv6 flowlabel <flowlabel-list>: Matches the specified IPv6 flow label values, ranging from 0 to 1048575.

vlan <vlan-list>: Matches the specified VLAN IDs. The list can contain up to 8 VLAN IDs, ranging from 1 to 4094.

cos <cos-list>: Matches the specified CoS values. The list can contain up to 8 values, ranging from 0 to 7.

Default: No match criterion is configured.

Command Mode: Class Map Mode.

Usage Guidelines: Only one match criterion can be configured in a class map. When an ACL is matched, permit rules select the traffic to which the policy map actions apply, and deny rules exclude traffic from the policy map actions. Configuring a different match criterion after one is configured fails, but configuring the same criterion again overwrites the previous one.

Example: Create class map c1 and configure it to match packets with IP precedence 0.

```
Switch(config)#class-map c1
Switch(config-classmap-c1)#match ip precedence 0
Switch(config-classmap-c1)#exit
```

7.17.3 service-policy

Command: service-policy <policy-map-name> in

no service-policy <policy-map-name> in

Function: Binds the specified flexible QinQ policy map to the ingress direction of the port. The **no** form of this command cancels the binding.

Parameters: <policy-map-name>: The name of the flexible QinQ policy map.

Default: No policy map is bound to the port.

Command Mode: Port Mode.

Usage Guidelines: Only one policy map can be bound to each port; the function takes effect after the policy map is bound to the port.

Example: Apply policy map p1 to port Ethernet 1/0/1 for flexible QinQ.

```
Switch(Config-If-Ethernet1/0/1)#service-policy p1 in
```

7.17.4 set

Command: `set s-vid <new-vid>`
`no set s-vid`

Function: Assigns a new outer VLAN ID to packets that match the class map. The **no** form of this command cancels the operation.

Parameters: s-vid <new-vid>: The VID of the outer VLAN tag.

Default: No value is assigned.

Command Mode: Policy Class Map Mode.

Usage Guidelines: The new value is assigned only to classified traffic that matches the match criterion.

Example: Set the VID of the outer VLAN tag to 3 for packets that match class c2.

```
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c2
Switch(Config-PolicyMap-p1-Class-c2)#set s-vid 3
Switch(Config-PolicyMap-p1-Class-c2)#exit
```

Chapter 8 Commands for Reliability

8.1 MSTP

8.1.1 MSTP

8.1.1.1 abort

Command: `abort`

Function: Discards the current MSTP region configuration, exits MSTP Region Mode, and returns to Global Mode.

Command Mode: MSTP Region Mode.

Usage Guidelines: Exits MSTP Region Mode without saving the current configuration. The previous MSTP region configuration remains in effect.

Example: Exit MSTP Region Mode without saving the current configuration.

```
Switch(Config-Mstp-Region)#abort
Switch(config)#
```

8.1.1.2 exit

Command: `exit`

Function: Saves the current MSTP region configuration, exits MSTP Region Mode, and returns to Global Mode.

Command Mode: MSTP Region Mode.

Usage Guidelines: Exits MSTP Region Mode and saves the current configuration.

Example: Exit MSTP Region Mode and save the current configuration.

```
Switch(Config-Mstp-Region)#exit
Switch(config)#
```

8.1.1.3 instance vlan

Command: `instance <instance-id> vlan <vlan-list>`
`no instance <instance-id> [vlan <vlan-list>]`

Function: Creates an instance and sets the mapping between VLANs and the instance in MSTP Region Mode. The **no instance <instance-id> [vlan <vlan-list>]** command removes the specified instance or the specified VLAN mappings.

Parameters: <instance-id> is the instance number, ranging from 0 to 64. **<vlan-list>** is a list of consecutive or non-consecutive VLAN IDs: "-" indicates a consecutive range, and ";" separates non-consecutive IDs.

Command Mode: MSTP Region Mode.

Default: Before any instances are created, only instance 0 exists, and VLANs 1 to 4094 all belong to instance 0.

Usage Guidelines: This command sets the mapping between VLANs and instances. Switches are in the same MSTP region only if all mappings and other attributes are the same. Before any instances are configured, all VLANs belong to instance 0. MSTP supports up to 64 MSTIs (excluding the CIST). The CIST can be regarded as MSTI 0; the other instances are numbered 1 to 64.

Example: Map VLANs 1-10 and 100-110 to instance 1.

```
Switch(config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#instance 1 vlan 1-10;100-110
```

8.1.1.4 name

Command: `name <name>`
`no name`

Function: Sets the MSTP region name in MSTP Region Mode. The **no name** command restores the default.

Parameters: <name> is the MSTP region name, fewer than 32 characters.

Command Mode: MSTP Region Mode.

Default: The MAC address of the bridge.

Usage Guidelines: Sets the MSTP region name. Bridges with the same MSTP region name and the same other attributes are in the same MSTP region.

Example: Set the MSTP region name to mstp-test.

```
Switch(config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#name mstp-test
```

8.1.1.5 no

Command: `no <instance-id> | <name> | <revision-level>`

Function: Cancels a command or restores its initial value.

Parameters: <instance-id>: The instance number. **<name>**: The MSTP region name. **<revision-level>**: The revision level of the MST configuration.

Command Mode: MSTP Region Mode.

Default: The default revision level is 0.

Usage Guidelines: Deletes the specified instance or the MSTP region name, or restores the revision level to its default of 0.

Example: Delete instance 1.

```
Switch(Config-Mstp-Region)#no instance 1
```

8.1.1.6 revision-level

Command: `revision-level <level>`
`no revision-level`

Function: Sets the revision level of the MSTP configuration in MSTP Region Mode. The **no revision-level** command restores the default of 0.

Parameters: <level> is the revision level, ranging from 0 to 65535.

Command Mode: MSTP Region Mode.

Default: 0.

Usage Guidelines: Sets the revision level of the MSTP configuration. Bridges with the same MSTP revision level and the same other attributes are in the same MSTP region.

Example: Set the revision level to 2000.

```
Switch(config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)# revision-level 2000
```

8.1.1.7 spanning-tree

Command: `spanning-tree`
`no spanning-tree`

Function: Enables MSTP in Global Mode or Port Mode. The **no spanning-tree** command disables MSTP.

Command Mode: Global Mode and Port Mode.

Default: Disabled.

Usage Guidelines: When MSTP is enabled in Global Mode, it is enabled on all ports except those on which MSTP has been explicitly disabled.

Example: Enable MSTP in Global Mode and disable it on interface Ethernet 1/0/2.

```
Switch(config)#spanning-tree
Switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)#no spanning-tree
```

8.1.1.8 spanning-tree cost

Command: `spanning-tree cost <cost>`
`no spanning-tree cost`

Function: Sets the path cost of the current port. The **no spanning-tree cost** command restores the default.

Parameters: <cost> is the path cost, ranging from 1 to 200,000,000.

Command Mode: Port Mode.

Default: The port cost depends on the port bandwidth.

Port Type	Default path cost	Recommended range
10 Mbps	2000000	2000000-20000000
100 Mbps	200000	200000-2000000
1 Gbps	20000	20000-200000
10 Gbps	2000	2000-20000

The default costs of aggregated ports are as follows:

Port Type	Number of aggregated ports	Default port cost
10 Mbps	N	2000000/N
100 Mbps	N	200000/N
1 Gbps	N	20000/N
10 Gbps	N	2000/N

Usage Guidelines: The port cost controls the cost from the current port to the root bridge, and thereby the election of the root port and designated port of the instance.

Example: Set the cost of port Ethernet 1/0/2 to 3000000.

```
Switch(Config-If-Ethernet1/0/2)#spanning-tree cost 3000000
```

8.1.1.9 spanning-tree digest-snooping

Command: `spanning-tree digest-snooping`
`no spanning-tree digest-snooping`

Function: Configures the port to use the configuration digest of the peer port. The **no spanning-tree digest-snooping** command restores the use of the digest generated by the port.

Parameters: None.

Command Mode: Port Mode.

Default: The digest of the peer port is not used.

Usage Guidelines: According to the MSTP standard, the region configuration digest is generated by the MD5 algorithm from a public key, instance IDs, and VLAN IDs. Some vendors do not use the public key, which causes incompatibility. With this command, the port uses the digest of the peer port, providing compatibility with such vendors' equipment.

Note: Because the digest is derived from instance IDs and VLAN IDs, this command may cause devices with different instance-to-VLAN mappings to be treated as being in the same region. Before using this command, make sure that the instance-to-VLAN mapping is the same on all devices. If several devices are connected, run this command on all connected ports.

Example: Configure the port to use the configuration digest of the peer port.

```
Switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)#spanning-tree digest-snooping
Switch(Config-If-Ethernet1/0/2)#
```

8.1.1.10 spanning-tree format

Command: spanning-tree format {standard | privacy | auto}
no spanning-tree format

Function: Configures the BPDU format of the port for interoperability with other vendors' products. The **no** form of this command restores the default format.

Parameters: standard: The BPDU format defined by IEEE.

privacy: A proprietary BPDU format compatible with Cisco equipment.

auto: The format is determined automatically from the received BPDUs.

Command Mode: Port Mode.

Default: auto.

Usage Guidelines: Cisco uses a BPDU format that differs from the IEEE format, and many vendors have adopted the Cisco format for compatibility, so the switch supports both. **standard** is the IEEE format, and **privacy** is the Cisco-compatible format. If the format used by the peer is unknown, **auto** is recommended so that the format is identified from the BPDUs the peer sends. **auto** is the default for better compatibility with earlier and other vendors' products. When **auto** is configured, the privacy format is used until a BPDU is received from the peer.

When the format is not **auto** and the BPDU format received from the peer does not match the configured format, the port that receives the mismatched BPDU is set to the Discarding state. This prevents both sides from considering themselves the root, which would create loops.

When the format is **auto** and more than one incompatible device is connected to the port (for example, a device connected through a hub, or a device that transparently transmits BPDUs connected to several MSTP devices), format changes are counted, and the port is disabled when the count reaches a threshold. The port can then be re-enabled only by the administrator.

Example: Set the BPDU format of the port to the IEEE format.

```
Switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)#spanning-tree format standard
Switch(Config-If-Ethernet1/0/2)#
```

8.1.1.11 spanning-tree forward-time

Command: spanning-tree forward-time <time>
no spanning-tree forward-time

Function: Sets the forward delay of the switch. The **no spanning-tree forward-time** command restores the default.

Parameters: <time> is the forward delay, in seconds, ranging from 4 to 30.

Command Mode: Global Mode.

Default: 15 seconds.

Usage Guidelines: When the network topology changes, a port changes from the blocking state to the forwarding state after a delay called the forward delay. The forward delay works together with the

hello time and max age, and the parameters must meet the following conditions; otherwise, MSTP may not work correctly:

```
2 * (Bridge_Forward_Delay - 1.0 seconds) >= Bridge_Max_Age
Bridge_Max_Age >= 2 * (Bridge_Hello_Time + 1.0 seconds)
```

Example: Set the MSTP forward delay to 20 seconds in Global Mode.

```
Switch(config)#spanning-tree forward-time 20
```

8.1.1.12 spanning-tree hello-time

Command: spanning-tree hello-time <time>
no spanning-tree hello-time

Function: Sets the hello time of the switch. The **no spanning-tree hello-time** command restores the default.

Parameters: <time> is the hello time, in seconds, ranging from 1 to 10.

Command Mode: Global Mode.

Default: 2 seconds.

Usage Guidelines: The hello time is the interval at which the switch sends BPDUs. It works together with the forward delay and max age, and the parameters must meet the following conditions; otherwise, MSTP may not work correctly:

```
2 * (Bridge_Forward_Delay - 1.0 seconds) >= Bridge_Max_Age
Bridge_Max_Age >= 2 * (Bridge_Hello_Time + 1.0 seconds)
```

Example: Set the MSTP hello time to 5 seconds in Global Mode.

```
Switch(config)#spanning-tree hello-time 5
```

8.1.1.13 spanning-tree link-type p2p

Command: spanning-tree link-type p2p {auto | force-true | force-false}
no spanning-tree link-type

Function: Sets the link type of the current port. The **no spanning-tree link-type** command restores automatic detection.

Parameters: auto: Detects the link type automatically. **force-true**: Forces the link to be point-to-point. **force-false**: Forces the link to be non-point-to-point.

Command Mode: Port Mode.

Default: auto; MSTP detects the link type automatically.

Usage Guidelines: In automatic mode, MSTP sets the link type to point-to-point when the port is full duplex and to shared when the port is half duplex.

Example: Force ports Ethernet 1/0/7-8 to the point-to-point link type.

```
Switch(config)#interface ethernet 1/0/7-8
Switch(Config-Port-Range)#spanning-tree link-type p2p force-true
```

8.1.1.14 spanning-tree maxage

Command: spanning-tree maxage <time>
no spanning-tree maxage

Function: Sets the maximum age of BPDUs. The **no spanning-tree maxage** command restores the default.

Parameters: <time> is the maximum age, in seconds, ranging from 6 to 40.

Command Mode: Global Mode.

Default: 20 seconds.

Usage Guidelines: The lifetime of a BPDU is called the max age. The max age works together with the hello time and forward delay, and the parameters must meet the following conditions; otherwise, MSTP may not work correctly:

```
2 * (Bridge_Forward_Delay - 1.0 seconds) >= Bridge_Max_Age
Bridge_Max_Age >= 2 * (Bridge_Hello_Time + 1.0 seconds)
```

Example: Set the max age to 25 seconds in Global Mode.

```
Switch(config)#spanning-tree maxage 25
```

8.1.1.15 spanning-tree max-hop

Command: `spanning-tree max-hop <hop-count>`
`no spanning-tree max-hop`

Function: Sets the maximum number of hops of BPDUs in the MSTP region. The **no spanning-tree max-hop** command restores the default.

Parameters: <hop-count> is the maximum number of hops, ranging from 1 to 40.

Command Mode: Global Mode.

Default: 20.

Usage Guidelines: In addition to the max age, MSTP uses the max hop count to limit the lifetime of BPDUs. The hop count decreases as BPDUs travel through the network: a BPDU originated by the MSTI root bridge carries the maximum value, and each bridge that receives it decrements the value by 1. A port that receives a BPDU with a hop count of 0 discards the BPDU and becomes a designated port that sends BPDUs.

Example: Set the maximum hop count to 32.

```
Switch(config)#spanning-tree max-hop 32
```

8.1.1.16 spanning-tree mcheck

Command: `spanning-tree mcheck`

Function: Forces the port to run in MSTP mode.

Command Mode: Port Mode.

Default: The port runs in MSTP mode.

Usage Guidelines: If the network connected to the current port runs IEEE 802.1D STP, the port switches to STP mode. This command forces the port back to MSTP mode; however, if the port receives STP BPDUs again, it switches back to STP mode.

This command can be used only when the switch runs in IEEE 802.1s MSTP mode; it has no effect when the switch runs in IEEE 802.1D STP mode.

Example: Force port Ethernet 1/0/2 to run in MSTP mode.

```
Switch(Config-If-Ethernet1/0/2)#spanning-tree mcheck
```

8.1.1.17 spanning-tree mode

Command: `spanning-tree mode {mstp | stp | rstp}`
`no spanning-tree mode`

Function: Sets the spanning tree mode of the switch. The **no spanning-tree mode** command restores the default.

Parameters: mstp: IEEE 802.1s MSTP mode. **stp**: IEEE 802.1D STP mode. **rstp**: RSTP mode.

Command Mode: Global Mode.

Default: MSTP mode.

Usage Guidelines: In IEEE 802.1D STP mode, the switch sends only standard IEEE 802.1D BPDUs and TCN BPDUs, and discards MSTP BPDUs.

Example: Set the switch to STP mode.

```
Switch(config)#spanning-tree mode stp
```

8.1.1.18 spanning-tree mst configuration

Command: `spanning-tree mst configuration`
`no spanning-tree mst configuration`

Function: Enters MSTP Region Mode, where MSTP region attributes can be configured. The **no spanning-tree mst configuration** command restores the MSTP region attributes to their defaults.

Command Mode: Global Mode.

Default: The default MSTP region attributes are as follows:

MSTP attribute	Default value
Instance	Only instance 0 exists. All VLANs (1 to 4094) are mapped to instance 0.
Name	MAC address of the bridge
Revision	0

Usage Guidelines: Whether or not the switch is running MSTP, you can enter MSTP Region Mode, configure the attributes, and save the configuration. When the switch runs MSTP, it generates the MST configuration identifier from the MSTP configuration. Only switches with the same MST configuration identifier are in the same MSTP region.

Example: Enter MSTP Region Mode.

```
Switch(config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#
```

8.1.1.19 spanning-tree mst cost

Command: `spanning-tree mst <instance-id> cost <cost>`
`no spanning-tree mst <instance-id> cost`

Function: Sets the path cost of the current port in the specified instance. The **no spanning-tree mst <instance-id> cost** command restores the default.

Parameters: <instance-id> is the instance ID, ranging from 0 to 64. **<cost>** is the path cost; the range depends on the cost format: 1 to 200,000,000 for the default dot1t format and 1 to 65535 for the dot1d format.

Command Mode: Port Mode.

Default: The port cost depends on the port bandwidth.

Port Type	Default path cost	Recommended range
10 Mbps	2000000	2000000-20000000
100 Mbps	200000	200000-2000000
1 Gbps	20000	20000-200000
10 Gbps	2000	2000-20000

The default costs of aggregated ports are as follows:

Port Type	Number of aggregated ports	Default port cost
10 Mbps	N	2000000/N
100 Mbps	N	200000/N
1 Gbps	N	20000/N
10 Gbps	N	2000/N

Port speed	Port type	Port cost	
		802.1D-2008	802.1T

0		65535	200,000,000
10Mbps	Half duplex Full duplex Aggregated link with 2 ports Aggregated link with 3 ports Aggregated link with 4 ports	100 99 95 95 95	2,000,000 1,999,999 1,000,000 666,666 500,000
100Mbps	Half duplex Full duplex Aggregated link with 2 ports Aggregated link with 3 ports Aggregated link with 4 ports	19 18 15 15 15	200,000 199,999 100,000 66,666 50,000
1000Mbps	Full duplex Aggregated link with 2 ports Aggregated link with 3 ports Aggregated link with 4 ports	4 3 3 3	20,000 10,000 6,666 5,000
10Gbps	Full duplex Aggregated link with 2 ports Aggregated link with 3 ports Aggregated link with 4 ports	2 1 1 1	2,000 1,000 666 500

Usage Guidelines: The port cost controls the cost from the current port to the root bridge, and thereby the election of the root port and designated port of the instance.

Example: Set the MSTP cost of port Ethernet 1/0/2 in instance 2 to 3000000.

```
Switch(Config-If-Ethernet1/0/2)#spanning-tree mst 2 cost 3000000
```

8.1.1.20 spanning-tree cost-format

Command: `spanning-tree cost-format {dot1d | dot1t}`

Function: Selects the path cost format, dot1d or dot1t, in Global Mode. The default format is dot1t.

Command Mode: Global Mode.

Default: dot1t.

Usage Guidelines: There are two path cost formats: dot1d, defined in IEEE 802.1D-2008, and dot1t, defined in IEEE 802.1t. Their ranges differ: dot1d ranges from 1 to 65535, and dot1t from 1 to 200,000,000.

If a link cost has already been configured manually with **spanning-tree cost**, the path cost format can be changed with **spanning-tree cost-format** only after that configuration is cleared.

Example: Set the cost format in Global Mode.

```
Switch(config)#spanning-tree cost-format dot1d
```

8.1.1.21 spanning-tree mst loopguard

Command: spanning-tree [mst <instance-id>] loopguard
no spanning-tree [mst <instance-id>] loopguard

Function: Enables loop guard for the specified instance. The **no** form of this command disables it.

Parameters: <instance-id>: The MSTP instance ID.

Command Mode: Port Mode.

Default: Disabled.

Usage Guidelines: Loop guard prevents a root port or alternate port from becoming a designated port because of a unidirectional link failure. When the BPDU receive timer expires, a port configured with loop guard is set to the blocking state.

Example: Enable loop guard on port Ethernet 1/0/2 for instance 0.

```
Switch(Config)#interface ethernet 1/0/2
Switch(Config-Ethernet-1/0/2)#spanning-tree mst 0 loopguard
Switch(Config-Ethernet-1/0/2)#
```

8.1.1.22 spanning-tree mst port-priority

Command: spanning-tree mst <instance-id> port-priority <port-priority>
no spanning-tree mst <instance-id> port-priority

Function: Sets the port priority for the specified instance. The **no spanning-tree mst <instance-id> port-priority** command restores the default.

Parameters: <instance-id> is the instance ID, ranging from 0 to 64. **<port-priority>** is the port priority, ranging from 0 to 240 in multiples of 16 (0, 16, 32, ... 240).

Command Mode: Port Mode.

Default: 128.

Usage Guidelines: The port priority determines the port ID in the instance and thereby the root port and designated port of the instance. The lower the value, the higher the priority.

Example: Set the priority of port Ethernet 1/0/2 to 32 for instance 1.

```
Switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)#spanning-tree mst 1 port-priority 32
```

8.1.1.23 spanning-tree mst priority

Command: spanning-tree mst <instance-id> priority <bridge-priority>
no spanning-tree mst <instance-id> priority

Function: Sets the bridge priority for the specified instance. The **no spanning-tree mst <instance-id> priority** command restores the default.

Parameters: <instance-id> is the instance ID, ranging from 0 to 64. **<bridge-priority>** is the bridge priority, ranging from 0 to 61440 in multiples of 4096 (0, 4096, 8192, ... 61440).

Command Mode: Global Mode.

Default: 32768.

Usage Guidelines: The bridge priority changes the bridge ID for the specified instance, which affects the election of the root bridge and designated ports of the instance.

Example: Set the priority for instance 2 to 4096.

```
Switch(config)#spanning-tree mst 2 priority 4096
```

8.1.1.24 spanning-tree mst rootguard

Command: spanning-tree [mst <instance-id>] rootguard
no spanning-tree [mst <instance-id>] rootguard

Function: Enables root guard for the specified instance; root guard prevents the port from becoming an MSTP root port. The **no spanning-tree mst <instance-id> rootguard** command disables root guard.

Parameters: <instance-id>: The MSTP instance ID.

Command Mode: Port Mode.

Default: Disabled.

Usage Guidelines: A port configured with root guard cannot become an MSTP root port. If a superior BPDU is received on a root guard port, MSTP does not recalculate the spanning tree but sets the port to the root-inconsistent (blocked) state. If no superior BPDU is received on a blocked root guard port, the port returns to the forwarding state. Root guard keeps the spanning tree topology relatively stable when a new switch is added to the network.

Example: Enable root guard on port Ethernet 1/0/2 in instance 0.

```
Switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)#spanning-tree mst 0 rootguard
Switch(Config-If-Ethernet1/0/2)#
```

8.1.1.25 spanning-tree portfast

Command: spanning-tree portfast [bpdufilter | bpduguard] [recovery <30-3600>]
no spanning-tree portfast

Function: Configures the current port as an edge port and sets its BPDU filter or BPDU guard mode. The **no spanning-tree portfast** command configures the port as a non-edge port.

Parameters: bpdufilter: Sets the edge port to BPDU filter mode.

bpduguard: Sets the edge port to BPDU guard mode.

recovery: Allows the edge port to recover automatically after a BPDU guard violation.

<30-3600>: The recovery time in seconds. By default, the port does not recover automatically.

Command Mode: Port Mode.

Default: When MSTP is enabled, all ports are non-edge ports.

Usage Guidelines: An edge port moves from the discarding state to the forwarding state without the forward delay. When an edge port receives a BPDU, it becomes a non-edge port.

Example: Set the edge port to BPDU guard mode with a recovery time of 60 seconds.

```
Switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)#spanning-tree portfast bpduguard recovery 60
Switch(Config-If-Ethernet1/0/2)#
```

8.1.1.26 spanning-tree port-priority

Command: spanning-tree port-priority <port-priority>
no spanning-tree port-priority

Function: Sets the port priority. The **no spanning-tree port-priority** command restores the default.

Parameters: <port-priority> is the port priority, ranging from 0 to 240 in multiples of 16 (0, 16, 32, 48, ... 240).

Command Mode: Port Mode.

Default: 128.

Usage Guidelines: The port priority affects the selection of the designated port. The lower the value, the higher the priority.

Example: Set the priority of port Ethernet 1/0/1 to 4096.

```
Switch(Config-If-Ethernet1/0/1)#spanning-tree port-priority 4096
```

8.1.1.27 spanning-tree priority

Command: `spanning-tree priority <bridge-priority>`
`no spanning-tree priority`

Function: Configures the spanning tree bridge priority. The **no spanning-tree priority** command restores the default.

Parameters: <bridge-priority> is the bridge priority of the switch, a multiple of 4096 from 0 to 61440 (0, 4096, 8192, ... 61440).

Command Mode: Global Mode.

Default: 32768.

Usage Guidelines: Changing the priority changes the bridge ID of the switch. The priority is also used to elect the root bridge and designated ports. The smaller the value, the higher the priority.

Example: Set the priority to 4096.

```
Switch(config)#spanning-tree priority 4096
```

8.1.1.28 spanning-tree rootguard

Command: `spanning-tree rootguard`
`no spanning-tree rootguard`

Function: Enables root guard on the port; the port cannot become a root port. The **no spanning-tree rootguard** command disables root guard.

Parameters: None.

Command Mode: Port Mode.

Default: Disabled.

Usage Guidelines: A port configured with root guard cannot become an MSTP root port. If a superior BPDU is received on a root guard port, MSTP does not recalculate the spanning tree but sets the port to the root-inconsistent (blocked) state. If no superior BPDU is received on a blocked root guard port, the port returns to the forwarding state. Root guard keeps the spanning tree topology relatively stable when a new switch is added to the network.

Example: Enable root guard on port Ethernet 1/0/1.

```
Switch(Config-If-Ethernet1/0/1)#spanning-tree rootguard
```

8.1.1.29 spanning-tree tcflush (Global mode)

Command: `spanning-tree tcflush {enable| disable| protect}`
`no spanning-tree tcflush`

Function: Configures the MAC flush behavior when the spanning tree topology changes. The **no spanning-tree tcflush** command restores the default.

Parameters: enable: Flushes each time the topology changes.

disable: Does not flush when the topology changes.

protect: Flushes at most once every 10 seconds.

Command Mode: Global Mode.

Default: Enabled.

Usage Guidelines: According to MSTP, when the topology changes, the port that sends the topology change message clears the MAC/ARP table (flush). In some networks, flushing at every topology change is unnecessary. In addition, to protect against network attacks, the administrator can configure the flush mode with this command.

Note: The **disable** mode is not recommended for complex networks, especially those that require fast switchover between spanning tree branches.

Example: Disable flushing on topology change.

```
Switch(config)#spanning-tree tcflush disable
Switch(config)#
```

8.1.1.30 spanning-tree tcflush (Port mode)

Command: spanning-tree tcflush {enable| disable| protect}
no spanning-tree tcflush

Function: Configures the MAC flush behavior of the port when the spanning tree topology changes. The **no spanning-tree tcflush** command restores the default.

Parameters: enable: Flushes each time the topology changes.

disable: Does not flush when the topology changes.

protect: Flushes at most once every 10 seconds.

Command Mode: Port Mode.

Default: The global configuration is used.

Usage Guidelines: According to MSTP, when the topology changes, the port that sends the topology change message clears the MAC/ARP table (flush). In some networks, flushing at every topology change is unnecessary. In addition, to protect against network attacks, the administrator can configure the flush mode with this command.

Note: The **disable** mode is not recommended for complex networks, especially those that require fast switchover between spanning tree branches.

Example: Disable flushing on topology change on port Ethernet 1/0/2.

```
Switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)#spanning-tree tcflush disable
Switch(Config-If-Ethernet1/0/2)#
```

8.1.1.31 spanning-tree transmit-hold-count

Command: spanning-tree transmit-hold-count <tx-hold-count-value>
no spanning-tree transmit-hold-count

Function: Sets the maximum transmit hold count of ports.

Parameters: <tx-hold-count-value>: Ranging from 1 to 255. The default is 10.

Command Mode: Global Mode.

Default: 10.

Usage Guidelines: Sets the maximum number of BPDUs sent within one hello time interval, to control BPDU traffic. The value applies to the whole MST bridge.

Example: Set the maximum transmit hold count to 20.

```
Switch(config)#spanning-tree transmit-hold-count 20
```

8.1.2 Monitor and Debug

8.1.2.1 debug spanning-tree

Command: debug spanning-tree
no debug spanning-tree

Function: Enables MSTP debugging. The **no debug spanning-tree** command disables MSTP debugging.

Command Mode: Admin Mode.

Usage Guidelines: This command is the master switch for all MSTP debugging. Enable the specific debugging items first; this command then displays the corresponding debugging information. This command is generally used by experienced technicians.

Example: Enable debugging of BPDUs received on port Ethernet 1/0/1.

```
Switch#debug spanning-tree
Switch#debug spanning-tree bpdu rx interface e1/0/1
```

8.1.2.2 show mst-pending

Command: show mst-pending

Function: Displays the pending configuration of the current MSTP region in MSTP Region Mode.

Command Mode: Admin Mode.

Usage Guidelines: In MSTP Region Mode, displays the pending configuration of the current MSTP region, such as the region name, revision level, and VLAN-to-instance mapping.

Note: Before you exit MSTP Region Mode, the displayed parameters may not yet be in effect.

Example: Display the pending configuration of the current MSTP region.

```
Switch(config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#show mst-pending
Name       test
Revision     0
Instance     Vlans Mapped
---------------------------------
00           1-29, 31-39, 41-4093
03           30
04           40
05           4094
---------------------------------
Switch(Config-Mstp-Region)#
```

8.1.2.3 show spanning-tree

Command: show spanning-tree [mst [<instance-id>]] [interface <interface-list>] [detail]

Function: Displays MSTP information.

Parameters: <interface-list> is the interface list. **<instance-id>** is the instance ID, ranging from 0 to 64. **detail** displays detailed spanning tree information.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the MSTP information of the instances on the current bridge.

Example: Display the MSTP information of the bridge.

```
Switch#sh spanning-tree
                -- MSTP Bridge Config Info --
Standard     :  IEEE 802.1s
Bridge MAC   :  00: 03: 0f: 01: 0e: 30
Bridge Times :  Max Age 20, Hello Time 2, Forward Delay 15
```

```
Force Version:  3
############################ Instance 0 ############################
Self Bridge Id   : 32768 -  00: 03: 0f: 01: 0e: 30
Root Id          : 16384.00: 03: 0f: 01: 0f: 52
Ext.RootPathCost : 200000
Region Root Id   : this switch
Int.RootPathCost : 0
Root Port ID     : 128.1
Current port list in Instance 0:
Ethernet1/0/1 Ethernet1/0/2 (Total 2)
 PortName      ID      ExtRPC   IntRPC  State Role     DsgBridge     DsgPort
-------------- ------- --------- --------- --- ---- ------------------
-------
 Ethernet1/0/1  128.001         0       0 FWD ROOT 16384.00030f010f52 128.007
 Ethernet1/0/2  128.002         0        0 BLK ALTR 16384.00030f010f52
128.011
############################ Instance 3 ############################
Self Bridge Id   : 0.00: 03: 0f: 01: 0e: 30
Region Root Id   : this switch
Int.RootPathCost : 0
Root Port ID     : 0
Current port list in Instance 3:
Ethernet1/0/1 Ethernet1/0/2 (Total 2)
PortName      ID    IntRPC   State Role     DsgBridge     DsgPort
-------------- ------- --------- --- ---- ------------------ -------
 Ethernet1/0/1  128.001         0 FWD MSTR     0.00030f010e30 128.001
 Ethernet1/0/2  128.002         0 BLK ALTR     0.00030f010e30 128.002
############################ Instance 4 ############################
Self Bridge Id   : 32768.00: 03: 0f: 01: 0e: 30
Region Root Id   : this switch
Int.RootPathCost : 0
Root Port ID     : 0
Current port list in Instance 4:
Ethernet1/0/1 Ethernet1/0/2 (Total 2)
PortName      ID    IntRPC   State Role     DsgBridge     DsgPort
-------------- ------- --------- --- ---- ------------------ -------
 Ethernet1/0/1 128.001         0 FWD MSTR 32768.00030f010e30 128.001
 Ethernet1/0/2 128.002         0 BLK ALTR 32768.00030f010e30 128.002
```

Output	Description
Bridge information	
Standard	STP version (standard)
Bridge MAC	MAC address of the bridge
Bridge Times	Max age, hello time, and forward delay of the bridge
Force Version	Forced STP version
Instance information	
Self Bridge Id	Priority and MAC address of the current bridge in the current instance
Root Id	Priority and MAC address of the root bridge in the current instance
Ext.RootPathCost	Total cost from the current bridge to the root of the entire network
Int.RootPathCost	Cost from the current bridge to the regional root of the current instance
Root Port ID	Root port of the current instance on the current bridge
MSTP port list of the current instance	
PortName	Port name
ID	Port priority and port index

ExtRPC	Port cost to the root of the entire network
IntRPC	Cost from the current port to the regional root of the current instance
State	Port state in the current instance
Role	Port role in the current instance
DsgBridge	Upstream designated bridge of the current port in the current instance
DsgPort	Upstream designated port of the current port in the current instance

8.1.2.4 show spanning-tree mst config

Command: `show spanning-tree mst config`

Function: Displays the MSTP configuration in Admin Mode.

Command Mode: Admin Mode.

Usage Guidelines: In Admin Mode, displays the MSTP configuration parameters, such as the region name, revision level, and VLAN-to-instance mapping.

Example: Display the MSTP configuration of the switch.

```
Switch#show spanning-tree mst config
Name         test
Revision     0
Instance     Vlans Mapped
---------------------------------
00          1-29, 31-39, 41-4094
03           30
04          40
---------------------------------
```

8.1.3 MSTP Spanning-tree Process

8.1.3.1 spanning-tree process

Command: `spanning-tree process <process-id>`
`no spanning-tree process <process-id>`

Function: Creates an MSTP process.

Parameters: <process-id>: The process ID, ranging from 1 to 31.

Command Mode: Global Mode.

Default: None.

Usage Guidelines: Creates an MSTP process. Multiple MSTP processes can be configured on a device, and each process is independent. Process 0 exists by default.

Example: Create MSTP process 1.

```
Switch(config)#spanning-tree process 1
```

8.1.3.2 spanning-tree tc-notify process0

Command: `spanning-tree tc-notify process0`
`no spanning-tree tc-notify process0`

Function: Configures MSTP process N to notify the instances in MSTP process 0 of topology changes (TC).

Parameters: None.

Command Mode: MSTP Process Mode.

Default: None.

Usage Guidelines: When the topology of MSTP process N changes, the device receives TC packets, and process N notifies the instances in MSTP process 0 on the shared link. Process 0 then refreshes its entries so that traffic is not interrupted.

Example: Configure process 1 to notify process 0 of topology changes.

```
Switch(Config-Mstp-Process-1)#spanning-tree tc-notify process0
```

8.2 VRRP

8.2.1 advertisement-interval

Command: advertisement-interval <adver_interval>
no advertisement-interval

Function: Sets the VRRP advertisement interval. The **no advertisement-interval** command restores the default.

Parameters: <adver_interval> is the interval at which VRRP packets are sent, in seconds, ranging from 1 to 10.

Default: 1 second.

Command Mode: VRRP Mode.

Usage Guidelines: The master in a VRRP standby group sends VRRP packets to member routers (or Layer 3 switches) at a specific interval, the advertisement interval, to announce that it is working properly. If a backup does not receive VRRP packets from the master within a certain period (the master down interval), it assumes that the master has failed and becomes the master.

Use this command to adjust the interval at which the master sends VRRP packets. All members of the same standby group must use the same value. For a backup, the master down interval is three times the advertisement interval. Very heavy traffic or different timer settings between routers (or Layer 3 switches) may cause the master down interval to expire and trigger frequent state changes. This can be avoided by increasing the advertisement interval and setting a longer preemption delay.

Example: Set the VRRP advertisement interval to 3 seconds.

```
Switch(Config-Router-Vrrp)# advertisement-interval 3
```

8.2.2 circuit-failover

Command: circuit-failover {IFNAME | Vlan <ID>} <value_reduced>
no circuit-failover

Function: Configures the VRRP monitored interface.

Parameters: IFNAME | Vlan <ID> is the interface to be monitored.

<value_reduced> is the amount by which the priority is decreased, ranging from 1 to 253.

Default: Not configured by default.

Command Mode: VRRP Mode.

Usage Guidelines: Interface monitoring extends the backup function: VRRP not only provides failover when a router (or Layer 3 switch) fails, but also lowers the priority of a router (or Layer 3 switch) when a monitored interface goes down, so that backup works smoothly.

With this command, when a monitored interface goes from up to down, the priority of the router (or Layer 3 switch) in its standby group decreases, so that a backup with a higher priority can take over as master.

Example: Monitor interface VLAN 2 and decrease the priority by 10 when it goes down.

```
Switch(Config-Router-Vrrp)# circuit-failover vlan 2 10
```

8.2.3 debug vrrp

Command: debug vrrp [all | event | packet [recv | send]]
no debug vrrp [all | event | packet [recv | send]]

Function: Displays debugging information about VRRP standby group status and packet transmission. The **no debug vrrp** command disables the debugging.

Default: Disabled.

Command Mode: Admin Mode.

Example:

```
Switch#debug vrrp
2001/01/01 00:50:28 : IMI: VRRP SEND[Hello]: Advertisement sent for vrid=[1],
virtual-ip=[10.1.1.1]
2001/01/01 00:50:30 : IMI: VRRP SEND[Hello]: Advertisement sent for vrid=[1],
virtual-ip=[10.1.1.1]
2001/01/01 00:50:31 : IMI: VRRP SEND[Hello]: Advertisement sent for vrid=[1],
virtual-ip=[10.1.1.1]
2001/01/01 00:50:32 : IMI: VRRP SEND[Hello]: Advertisement sent for vrid=[1],
virtual-ip=[10.1.1.1]
2001/01/01 00:50:33 : IMI: VRRP SEND[Hello]: Advertisement sent for vrid=[1],
virtual-ip=[10.1.1.1]
```

8.2.4 disable

Command: disable

Function: Deactivates VRRP.

Parameters: None.

Default: Not configured.

Command Mode: VRRP Mode.

Usage Guidelines: Deactivates a virtual router. The VRRP configuration can be modified only when VRRP is deactivated.

Example: Deactivate virtual router 10.

```
Switch(config)# router vrrp 10
Switch(Config-Router-Vrrp)#disable
```

8.2.5 enable

Command: enable

Function: Activates VRRP.

Parameters: None.

Default: Not configured.

Command Mode: VRRP Mode.

Usage Guidelines: Activates the virtual router. Only a router (or Layer 3 switch) interface activated with this command is part of the standby group. The VRRP virtual IP address and interface must be configured before the virtual router is activated.

Example: Activate virtual router 10.

```
Switch(config)#router vrrp 10
Switch(Config-Router)#enable
```

8.2.6 interface

Command: `interface {IFNAME | Vlan <ID>}`
`no interface`

Function: Configures the VRRP interface.

Parameters: IFNAME: The interface name, for example, Vlan1.

Vlan <ID>: The VLAN ID.

Default: Not configured.

Command Mode: VRRP Mode.

Usage Guidelines: Adds a Layer 3 interface to an existing standby group. The **no interface** command removes the Layer 3 interface from the standby group.

Example: Configure interface VLAN 1 as the VRRP interface.

```
Switch(config-router)#router vrrp 10
Switch(Config-router)#interface vlan 1
```

8.2.7 preempt-mode

Command: `preempt-mode {true | false}`

Function: Configures the VRRP preemption mode.

Parameters: true: Preemption mode. **false**: Non-preemption mode.

Command Mode: VRRP Mode.

Default: Preemption mode.

Usage Guidelines: If a router (or Layer 3 switch) with a high priority must preemptively become the master, enable preemption mode.

Example: Set non-preemption mode.

```
Switch(Config-Router-Vrrp)#preempt-mode false
```

8.2.8 priority

Command: `priority <value>`

Function: Configures the VRRP priority.

Parameters: <value> is the priority, ranging from 1 to 254.

Default: 100 for all backup routers (or Layer 3 switches) in a standby group.

Command Mode: VRRP Mode.

Usage Guidelines: The priority determines the ranking of a router (or Layer 3 switch) in a standby group; the higher the priority, the more likely the router is to become the master. A router (or Layer 3 switch) that owns the virtual IP address always has priority 254, which cannot be changed. If two or more routers (or Layer 3 switches) in a standby group have the same priority, the one with the highest VLAN interface IP address becomes the master.

Example: Set the VRRP priority to 150.

```
Switch(Config-Router-Vrrp)# priority 150
```

8.2.9 router vrrp

Command: `router vrrp <vrid>`
`no router vrrp <vrid>`

Function: Creates or removes a virtual router.

Parameters: <vrid> is the virtual router number, ranging from 1 to 255.

Default: Not configured.

Command Mode: Global Mode.

Usage Guidelines: Creates or removes a virtual router, identified by a unique virtual router number. Virtual router configuration is available only after the virtual router is created. Up to 192 virtual routers can be configured.

Example: Configure virtual router 10.

```
Switch(config)# router vrrp 10
```

8.2.10 show vrrp

Command: show vrrp [<vrid>]

Function: Displays the status and configuration of VRRP standby groups.

Parameters: <vrid> is the virtual router number, ranging from 1 to 255.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the configuration and current state of virtual routers. If no virtual router number is specified, all virtual routers are displayed.

Example:

```
Switch# show vrrp
VrId <1>
State is Initialize
Virtual IP is 10.1.20.10 (Not IP owner)
Interface is Vlan1
Priority not configured, Current priority is 254
Advertisement interval is 1 sec
Preempt mode is TRUE
Circuit failover interface Vlan1, Priority Delta 1, Status UP
VrId <10>
State is Initialize
Virtual IP is1.1.1.1 (Not IP owner)
Interface is unset
Priority is unset
Advertisement interval is unset
Preempt mode is TRUE
Switch#
```

Output	Description
State	State
Virtual IP	Virtual IP address
Interface	Interface name
Priority	Priority
Advertisement interval	Advertisement interval
Preempt	Preemption mode
Circuit failover interface	Interface monitoring information

8.2.11 virtual-ip

Command: virtual-ip <A.B.C.D>
no virtual-ip

Function: Configures the VRRP virtual IP address.

Parameters: <A.B.C.D> is the IP address in dotted decimal notation.

Default: Not configured.

Command Mode: VRRP Mode.

Usage Guidelines: Adds a virtual IP address to an existing standby group. The **no virtual-ip** command removes the virtual IP address from the standby group. Each standby group can have only one virtual IP address. When the VRRP priority is not 255 (the router is not the IP address owner), the virtual IP address and the interface IP address must be on the same network segment.

Example: Set the virtual IP address of the standby group to 10.1.1.1.

```
Switch(Config-Router-Vrrp)# virtual-ip 10.1.1.1
```

8.2.12 vrrp track

Command: vrrp track interface {ethernet IFNAME|IFNAME} priority <priority_value>
no vrrp track interface {ethernet IFNAME|IFNAME}

Function: Configures a monitored port for the VRRP session.

Parameters: interface {ethernet IFNAME | IFNAME}: The port name.

<priority_value>: The priority, ranging from 1 to 254.

Command Mode: VRRP Mode.

Default: Disabled.

Usage Guidelines: Configures a port whose status is monitored by the VRRP session. When the port goes down, the local VRRP priority changes to the configured value, which can change the VRRP session state. For example, if the local VRRP priority becomes lower than that of the peer, the local VRRP state changes to Backup.

Example:

```
Switch(config)#router vrrp 1
Switch(config-router)#vrrp track interface ethernet 1/0/5 priority 60
```

8.3 MRPP

8.3.1 control-vlan

Command: control-vlan <vid>
no control-vlan

Function: Configures the control VLAN ID of the MRPP ring. The **no control-vlan** command deletes the control VLAN ID.

Parameters: <vid> is the control VLAN ID, ranging from 1 to 4094.

Command Mode: MRPP Ring Mode.

Default: None.

Usage Guidelines: Specifies the control VLAN ID of the MRPP ring, which can currently be any value from 1 to 4094. To avoid confusion, use a VLAN ID that is not otherwise configured and is the same as the MRPP ring ID. All switches on the same MRPP ring must use the same control VLAN ID; otherwise, the MRPP ring may not work properly or may form a broadcast loop.

mrpp enable must be configured before this command. The MRPP ring takes effect after the primary port, secondary port, node mode, and **enable** commands are configured after **control-vlan**.

Example: Set the control VLAN of MRPP ring 4000 to 4000.

```
Switch(config)#mrpp ring 4000
Switch(mrpp-ring-4000)#control-vlan 4000
```

8.3.2 clear mrpp statistics

Command: `clear mrpp statistics [<ring-id>]`

Function: Clears the statistics of MRPP packets received and sent on MRPP rings.

Parameters: <ring-id> is the MRPP ring ID, ranging from 1 to 4096. If no ID is specified, the statistics of all MRPP rings are cleared.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: None.

Example: Clear the statistics of MRPP ring 4000.

```
Switch#clear mrpp statistics 4000
```

8.3.3 debug mrpp

Command: `debug mrpp`
`no debug mrpp`

Function: Enables MRPP debugging. The **no debug mrpp** command disables it.

Command Mode: Admin Mode.

Parameters: None.

Usage Guidelines: MRPP debugging shows MRPP protocol message processing and packet reception, which is useful for monitoring and troubleshooting.

Example: Enable MRPP debugging.

```
Switch#debug mrpp
```

8.3.4 enable

Command: `enable`
`no enable`

Function: Enables the configured MRPP ring. The **no enable** command disables the MRPP ring.

Parameters: None.

Command Mode: MRPP Ring Mode.

Default: Disabled.

Usage Guidelines: MRPP must be enabled globally before this command is executed. The MRPP ring takes effect when the other required commands are also configured.

Example: Configure the switch as the master node of MRPP ring 4000 and enable the ring.

```
Switch(config)#mrpp enable
Switch(config)#mrpp ring 4000
Switch(mrpp-ring-4000)#control-vlan 4000
Switch(mrpp-ring-4000)# node-mode master
Switch(mrpp-ring-4000)#fail-timer 18
Switch(mrpp-ring-4000)#hello-timer 6
Switch(mrpp-ring-4000)#enable
Switch(mrpp-ring-4000)#exit
Switch(config)#in ethernet1/0/1
Switch(config-If-Ethernet1/0/1)#mrpp ring 4000 primary-port
Switch(config)#in ethernet 1/0/3
Switch(config-If-Ethernet1/0/3)#mrpp ring 4000 secondary-port
```

8.3.5 errp domain

Command: `errp domain <domain-id>`
`no errp domain <domain-id>`

Function: Creates an ERRP domain. The **no** form of this command deletes the ERRP domain.

Parameters: <domain-id>: The ERRP domain ID, ranging from 0 to 15.

Command Mode: Global Mode.

Usage Guidelines: To configure an ERRP domain ID, enable ERRP compatible mode first. This command creates an ERRP domain if none exists; the **no** form deletes the domain with the specified ID.

Example: Configure an ERRP domain ID globally.

```
Switch(Config)#errp domain 1
```

8.3.6 fail-timer

Command: `fail-timer <timer>`
`no fail-timer`

Function: Configures the fail timer within which the master node of the MRPP ring must receive Hello packets. The **no fail-timer** command restores the default.

Parameters: <timer> ranges from 3 to 300 seconds.

Command Mode: MRPP Ring Mode.

Default: 3 seconds.

Usage Guidelines: If the master node of the MRPP ring does not receive, within the fail timer, the Hello packets sent from its primary port, the ring is considered failed. Transit nodes do not need this timer. To allow for the delay of Hello packets forwarded by transit nodes, the fail timer must be at least three times the Hello timer. On rings with long delays, increase the default value so that the master node does not miss Hello packets within the fail timer because of the delay.

Example: Set the fail timer of MRPP ring 4000 to 10 seconds.

```
Switch(config)# mrpp ring 4000
Switch(mrpp-ring-4000)#fail-timer 10
```

8.3.7 hello-timer

Command: `hello-timer <timer>`
`no hello-timer`

Function: Configures the interval at which the master node of the MRPP ring sends Hello packets. The **no hello-timer** command restores the default.

Parameters: <timer> ranges from 1 to 100 seconds.

Command Mode: MRPP Ring Mode.

Default: 1 second.

Usage Guidelines: The master node of the MRPP ring sends Hello packets at the configured interval. If the secondary port of the master node receives the packets within the configured period, the ring is normal; otherwise, it has failed. Transit nodes do not need this timer.

Example: Set the Hello timer of MRPP ring 4000 to 3 seconds.

```
Switch(config)# mrpp ring 4000
Switch(mrpp-ring-4000)#hello-timer 3
```

8.3.8 mrpp eaps compatible

Command: **`mrpp eaps compatible`**
`no mrpp eaps compatible`

Function: Enables EAPS compatible mode. The **no** form of this command disables it.

Parameters: None.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: MRPP must be enabled before EAPS compatible mode is configured. When executing **no mrpp eaps compatible**, make sure that MRPP is enabled on the switch.

Example: Enable EAPS compatible mode globally.

```
Switch(Config)#mrpp enable
Switch(Config)#mrpp eaps compatible
```

8.3.9 mrpp enable

Command: **`mrpp enable`**
`no mrpp enable`

Function: Enables the MRPP protocol module. The **no mrpp enable** command disables MRPP.

Parameters: None.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: MRPP must be enabled before MRPP rings are configured. Before executing **no mrpp enable**, make sure that the MRPP rings enabled on the switch are disabled.

Example: Enable MRPP globally.

```
Switch(config)#mrpp enable
```

8.3.10 mrpp errp compatible

Command: **`mrpp errp compatible`**
`no mrpp errp compatible`

Function: Enables ERRP compatible mode. The **no** form of this command disables it.

Parameters: None.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: MRPP must be enabled before ERRP compatible mode is configured. In addition, ports in ERRP compatible mode must be in Hybrid or Trunk mode and must allow packets of the control VLAN.

Example: Enable ERRP compatible mode globally.

```
Switch(Config)#mrpp enable
Switch(Config)#mrpp errp compatible
Switch(Config)#mrpp ring 2
Switch(mrpp-ring-2)#control-vlan 4000
Switch(config-if-ethernet1/0/51)#switchport mode hybrid
Switch(config-if-ethernet1/0/51)#switchport hybrid allowed vlan 4000 tag
Switch(config-if-ethernet1/0/52)#switchport mode hybrid
Switch(config-if-ethernet1/0/52)#switchport hybrid allowed vlan 4000 tag
```

8.3.11 mrpp poll-time

Command: `mrpp poll-time <20-2000>`

Function: Configures the MRPP polling interval.

Command Mode: Global Mode.

Usage Guidelines: Adjusts the MRPP polling interval, in milliseconds. The default is 100 ms.

Example: Set the polling interval to 200 ms.

```
Switch(Config)# mrpp poll-time 200
```

8.3.12 mrpp ring

Command: `mrpp ring <ring-id>`
`no mrpp ring <ring-id>`

Function: Creates an MRPP ring and enters MRPP Ring Mode. The **no mrpp ring <ring-id>** command deletes the MRPP ring.

Parameters: <ring-id> is the MRPP ring ID, ranging from 1 to 4096.

Command Mode: Global Mode.

Usage Guidelines: If the MRPP ring does not exist, this command creates it and enters MRPP Ring Mode. Disable the MRPP ring before executing **no mrpp ring**.

Example:

```
Switch(config)#mrpp ring 100
```

8.3.13 mrpp ring primary-port

Command: `mrpp ring <ring-id> primary-port`
`no mrpp ring <ring-id> primary-port`

Function: Specifies the primary port of the MRPP ring.

Parameters: <ring-id> is the MRPP ring ID, ranging from 1 to 4096.

Command Mode: Port Mode.

Default: None.

Usage Guidelines: Specifies the primary port of the MRPP ring. The master node sends Hello packets from the primary port and receives them on the secondary port. On a transit node, the primary and secondary ports have the same function.

mrpp enable must be configured before **control-vlan**. The MRPP ring takes effect after the primary port, secondary port, node mode, and **enable** commands are configured after **control-vlan**.

Example: Set the primary port of MRPP ring 4000 to Ethernet 1/0/1.

```
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)#mrpp ring 4000 primary-port
```

8.3.14 mrpp ring secondary-port

Command: `mrpp ring < ring-id > secondary-port`
`no mrpp ring < ring-id > secondary-port`

Function: Specifies the secondary port of the MRPP ring.

Parameters: <ring-id> is the MRPP ring ID, ranging from 1 to 4096.

Command Mode: Port Mode.

Default: None.

Usage Guidelines: Specifies the secondary port of the MRPP ring. The master node receives on the secondary port the Hello packets it sent from the primary port. On a transit node, the primary and secondary ports have the same function.

mrpp enable must be configured before **control-vlan**. The MRPP ring takes effect after the primary port, secondary port, node mode, and **enable** commands are configured after **control-vlan**.

Example: Set the secondary port of MRPP ring 4000 to Ethernet 1/0/3.

```
Switch(config)#interface ethernet1/0/3
Switch(Config-If-Ethernet1/0/3)#mrpp ring 4000 secondary-port
```

8.3.15 node-mode

Command: node-mode {maser | transit}

Function: Configures the node type as master node or transit node.

Parameters: master: Master node. **transit**: Transit node.

Command Mode: MRPP Ring Mode.

Default: Transit node.

Usage Guidelines: None.

Example: Configure the switch as the master node of MRPP ring 4000.

```
Switch(config)# mrpp ring 4000
Switch(mrpp-ring-4000)#node-mode master
```

8.3.16 show mrpp

Command: show mrpp [<ring-id>]

Function: Displays the MRPP ring configuration.

Parameters: <ring-id> is the MRPP ring ID, ranging from 1 to 4096. If no ID is specified, the configuration of all MRPP rings is displayed.

Command Mode: Admin Mode and Configuration Mode.

Default: None.

Usage Guidelines: None.

Example: Display the configuration of MRPP ring 4000.

```
Switch# show mrpp 4000
```

8.3.17 show mrpp statistics

Command: show mrpp statistics [<ring-id>]

Function: Displays the statistics of packets received and sent on MRPP rings.

Parameters: <ring-id> is the MRPP ring ID, ranging from 1 to 4096. If no ID is specified, the statistics of all MRPP rings are displayed.

Command Mode: Admin Mode and Configuration Mode.

Default: None.

Usage Guidelines: None.

Example: Display the statistics of MRPP ring 4000.

```
Switch# show mrpp statistic 4000
```

8.4 ULPP

8.4.1 clear ulpp flush counter interface

Command: `clear ulpp flush counter interface <name>`

Function: Clears the flush packet statistics.

Parameters: <name> is the port name.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example: Clear the flush packet statistics of port Ethernet 1/0/1.

```
Switch#clear ulpp flush counter interface e1/0/1
ULPP flush counter has been reset.
```

8.4.2 control vlan

Command: `control vlan <integer>`
`no control vlan`

Function: Configures the control VLAN of the ULPP group. The **no** form of this command restores the default.

Parameters: <integer> is the control VLAN ID used to send flush packets, ranging from 1 to 4094.

Default: VLAN 1.

Command Mode: ULPP Group Mode.

Usage Guidelines: Configures the control VLAN of the ULPP group. The VLAN must already exist and cannot be deleted after it is configured. It must belong to the VLANs protected by the ULPP group, to prevent flush packets from looping.

Example: Set the sending control VLAN of the ULPP group to 10.

```
Switch(config)# ulpp group 20
Switch(ulpp-group-20)# control vlan 10
```

8.4.3 debug ulpp error

Command: `debug ulpp error`
`no debug ulpp error`

Function: Displays ULPP error information. The **no** form of this command disables it.

Parameters: None.

Default: Not displayed.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example: Display ULPP error information.

```
Switch# debug ulpp error
Unrecognized Flush packet received.
```

8.4.4 debug ulpp event

Command: `debug ulpp event`
`no debug ulpp event`

Function: Displays ULPP event information. The **no** form of this command disables it.

Parameters: None.

Default: Not displayed.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example: Display ULPP event information.

```
Switch# debug ulpp event
ULPP group 1 state changes:
Master port ethernet 1/0/1 in ULPP group 1 changed state to Forwading.
Slave port ethernet 1/0/2 in ULPP group 1 changed state to Standby.
```

8.4.5 debug ulpp flush {send | receive} interface

Command: `debug ulpp flush {send | receive} interface <name>`
`no debug ulpp flush {send | receive} interface <name>`

Function: Displays information about flush packets sent or received (not the detailed packet contents). The **no** form of this command disables it.

Parameters: <name> is the port name.

Default: Not displayed.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example: Display information about flush packets sent on port Ethernet 1/0/1.

```
Switch# debug ulpp flush send interface e1/0/1
Flush packet send on port Ethernet 1/0/1.
```

8.4.6 description

Command: `description <string>`
`no description`

Function: Configures the description of the ULPP group. The **no** form of this command deletes the description.

Parameters: <string> is the description of the ULPP group, up to 128 characters.

Default: No description is configured.

Command Mode: ULPP Group Mode.

Usage Guidelines: None.

Example: Set the description of the ULPP group to test.

```
Switch(config)# ulpp group 20
Switch(ulpp-group-20)# description test
```

8.4.7 flush disable arp

Command: `flush disable arp`

Function: Disables sending flush packets that delete ARP entries.

Parameters: None.

Default: Enabled.

Command Mode: ULPP Group Mode.

Usage Guidelines: With this command configured, when the link switches over, the switch does not send flush packets to notify the upstream device to delete ARP entries.

Example: Disable sending flush packets that delete ARP entries.

```
Switch(config)# ulpp group 20
Switch(ulpp-group-20)# flush disable arp
```

8.4.8 flush disable mac

Command: `flush disable mac`

Function: Disables sending flush packets that update the MAC address table.

Parameters: None.

Default: Enabled.

Command Mode: ULPP Group Mode.

Usage Guidelines: With this command configured, when the link switches over, the switch does not send flush packets to notify the upstream device to update the MAC address table.

Example: Disable sending flush packets that update the MAC address table.

```
Switch(config)# ulpp group 20
Switch(ulpp-group-20)# flush disable mac
```

8.4.9 flush disable mac-vlan

Command: `flush disable mac-vlan`

Function: Disables sending flush packets that delete dynamic unicast MAC addresses by VLAN.

Parameters: None.

Default: Disabled.

Command Mode: ULPP Group Mode.

Usage Guidelines: With this command configured, when the link switches over, the switch does not send flush packets to notify the upstream device to delete dynamic unicast MAC addresses by VLAN.

Example: Disable sending mac-vlan flush packets.

```
Switch(config)#ulpp group 1
Switch(ulpp-group-1)#flush disable mac-vlan
```

8.4.10 flush enable arp

Command: `flush enable arp`

Function: Enables sending flush packets that delete ARP entries.

Parameters: None.

Default: Enabled.

Command Mode: ULPP Group Mode.

Usage Guidelines: With this function enabled, when the link switches over, the switch sends flush packets to notify the upstream device to delete ARP entries.

Example: Enable sending flush packets that delete ARP entries.

```
Switch(config)# ulpp group 20
Switch(ulpp-group-20)# flush enable arp
```

8.4.11 flush enable mac

Command: `flush enable mac`

Function: Enables sending flush packets that update the MAC address table.

Parameters: None.

Default: Enabled.

Command Mode: ULPP Group Mode.

Usage Guidelines: With this function enabled, when the link switches over, the switch sends flush packets to notify the upstream device to update the MAC address table.

Example: Enable sending flush packets that update the MAC address table.

```
Switch(config)# ulpp group 20
Switch(ulpp-group-20)# flush enable mac
```

8.4.12 flush enable mac-vlan

Command: `flush enable mac-vlan`

Function: Enables sending flush packets that delete dynamic unicast MAC addresses by VLAN.

Parameters: None.

Default: Disabled.

Command Mode: ULPP Group Mode.

Usage Guidelines: With this command configured, when the link switches over, the switch sends flush packets to notify the upstream device to delete dynamic unicast MAC addresses by VLAN.

Example: Enable sending mac-vlan flush packets.

```
Switch(config)#ulpp group 1
Switch(ulpp-group-1)#flush enable mac-vlan
```

8.4.13 preemption delay

Command: `preemption delay <integer>`
`no preemption delay`

Function: Configures the preemption delay. The **no** form of this command restores the default.

Parameters: <integer>: The preemption delay, ranging from 1 to 600 seconds.

Default: 30 seconds.

Command Mode: ULPP Group Mode.

Usage Guidelines: The preemption delay is the time before the master port preempts the forwarding state, which prevents link flapping. The preemption delay takes effect after preemption mode is enabled.

Example: Set the preemption delay of the ULPP group to 50 seconds.

```
Switch(config)# ulpp group 20
Switch(ulpp-group-20)# preemption delay 50
```

8.4.14 preemption mode

Command: `preemption mode`
`no preemption mode`

Function: Enables or disables the preemption mode of the ULPP group.

Parameters: None.

Default: Preemption is disabled.

Command Mode: ULPP Group Mode.

Usage Guidelines: If preemption mode is configured for the ULPP group, the slave port is forwarding, and the master port is in standby, then after the preemption delay the master port changes to forwarding and the slave port changes to standby.

Example: Enable the preemption mode of the ULPP group.

```
Switch(config)# ulpp group 20
```

```
Switch(ulpp-group-20)# preemption mode
```

8.4.15 protect vlan-reference-instance

Command: protect vlan-reference-instance <instance-list>
no protect vlan-reference-instance <instance-list>

Function: Configures the VLANs protected by the ULPP group. The **no** form of this command cancels the protected VLANs.

Parameters: <instance-list> is a list of MSTP instances, such as i;j-k. The number of instances in the list is not limited.

Default: No VLANs are protected; no instances are referenced.

Command Mode: ULPP Group Mode.

Usage Guidelines: Protects VLANs by referencing MSTP instances. The VLANs of a referenced instance are forwarding on one port of the group and blocked on the other. Each ULPP group can reference any MSTP instance, including instances that do not exist (in which case no VLANs are protected), but different ULPP groups cannot reference the same instance.

Example: Configure the ULPP group to protect the VLANs of instance 1.

```
Switch(config)# ulpp group 20
Switch(ulpp-group-20)# protect vlan-reference-instance 1
```

8.4.16 show ulpp flush counter interface

Command: show ulpp flush counter interface {ethernet <IFNAME> | <IFNAME>}

Function: Displays flush packet statistics.

Parameters: <IFNAME> is the port name.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays flush packet statistics, such as the number of flush packets received and the time the last flush packet was received.

Example: Display the flush packet statistics of port Ethernet 1/0/1.

```
Switch# show ulpp flush counter interface e1/0/1
Received flush packets: 10
```

8.4.17 show ulpp flush-receive-port

Command: show ulpp flush-receive-port

Function: Displays the ports that receive flush packets, with their flush types and control VLANs.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example: Display the ports that receive flush packets.

```
Switch# show ulpp flush-receive-port
ULPP flush-receive portlist:
Portname        Type  Control Vlan
-----------------------------------------------
Ethernet1/0/1      ARP   1
Ethernet1/0/3      MAC   1;3;5-10
```

8.4.18 show ulpp group

Command: `show ulpp group [group-id]`

Function: Displays the configuration of the configured ULPP groups.

Parameters: [group-id]: Displays the information of the specified ULPP group.

Default: Information of all configured ULPP groups is displayed.

Command Mode: Admin Mode.

Usage Guidelines: Displays the configuration of ULPP groups, such as the state of the master and slave ports, preemption mode, and preemption delay.

Example: Display the configuration of ULPP group 1.

```
Switch# show ulpp group 1
ULPP group 1 information:
Description: abc
Preemption mode: on
Preemption delay: 30s
Control VLAN:1
Protected VLAN: Reference Instance 1
Member          Role        State
--------------------------------------------------------------
Ethernet1/0/1      MASTER     FORWARDING
Ethernet1/0/2      SLAVE       STANDBY
```

8.4.19 ulpp control vlan

Command: `ulpp control vlan <vlan-list>`
`no ulpp control vlan <vlan-list>`

Function: Configures the control VLANs on which the port receives flush packets. The **no** form of this command restores the default.

Parameters: <vlan-list> is the list of control VLANs on which flush packets are received, such as i;j-k. Each list can contain up to 100 VLANs. Receiving control VLANs can be added to the port.

Default: VLAN 1.

Command Mode: Port Mode.

Usage Guidelines: Configures the receiving control VLANs of the port. The VLANs must already exist and cannot be deleted after they are configured.

Example: Set the receiving control VLAN to 10.

```
Switch(config)# interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)# ulpp control vlan 10
```

8.4.20 ulpp flush disable arp

Command: `ulpp flush disable arp`

Function: Disables receiving flush packets that delete ARP entries.

Parameters: None.

Default: Disabled (flush packets that delete ARP entries are not received).

Command Mode: Port Mode.

Usage Guidelines: With this command configured, the port does not process flush packets that delete ARP entries.

Example: Disable receiving flush packets that delete ARP entries.

```
Switch(config)# interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)# ulpp flush disable arp
```

8.4.21 ulpp flush disable mac

Command: `ulpp flush disable mac`

Function: Disables receiving flush packets that update the MAC address table.

Parameters: None.

Default: Disabled (flush packets that update the MAC address table are not received).

Command Mode: Port Mode.

Usage Guidelines: With this command configured, the port does not process flush packets that update the MAC address table.

Example: Disable receiving flush packets that update the MAC address table.

```
Switch(config)# interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)# ulpp flush disable mac
```

8.4.22 ulpp flush disable mac-vlan

Command: `ulpp flush disable mac-vlan`

Function: Disables receiving mac-vlan flush packets.

Parameters: None.

Default: Disabled.

Command Mode: Port Mode.

Usage Guidelines: With this command configured, mac-vlan flush packets received on the port are forwarded in hardware without being processed.

Example: Disable receiving mac-vlan flush packets on the port.

```
Switch(config)#interface e1/0/2
Switch(config-if-ethernet1/0/2)#ulpp flush disable mac-vlan
```

8.4.23 ulpp flush enable arp

Command: `ulpp flush enable arp`

Function: Enables receiving flush packets that delete ARP entries.

Parameters: None.

Default: Disabled.

Command Mode: Port Mode.

Usage Guidelines: Enable this function to receive flush packets that delete ARP entries.

Example: Enable receiving flush packets that delete ARP entries.

```
Switch(config)# interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)# ulpp flush enable arp
```

8.4.24 ulpp flush enable mac

Command: `ulpp flush enable mac`

Function: Enables receiving flush packets that update the MAC address table.

Parameters: None.

Default: Disabled.

Command Mode: Port Mode.

Usage Guidelines: Enable this function to receive flush packets that update the MAC address table.

Example: Enable receiving flush packets that update the MAC address table.

```
Switch(config)# interface ethernet 1/0/1
```

```
Switch(config-If-Ethernet1/0/1)# ulpp flush enable mac
```

8.4.25 ulpp flush enable mac-vlan

Command: `ulpp flush enable mac-vlan`

Function: Enables receiving mac-vlan flush packets.

Parameters: None.

Default: Disabled.

Command Mode: Port Mode.

Usage Guidelines: With this function enabled, the interface processes received mac-vlan flush packets and deletes dynamic unicast MAC addresses according to the VLAN information in the packets.

Example: Enable receiving mac-vlan flush packets on the port.

```
Switch(config)#interface e1/0/2
Switch(config-if-ethernet1/0/2)#ulpp flush enable mac-vlan
```

8.4.26 ulpp group

Command: `ulpp group <integer>`
`no ulpp group <integer>`

Function: Creates a ULPP group, or enters ULPP Group Mode if the group exists. The **no** form of this command deletes the ULPP group.

Parameters: <integer> is the ULPP group ID, ranging from 1 to 48.

Command Mode: Global Mode.

Default: No ULPP group is configured.

Usage Guidelines: None.

Example: Create ULPP group 20 or enter its configuration mode.

```
Switch(config)# ulpp group 20
Switch(ulpp-group-20)#
```

8.4.27 ulpp group master

Command: `ulpp group <integer> master`
`no ulpp group <integer> master`

Function: Configures the master port of the ULPP group. The **no** form of this command deletes the master port.

Parameters: <integer> is the ULPP group ID, ranging from 1 to 48.

Default: No master port is configured.

Command Mode: Port Mode.

Usage Guidelines: The master and slave ports of a group can be configured in any order, but the protected VLANs must be configured before the member ports. Each group has only one master port; if a master port already exists, the configuration fails.

Example: Configure the master port of the ULPP group.

```
Switch(config)# interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)# ulpp group 20 master
```

8.4.28 ulpp group slave

Command: ulpp group <integer> slave
no ulpp group <integer> slave

Function: Configures the slave port of the ULPP group. The **no** form of this command deletes the slave port.

Parameters: <integer> is the ULPP group ID, ranging from 1 to 48.

Default: No slave port is configured.

Command Mode: Port Mode.

Usage Guidelines: The master and slave ports of a group can be configured in any order, but the protected VLANs must be configured before the member ports. Each group has only one slave port; if a slave port already exists, the configuration fails.

Example: Configure the slave port of the ULPP group.

```
Switch(config)# interface ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)# ulpp group 20 slave
```

8.5 ULSM

8.5.1 debug ulsm event

Command: debug ulsm event
no debug ulsm event

Function: Displays ULSM event information. The **no** form of this command disables it.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example: Display ULSM event information.

```
Switch# debug ulsm event
Downlink synchoronized with ULSM group, change state to Down.
```

8.5.2 show ulsm group

Command: show ulsm group [group-id]

Function: Displays the configuration of ULSM groups.

Parameters: [group-id]: The ULSM group ID.

Default: Information of all configured ULSM groups is displayed.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example: Display the configuration of ULSM group 1.

```
Switch# show ulsm group 1
ULSM group 1 information:
ULSM group state: Down
Member         Role          State         Down by ULSM
-------------------------------------------------------------------------------
---------------
ethernet1/0/1      UpLINK       Down
ethernet1/0/2      DownLINK     Down            Yes
```

8.5.3 ulsm group

Command: `ulsm group <group-id>`
`no ulsm group <group-id>`

Function: Creates a ULSM group. The **no** form of this command deletes the ULSM group.

Parameters: <group-id> is the ULSM group ID, ranging from 1 to 32.

Default: No ULSM group is configured.

Command Mode: Global Mode.

Usage Guidelines: None.

Example: Create ULSM group 10.

```
Switch(config)# ulsm group 10
```

8.5.4 ulsm group {uplink | downlink}

Command: `ulsm group <group-id> {uplink | downlink}`
`no ulsm group <group-id>`

Function: Configures the uplink or downlink ports of the ULSM group. The **no** form of this command removes the port from the group.

Parameters: <group-id>: The ULSM group ID, ranging from 1 to 32.

uplink: Configures the port as an uplink port.

downlink: Configures the port as a downlink port.

Default: The port does not belong to any ULSM group.

Command Mode: Port Mode.

Usage Guidelines: Configures the uplink and downlink ports of the ULSM group. Each ULSM group can have up to 8 uplink ports and 16 downlink ports.

Example: Configure port Ethernet 1/0/3 as an uplink port of ULSM group 10.

```
Switch(config)# interface ethernet 1/0/3
Switch(config-If-Ethernet1/0/3)# ulsm group 10 uplink
```

8.6 ERPS

8.6.1 ethernet tcn-propagation erps to {erps | stp}

Command: `ethernet tcn-propagation erps to {erps | stp}`
`no ethernet tcn-propagation erps to`

Function: Configures how topology change notifications are propagated. Currently, R-APS event notification between ERPS rings is supported: after its topology changes, a sub-ring sends R-APS event packets to the interconnected ring to notify the neighboring ring. By default, a topology change takes effect only within the ring and is not propagated outside it, so it does not affect the neighboring topology. The **no** form of this command deletes the notification method.

Parameters: erps: On topology change, sends R-APS event packets to notify the ERPS rings connected to this device. **stp**: On topology change, sends STP packets to notify the STP topology connected to this device.

Default: An ERPS ring topology change takes effect only within the ring, and no notification packets are sent.

Command Mode: Global Mode.

Usage Guidelines: Configures the topology change notification method of this device. When an ERPS ring instance detects a change, it sends notification packets: with **erps**, R-APS event packets are sent to other ERPS rings; with **stp**, STP packets are sent.

Example:

Send R-APS event notifications to the interconnected ring after a topology change.

```
Switch(config)#ethernet tcn-propagation erps to erps
```

Send STP notifications after a topology change.

```
Switch(config)#ethernet tcn-propagation erps to stp
```

Delete the topology change notification method.

```
Switch(config)#no ethernet tcn-propagation erps to
```

8.6.2 erps-ring <ring-name>

Command: `erps-ring < ring-name >`
`no erps-ring < ring-name >`

Function: Creates an ERPS ring and enters ERPS Ring Mode; if the ring exists, enters its configuration mode. The **no** form of this command deletes the ERPS ring.

Parameters: <ring-name>: The name of the ERPS ring, up to 64 characters consisting of letters, digits, and underscores. The first and last characters cannot be underscores.

Command Mode: Global Mode.

Default: No ERPS ring is configured.

Usage Guidelines: If the ring name exceeds 64 bytes, the message "Valid ERPS ring name should be no more than 64 bytes!" is displayed. If the ring name format is invalid, the message "Invalid ERPS ring name!" is displayed. If the maximum number of ERPS rings has been reached, the message "Support ERPS ring max number: 32!" is displayed. If the ERPS ring exists, the switch enters its configuration mode; otherwise, it creates the ring and enters ERPS Ring Mode.

Example:

Create ERPS ring ring1.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#
```

Delete ERPS ring ring1.

```
Switch(config)#no erps-ring ring1
```

8.6.3 version {v1 | v2}

Command: `version {v1 | v2}`
`no version`

Function: Configures the ERPS version supported by the ring. The current implementation supports v2, which is backward compatible with v1. v1 does not support management commands such as MS and FS, does not support multiple instances, and supports only revertive switching. If no instance is configured on the ERPS ring, the version can be configured repeatedly, and the last configuration takes effect. If an ERPS ring instance is configured on the ring, the version cannot be changed. The **no** form of this command restores the default, v2.

Parameters: v1: Supports v1, released in June 2008, with its amendment (April 2009). **v2**: Supports v2, released in March 2010, with its amendment (June 2010).

Command Mode: ERPS Ring Mode.

Default: v2.

Usage Guidelines:

1. If an ERPS ring instance is configured on the ring, the message "Cann't config version on ERPS ring whitch has ERPS instance, please delete ERPS instance firstly!" is displayed; otherwise, the configuration continues.

2. The ERPS ring is configured to support the specified protocol version.

3. If the ring is configured for v1, it does not support multiple instances; its instance does not support management commands such as MS and FS, and non-revertive switching does not take effect. Only revertive switching is supported.

4. If the ring is configured for v1, its instance processes ERPS packets in v1 format: R-APS packets are built and parsed in v1 format, and fields defined in v2 are ignored.

Example:

Configure ERPS ring ring1 to support v1.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#version v1
```

Configure ERPS ring ring1 to support v2.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#version v2
```

Remove the v1 setting of ERPS ring ring1 (restore v2).

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#no version
```

8.6.4 open-ring

Command: `open-ring`
`no open-ring`

Function: Configures the ERPS ring as an open sub-ring. If an ERPS ring instance is configured on the ring, the ring type cannot be changed until the instance is deleted. All nodes on the ring must have the same configuration. This type of ring can connect to other ERPS rings in interconnected topologies. The **no** form of this command restores the default, a closed major ring.

Parameters: None.

Command Mode: ERPS Ring Mode.

Default: Closed major ring.

Usage Guidelines: If an ERPS ring instance is configured on the ring, the message "Cann't config open-ring on ERPS ring whitch has ERPS instance, please delete ERPS instance firstly!" is displayed; otherwise, the ring is configured as a sub-ring.

Example:

Configure ERPS ring ring1 as an open sub-ring.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#open-ring
```

Delete the open sub-ring configuration.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#no open-ring
```

8.6.5 raps-virtual-channel {with | without}

Command: `raps-virtual-channel {with | without}`

Function: Configures whether the ERPS ring has an R-APS virtual channel. Configure it only on the nodes of a sub-ring; the configuration must be the same on all nodes.

Parameters: with: The ERPS ring has an R-APS virtual channel. **without**: The ERPS ring has no R-APS virtual channel.

Command Mode: ERPS Ring Mode.

Default: The ERPS ring has no R-APS virtual channel.

Usage Guidelines:

a) On a major ring, the message "Cann't config R-APS virtual channel on ERPS major ring!" is displayed.

b) Otherwise, the R-APS virtual channel is configured as specified.

Result: success or error. If the ERPS ring has no R-APS virtual channel, the R-APS channels of all instances of the ring are always unblocked and only the data channel is blocked; otherwise, both the R-APS channel and the data channel are blocked.

Example:

Configure an R-APS virtual channel on ERPS sub-ring ring1.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#raps-virtual-channel with
```

8.6.6 erps-ring <ring-name> port0 [port1-none]

Command: `erps-ring <ring-name> port0 [port1-none]`
`no erps-ring <ring-name> port0`

Function: Configures port0 of the ERPS ring node. Each node has only one port0; if port0 already exists, the new configuration does not overwrite it and an error is reported. **port1-none** indicates that the node has no port1 on this ring, that is, it is an interconnection node. The **no** form of this command deletes port0.

Parameters: <ring-name>: The ERPS ring name, up to 64 characters consisting of letters, digits, and underscores. The first and last characters cannot be underscores.

port1-none: The node has only port0 on this ERPS ring and no port1; it is an interconnection node.

Command Mode: Port Mode.

Default: No port0 is configured on the ERPS ring.

Usage Guidelines:

If the ring name exceeds 64 bytes, the message "Valid ERPS ring name should be no more than 64 bytes!" is displayed.

If the ring name format is invalid, the message "Invalid ERPS ring name!" is displayed.

If STP or another mutually exclusive module is enabled on the port, the message "Port %s has enable stp or other mutex module!" is displayed, where %s is the port name.

If the port is a member of an aggregation group, the message "Port %s is LAG member port!" is displayed, where %s is the port name.

If the ERPS ring does not exist, the message "The ERPS ring doesn't exist!" is displayed.

If port0 already exists on the ERPS ring, the message "Port0 exists on the ERPS ring already!" is displayed.

If the port is already configured as port1 of the ERPS ring, the message "Port %s is already configed as port1 on the ERPS ring!" is displayed, where %s is the port name.

If the ERPS ring is not an open ring, port1-none cannot be configured, and the message "Can not config port1-none on ERPS major ring!" is displayed.

Otherwise, the port is configured as port0 of the specified ERPS ring.

The switch then checks whether the ERPS ring configuration is complete; if so, it checks whether the ERPS instance configuration is complete; if so, it activates the instance and runs the protocol.

Example:

Configure Ethernet 1/0/1 as port0 of ERPS ring ring1.

```
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#erps-ring ring1 port0
```

Delete Ethernet 1/0/1 as port0 of ERPS ring ring1.

```
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#no erps-ring ring1 port0
```

8.6.7 erps-ring <ring-name> port1

Command: erps-ring <ring-name> port1
no erps-ring <ring-name> port1

Function: Configures port1 of the ERPS ring node. Each node has only one port1; if port1 already exists, the new configuration does not overwrite it and an error is reported. If port1-none is configured, port1 cannot be configured. The **no** form of this command deletes port1.

Parameters: <ring-name>: The ERPS ring name, up to 64 characters consisting of letters, digits, and underscores. The first and last characters cannot be underscores.

Command Mode: Port Mode.

Default: No port1 is configured on the ERPS ring.

Usage Guidelines:

If the ring name exceeds 64 bytes, the message "Valid ERPS ring name should be no more than 64 bytes!" is displayed.

If the ring name format is invalid, the message "Invalid ERPS ring name!" is displayed.

If STP or another mutually exclusive module is enabled on the port, the message "Port %s has enable stp or other mutex module!" is displayed, where %s is the port name.

If the port is a member of an aggregation group, the message "Port %s is LAG member port!" is displayed, where %s is the port name.

If the ERPS ring does not exist, the message "The ERPS ring doesn't exist!" is displayed.

If port1 already exists on the ERPS ring, the message "Port1 exists on the ERPS ring already!" is displayed.

If the port is already configured as port0 of the ERPS ring, the message "Port %s is already configed as port0 on the ERPS ring!" is displayed, where %s is the port name.

If port1-none is configured on the ERPS ring, the message "Has configed port1-none on the ERPS open ring!" is displayed.

Otherwise, the port is configured as port1 of the specified ERPS ring.

The switch then checks whether the ERPS ring configuration is complete; if so, it checks whether the ERPS instance configuration is complete; if so, it activates the instance and runs the protocol.

Example:

Configure Ethernet 1/0/1 as port1 of ERPS ring ring1.

```
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#erps-ring ring1 port1
```

Delete Ethernet 1/0/1 as port1 of ERPS ring ring1.

```
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#no erps-ring ring1 port1
```

8.6.8 failure-detect {cc | physical-link-or-cc} domain <domain-name> service {< ma-name > | number < ma-num > | pvlan < vlan-id >} mep <mep-id> rmep<rmep-id>

Command: {port0 | port1} failure-detect {cc | physical-link-or-cc} domain <domain-name> service {< ma-name > | number < ma-num > | pvlan < vlan-id >} mep <mep-id> rmep<rmep-id>

no {port0 | port1} failure-detect

Function: Configures the failure detection type of the ERPS ring ports. For CC detection, specify the maintenance domain and maintenance association to which the CC belongs and the monitored link (identified by the mep-id and rmep-id pair). The ring port must already be added to the ERPS ring. The **no** form of this command deletes the failure detection type.

Parameters: {port0 | port1}: The failure detection type of port0 or port1.

{cc | physical-link-or-cc}: **cc**: The ERPS ring port detects failures reported by CC. **physical-link-or-cc**: The port detects failures reported by CC and physical link failures.

<domain-name>: The CFM domain name used for detection.

<ma-name>: The CFM service (MA) name used for detection.

<mep-id>: The local MEP ID monitored by CFM.

<rmep-id>: The remote MEP ID monitored by CFM.

Command Mode: ERPS Ring Mode.

Default: ERPS ring ports detect only physical link failures.

Usage Guidelines:

If the domain name exceeds 43 bytes, the message "Valid domain name should be no more than 43 bytes!" is displayed.

If the domain name format is invalid, the message "Invalid domain name!" is displayed.

If the service name exceeds 45 bytes, the message "Valid service name should be no more than 45 bytes!" is displayed.

If the service name format is invalid, the message "Invalid service name!" is displayed.

If the local MEP and the remote MEP are the same, the message "The local mep can not be the same as the remote mep!" is displayed; otherwise, the configuration continues.

The failure detection type of the ERPS ring port is set to the specified type. For the cc type, the configured MD, MA, MEP, and RMEP are saved and used to match received CFM failure notifications.

Example:

Set the detection type of port0 of ERPS ring ring1 to CC.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#port0 failure-defect cc domain domain1 service
serivice1 mep 1 rmep 2
```

Delete this configuration.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#no port0 failure-defect
```

8.6.9 erps-instance <instance-id>

Command: erps-instance <instance-id>

no erps-instance <instance-id>

Function: Creates an ERPS ring instance and enters ERPS Instance Mode; if the instance exists, enters its configuration mode. If the ERPS ring supports v2, multiple instances can be configured. The **no** form of this command deletes the ERPS ring instance.

Parameters: <instance-id>: The ERPS instance ID, ranging from 1 to 48.

Command Mode: ERPS Ring Mode.

Default: No ERPS ring instance is configured.

Usage Guidelines: If the ERPS ring supports v1 and more than one instance is configured, the message "Doesn't support multiple ERPS instance capability on the ring running version 1!" is displayed.

If the number of instances exceeds the supported maximum, the message "Support ERPS instance max number: 32 per ERPS ring!" is displayed.

If the instance already exists on the ERPS ring, the switch enters its configuration mode.

Otherwise, the switch creates the instance and enters ERPS Instance Mode.

Example:

Configure ERPS instance 1 on ERPS ring ring1.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)#
```

Delete ERPS instance 1 on ERPS ring ring1.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#no erps-instance 1
Switch(config-erps-ring-inst-1)#
```

8.6.10 description

Command: `description <instance-name>`
`no description <instance-name>`

Function: Configures the description of the ERPS instance. The **no** form of this command deletes the description.

Parameters: <instance-name>: The ERPS instance name, up to 64 characters consisting of letters, digits, and underscores. The first and last characters cannot be underscores.

Command Mode: ERPS Instance Mode.

Default: No instance name is configured.

Usage Guidelines: If the string exceeds 64 bytes, the message "Valid ERPS instance name should be no more than 64 bytes!" is displayed. If the string format is invalid, the message "Invalid ERPS instance name!" is displayed. Otherwise, the instance name is set to the specified string.

Example:

Set the name of ERPS instance 1 on ring1 to instance1.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)# description instance1
```

Delete the name of instance 1.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)# no description
```

8.6.11 ring-id <ring-id>

Command: `ring-id <ring-id>`
`no ring-id <ring-id>`

Function: Configures the last byte of the destination MAC address of R-APS packets sent by the ERPS ring node to carry the ring ID. If the ERPS ring supports v1, the ring ID can only be 1. The **no**

form of this command configures the packets not to carry the ring ID; the destination MAC address is then 01-19-A7-00-00-01.

Parameters: <ring-id>: The ERPS ring ID, ranging from 1 to 64.

Command Mode: ERPS Instance Mode.

Default: The destination MAC address is 01-19-A7-00-00-01.

Usage Guidelines: If the ERPS ring supports v1, the ring ID can only be 1, because v1 supports only the destination MAC address 01-19-A7-00-00-01; otherwise, the message "Cann't config ringid other than 1 on the ERPS ring running version 1!" is displayed.

If the ERPS ring supports v2, the last byte of the destination MAC address of R-APS packets sent by the ERPS ring node carries the specified ring ID.

Example:

Configure the R-APS packets sent by instance 2 of ERPS ring ring1 to carry ring ID 2 in the last byte of the destination MAC address.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 2
Switch(config-erps-ring-inst-2)#ring-id 2
```

Configure the R-APS packets sent by instance 2 of ERPS ring ring1 not to carry the ring ID; the destination MAC address is then 01-19-A7-00-00-01.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 2
Switch(config-erps-ring-inst-2)#no ring-id
```

8.6.12 rpl {port0 | port1} {owner | neighbour}

Command: `rpl {port0 | port1} {owner | neighbour}`
`no rpl {port0 | port1}`

Function: Configures a member port of the ERPS ring instance as the RPL owner or RPL neighbor. RPL roles of different instances on the same ERPS ring cannot be configured on the same member port. The **no** form of this command configures the member port as an ordinary ring port.

Parameters: {port0 | port1}: The RPL role of port0 or port1 in the ERPS ring instance.

{owner | neighbour}: **owner** configures the member port as the RPL owner; **neighbour** configures it as the RPL neighbor.

Command Mode: ERPS Instance Mode.

Default: None; the node is an ordinary ring node.

Usage Guidelines: If port1-none is configured, the node role of port1 cannot be configured, and the message "Has configed port1-none on the ERPS open ring!" is displayed.

If this instance node is already an RPL owner or RPL neighbor, this command cannot be applied to any member port, and the message "Has configed port rpl role: %s on the ERPS instance!" is displayed, where %s is the configured RPL role.

If another instance on the ERPS ring has already configured the specified RPL role, the message "Has configed port rpl role: %s in this or other ERPS instance on the ERPS ring!" is displayed. Otherwise, the specified member port of the instance is configured with the specified node role.

Example:

Configure port0 of instance 1 of ERPS ring ring1 as the RPL owner.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)# rpl port0 owner
```

Configure port0 of instance 1 of ERPS ring ring1 as an ordinary ring port.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)# no rpl port0
```

8.6.13 non-revertive

Command: non-revertive
no non-revertive

Function: Configures the ERPS ring instance as non-revertive. The **no** form of this command configures it as revertive. If the ERPS ring supports v1, this command has no effect and cannot be configured. This command can be configured only on the RPL owner node of a sub-ring.

Parameters: None.

Command Mode: ERPS Instance Mode.

Default: Revertive.

Usage Guidelines: If the ERPS ring supports v1, the message "Cann't config non-revertive on the ERPS ring running version 1!" is displayed.

If the ERPS ring supports v2, the ERPS ring instance is configured as non-revertive.

Example:

Configure instance 1 of ERPS ring ring1 as non-revertive.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)#non-revertive
```

Delete this configuration.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)#no non-revertive
```

8.6.14 guard-timer <guard-times>

Command: guard-timer <guard-times>
no guard-timer

Function: Configures the guard timer. The guard timer prevents an Ethernet ring node from acting on outdated R-APS packets, which could cause errors and loops. While the timer is running, all received R-APS packets (except those with Request/State "1110") are discarded. The **no** form of this command restores the default.

Parameters: <guard-times>: The guard time, in steps of 10 ms, ranging from 10 ms to 2 s.

Command Mode: ERPS Instance Mode.

Default: 500 ms.

Usage Guidelines: If the timer is not running, the guard timer of the ERPS ring instance is set to the specified time. If it is running, the new value is saved but the running timer is not reset: it continues with the previous value, and the new value takes effect the next time the timer starts.

Example:

Set the guard timer of instance 1 of ERPS ring ring1 to 1 second.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)guard-timer 100
```

Restore the default guard timer of instance 1 of ERPS ring ring1.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1) no guard-timer
```

8.6.15 holdoff-timer < holdoff-times>

Command: holdoff –timer <holdoff-times>
no holdoff -timer

Function: Configures the hold-off timer. The hold-off timer delays the reporting of faults by the Ethernet ring node. When a new fault occurs or an existing fault becomes more severe and the hold-off time is not 0, the fault is not reported to protection switching immediately; instead, the hold-off timer starts. When the timer expires, the node checks whether a link fault still exists; if it does, it is reported to protection switching (it need not be the same fault that started the timer). The **no** form of this command restores the default.

Parameters: <holdoff-times>: The hold-off time, in steps of 1 second, ranging from 0 to 10 seconds.

Command Mode: ERPS Instance Mode.

Default: 0 seconds.

Usage Guidelines: If the timer is not running, the hold-off timer of the ERPS ring instance is set to the specified time. If it is running, the new value is saved but the running timer is not reset: it continues with the previous value, and the new value takes effect the next time the timer starts.

Example:

Set the hold-off timer of instance 1 of ERPS ring ring1 to 5 seconds.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)#holdoff –timer 5
```

Restore the default hold-off timer of instance 1 of ERPS ring ring1.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)#no holdoff –timer
```

8.6.16 wtr-timer <wtr-times>

Command: wtr-timer <wtr-times>
no wtr-timer

Function: Configures the wait-to-restore (WTR) timer. The WTR timer prevents frequent protection switching on the RPL owner node caused by intermittent faults. When the RPL owner port receives fault recovery packets, it waits for the WTR time and checks whether the fault still exists on other nodes, instead of blocking the RPL owner port immediately, which could cause network oscillation. The **no** form of this command restores the default.

Parameters: <wtr-times>: The WTR time, in steps of 1 minute, ranging from 1 to 12 minutes.

Command Mode: ERPS Instance Mode.

Default: 5 minutes.

Usage Guidelines: If the timer is not running, the WTR timer of the ERPS ring instance is set to the specified time. If it is running, the new value is saved but the running timer is not reset: it continues with the previous value, and the new value takes effect the next time the timer starts.

Example:

Set the WTR timer of instance 1 of ERPS ring ring1 to 10 minutes.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)#wtr-timer 10
```

Restore the default WTR timer of instance 1 of ERPS ring ring1.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
```

```
Switch(config-erps-ring-inst-1)#no wtr-timer
```

8.6.17 protected-instance

Command: `protected-instance <instance-list>`
`no protected-instance <instance-list>`

Function: Configures the instances protected by the ERPS ring instance. An ERPS ring instance can protect any MSTP instance. The same MSTP instance cannot be referenced by multiple ERPS ring instances in the same topology. If this command is run more than once in the same ERPS ring instance, the protected instances accumulate. The **no** form of this command deletes the protected instances.

Parameters: <instance-list>: The list of MSTP instances protected by the ERPS ring instance, such as i, j-k. The number of instances in the list is not limited.

Command Mode: ERPS Instance Mode.

Default: The ERPS ring instance does not protect any MSTP instance.

Usage Guidelines: If an entered instance is already protected by another ERPS instance, the message "Instance: %d is protected by erps instance: %d on ring: %s!" is displayed, where the first %d is the MSTP instance ID, the second %d is the ERPS instance ID, and %s is the ERPS ring name.

Otherwise, the specified MSTP instances are configured as protected instances of the ERPS ring instance.

The switch then checks whether the ERPS instance configuration is complete; if so, it activates the instance and runs the protocol.

Example:

Configure instance 1 of ERPS ring ring1 to protect MSTP instance 2.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)#protected-instance 2
```

Delete this configuration.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)#no protected-instance 2
```

8.6.18 raps-mel <level-value>

Command: `raps-mel <level-value>`
`no raps-mel`

Function: Configures the MEL (maintenance entity group level) of the R-APS channel.

Parameters: <level-value>: The level of R-APS packets, ranging from 0 to 7.

Command Mode: ERPS Instance Mode.

Default: 7.

Usage Guidelines: Sets the R-APS channel level of the ERPS ring instance. After the configuration succeeds, the MEL field of R-APS packets sent by this instance carries the specified level, and only R-APS packets whose level is greater than or equal to the specified level are accepted; otherwise, an error is reported. The **no** form restores the default of 7. The MEL field in protocol packets determines whether a packet can pass: if the MEL configured on the ERPS ring is lower than that of the fault detection protocol, the packet level is too low and the packet cannot pass. All nodes in the instance must use the same level.

Example:

Set the R-APS channel level of instance 1 of ERPS ring ring1 to 5.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)raps-mel 5
```

Restore the R-APS channel level of instance 1 of ERPS ring ring1 to 7.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)no raps-mel
```

8.6.19 control-vlan <vlan-id>

Command: `control-vlan <vlan-id>`
`no control-vlan`

Function: Configures the control VLAN of R-APS packets on the R-APS channel. In the ERPS ring instance, this VLAN carries only ERPS protocol packets, not user traffic, which improves ERPS security. Ensure that the control VLAN is unique. R-APS packets are sent with this VLAN tag. The configuration must be the same on all nodes in the instance. The **no** form of this command deletes the control VLAN.

Parameters: <vlan-id>: The VLAN ID of R-APS packets, ranging from 2 to 4094.

Command Mode: ERPS Instance Mode.

Default: No control VLAN is configured.

Usage Guidelines: The configuration must meet the following requirements:

The protected VLAN configuration must be the same on all nodes in the instance.

The control VLAN must be unique.

If the ring of the instance is a major ring, the control VLAN and the protected VLANs must be in the same instance.

If the ring of the instance is an open sub-ring without an R-APS virtual channel, the control VLAN must belong to an instance by itself.

The member ports must belong to the control VLAN and the protected VLANs.

The control VLAN is processed as follows:

a) If the specified VLAN does not exist, the message "Error, VLAN %d does not exist!" is displayed, where %d is the entered value.

b) If a control VLAN is already configured for the ERPS ring instance, the message "Control vlan has existed already!" is displayed.

c) Otherwise, the control VLAN of the ERPS ring instance is set to the specified VLAN.

d) The switch then checks whether the ERPS instance configuration is complete; if so, it activates the instance and runs the protocol.

Note: The data VLANs and control VLANs of different ERPS instances cannot be associated with the same MSTI.

Example:

Set the control VLAN of instance 1 of ERPS ring ring1 to VLAN 10.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)control-vlan 10
```

Delete this configuration.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
```

```
Switch(config-erps-ring-inst-1)no control-vlan
```

8.6.20 forced-switch {port0 | port1}

Command: `forced-switch {port0 | port1}`

Function: Performs a forced switch on a port of the ERPS ring node. Two or more forced switches can exist at the same time in one ERPS ring instance, but only one forced switch can exist on one ring node. Avoid multiple forced switches in an ERPS ring instance, which can split the ring.

Parameters: {port0 | port1}: Performs the forced switch on port0 or port1 of the ring node.

Command Mode: ERPS Instance Mode.

Default: No forced switch exists in the ERPS ring instance.

Usage Guidelines: If the ring runs version 1, the message "Doesn't support the command on the ring running version 1!" is displayed; otherwise, the command continues.

If the instance configuration is incomplete (the instance is inactive), the message "The request is rejected because the ERP instance in unactive state!" is displayed; otherwise, the command continues.

If a local forced switch already exists on this node of the ring instance (only one of port0 and port1 can be in the local FS state at a time), the message "The FS request is rejected because an local FS request is present!" is displayed; otherwise, the command continues.

If the forced switch is currently the highest-priority request, the data channel and R-APS channel of the ERPS ring instance are blocked on the specified member port (port0 or port1), and the other member port of the node is unblocked.

While the forced switch is the highest-priority request, R-APS (FS) packets are sent continuously on both ring ports (port0 and port1).

A node that receives R-APS (FS) packets unblocks all its blocked ring ports if there is no higher-priority local request.

A node that receives R-APS (FS) packets flushes its FDB as required.

Example:

Perform a forced switch on port0 of instance 1 of ERPS ring ring1.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)#force-switch port0
```

8.6.21 manual-switch {port0 | port1}

Command: `manual-switch {port0 | port1}`

Function: Performs a manual switch on a port of the ERPS ring node. Only one manual switch can exist in one ERPS ring instance, and only when there is no SF fault or FS command in the instance.

Parameters: {port0 | port1}: Performs the manual switch on port0 or port1 of the ring node.

Command Mode: ERPS Instance Mode.

Default: No manual switch exists in the ERPS ring instance.

Usage Guidelines: If the ring runs version 1, the message "Doesn't support the command on the ring running version 1!" is displayed; otherwise, the command continues.

If the instance configuration is incomplete (the instance is inactive), the message "The request is rejected because the ERP instance in unactive state!" is displayed; otherwise, the command continues.

If an MS state already exists on the ERPS ring node, the message "The MS request is rejected because an existing MS request is present!" is displayed.

If a forced switch already exists on this node of the ring instance, the message "The MS request is rejected because an existing FS request is present!" is displayed; otherwise, the command continues.

If a fault exists in the ERPS ring instance, the message "The MS request is rejected because an existing SF is present!" is displayed; otherwise, the command continues.

If the manual switch is currently the highest-priority request, the data channel and R-APS channel of the ERPS ring instance are blocked on the specified member port (port0 or port1), and the other member port of the node is unblocked.

While the manual switch is the highest-priority request, R-APS (MS) packets are sent continuously on both ring ports (port0 and port1).

A node that receives R-APS (MS) packets unblocks all its blocked ring ports if there is no higher-priority local request.

A node that receives R-APS (MS) packets flushes its FDB as required.

Example:

Perform a manual switch on port0 of instance 1 of ERPS ring ring1.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)#manual-switch port0
```

8.6.22 clear command

Command: `clear command`

Function: Runs the clear command on the ERPS ring node. It clears active local management commands (forced switch and manual switch). It can also trigger reversion in revertive mode before the WTR or WTB timer expires, and switch traffic back from the RPL to the original link in non-revertive mode after fault recovery. For the last two cases, the command is normally run on the RPL owner node.

Parameters: None.

Command Mode: ERPS Instance Mode.

Default: None.

Usage Guidelines: If the ring runs version 1, the message "Doesn't support the command on the ring running version 1!" is displayed; otherwise, the command continues.

If the instance configuration is incomplete (the instance is inactive), the message "The request is rejected because the ERP instance in unactive state!" is displayed; otherwise, the command continues.

If a forced or manual switch exists on this node of the ring instance, the command is cleared while the data channel and R-APS channel of the blocked member ports remain blocked. R-APS (NR) packets are sent continuously on both member ports until R-APS (NR, RB) packets are received, indicating that the RPL is blocked, or until a higher-priority request (such as SF) occurs on the ring.

If a local forced or manual switch exists on this node, after the command is cleared and R-APS (NR) packets with a node ID greater than the local node ID are received, all ring ports without SF faults are unblocked and the node stops sending R-APS (NR) packets on both member ports.

If the ERPS ring instance of the RPL owner node is in revertive mode and the WTR or WTB timer is running, the timer is stopped, the RPL port is blocked, R-APS (NR, RB) packets are sent on both ring ports, and the FDB is flushed, triggering reversion early. Otherwise, the command continues.

If the ERPS ring instance of the RPL owner node is in non-revertive mode, the RPL port is blocked, R-APS (NR, RB) packets are sent on both ring ports, and the FDB is flushed, switching traffic from the RPL back to the original link.

Example:

Run the clear command on instance 1 of ERPS ring ring1.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)#clear command
```

8.6.23 show erps ring {<ring-name> | brief}

Command: show erps ring {<ring-name> | brief}

Function: Displays ERPS ring information.

Parameters: <ring-name>: The ERPS ring name, up to 64 characters consisting of letters, digits, and underscores. The first and last characters cannot be underscores. If it is not specified, all ERPS rings on the device are displayed.

brief: Displays summary information of the ERPS rings.

Command Mode: Admin Mode.

Default: None.

Example: Display summary information of all ERPS rings.

```
Switch#show erps ring brief
Ring-Name         Ring-topo    Port0   Port1   Version  Inst-Count
------------------------------------------------------------------------------
----------------------------
ring1          maijor-ring   1/0/1     1/0/2     V2      1
ring2          open-ring    1/0/5     1/0/6      V2      1
```

Output	Description
Ring-Name	ERPS ring name, up to 64 characters consisting of letters, digits, and underscores. The first and last characters cannot be underscores.
Ring-topo	ERPS ring topology: major-ring or open-ring
Port0	Port0 of the ERPS ring
Port1	Port1 of the ERPS ring
Version	ERPS version supported by the ring: V1 or V2
Inst-Count	Number of instances of the ERPS ring, ranging from 1 to 64

Display the information of ERPS ring ring1:

```
Switch#show erps ring ring1
R: RPL Owner
N: RPL Neighbour
C: Common Node
------------------------------------------------------------------------------
----------------------------
R-APS ring topology: open-ring
R-APS Virtual-Channel: with
Port0: Ethernet1/0/1              Failure-detect type: physical-link-or-cc
Port1: Ethernet1/0/2              Failure-detect type: physical-link
Instance  Contral  Protected  WTR_Timer  Guard_Timer  Holdoff_Timer  Port0
Port1
ID       Vlan    Instance   (min)        (csec)       (second)
------------------------------------------------------------------------------
---------------------------------
1         10        3      6           100            0           R      C
2         20        4      5           500            0           C      C
```

Output	Description
Instance ID	ERPS ring instance ID, ranging from 1 to 64
Contral Vlan	R-APS channel VLAN, used as the tag of R-APS packets

Protected Instance	MSTP instances protected by the ERPS ring instance
WTR_Timer	Wait-to-restore timer, ranging from 1 to 12 minutes
Guard_Timer	Guard timer, ranging from 10 ms to 2 s
Holdoff_Timer	Hold-off timer, ranging from 0 to 10 s
Port0	Port0 of the ERPS ring
Port1	Port1 of the ERPS ring
R-APS ring topology	ERPS ring topology: major-ring or open-ring
R-APS Virtual-Channel	For an ERPS sub-ring, whether there is an R-APS virtual channel: with or without

8.6.24 show erps instance [ring <ring-name> [instance <instance-id>]]

Command: `show erps instance [ring <ring-name> [instance <instance-id>]]`

Function: Displays ERPS ring instance information.

Parameters: <ring-name>: The ERPS ring name, up to 64 characters consisting of letters, digits, and underscores. The first and last characters cannot be underscores. If it is not specified, all ERPS ring instances on the device are displayed.

<instance-id>: The ERPS ring instance ID, ranging from 1 to 48. If it is not specified, all ERPS ring instances are displayed.

Command Mode: Admin Mode.

Default: None.

Example:

Display information of all ERPS ring instances.

```
Switch#show erps instance
ERPS Ring ring1
Instance 1
Description: instance1
Protected Instance: 1
Revertive mode: non-revertive
R-APS MEL: 7
R-APS Virtual-Channel: with
Control Vlan: 10
Ring ID:
Guard Timer (csec): 100
Holdoff Timer (seconds): 0
WTR Timer (min): 6
----------------------------------------------------------------
Port        Role            Port-Status
----------------------------------------------------------------
port0       RPL Owner      Blocked
port1       Common        Forwarding
```

Output	Description
Description	ERPS ring instance name
Protected Instance	MSTP instances protected by the ERPS ring instance
Revertive mode	ERPS ring revertive mode: revertive or non-revertive
R-APS MEL	Level of the R-APS channel carried in R-APS packets
R-APS Virtual-Channel	For an ERPS sub-ring, whether there is an R-APS virtual channel: with or without
Ring ID	Ring ID carried in packets sent by the ERPS ring instance, ranging from 1 to 64
Contral Vlan	R-APS channel VLAN, used as the tag of R-APS packets
WTR_Timer	Wait-to-restore timer, ranging from 1 to 12 minutes
Guard_Timer	Guard timer, ranging from 10 ms to 2 s

Holdoff_Timer	Hold-off timer, ranging from 0 to 10 s
Port	ERPS ring port: port0 or port1
Role	ERPS ring node role: RPL Owner, RPL Neighbor, or Common
Port Status	Blocked: the port is blocked. Forwarding: the port is forwarding.

8.6.25 show erps status [ring <ring-name> [instance <instance-id>]]

Command: `show erps status [ring <ring-name> [instance <instance-id>]]`

Function: Displays the status of ERPS ring instances.

Parameters: <ring-name>: The ERPS ring name, up to 64 characters consisting of letters, digits, and underscores. The first and last characters cannot be underscores. If it is not specified, all ERPS rings on the device are displayed.

<instance-id>: The ERPS ring instance ID, ranging from 1 to 48. If it is not specified, the status of all ERPS ring instances is displayed.

Command Mode: Admin Mode.

Default: None.

Example:

Display the status of all ERPS ring instances.

```
Switch#show erps status
ERPS ring ring1 instance 1 status：
Active：1
Node State：Idle
Time last topology change : Jan 01 00:17:25 2012
------------------------------------------------------------------------------
-----------------------
Port    Interface   Port-Status     Signal-Status   R-RAPS-NodeId    BPR
------------------------------------------------------------------------------
-----------------------
Port0   1/0/1        blocked       Non-failed   00-00-00-00-00-00   0
Port1   1/0/2        forwarding    Non-failed      00-00-00-00-00-00   0
```

Active	Current active status of the ERPS ring instance: 1 or 0
Node State	Current state of the ERPS ring instance: Idle, Protection, Forced-switch, Manual-switch, or Pending
Port Status	Blocked: the port is blocked. Forwarding: the port is forwarding.
Signal Status	Fault status of the ERPS ring port: Non-failed: no fault. Failed: a fault has occurred.
Remote R-APS NodeId	Node ID (MAC address) carried in the last R-APS packet received on the ERPS ring port
BPR	Blocked port reference (BPR) carried in the last R-APS packet received on the ERPS ring port: port0 or port1, whichever is blocked
Time last topology change	Time of the last topology change

8.6.26 show erps statistics [ring <ring-name> [instance <instance-id>]]

Command: `show erps statistics [ring <ring-name> [instance <instance-id>]]`

Function: Displays ERPS ring instance statistics.

Parameters: <ring-name>: The ERPS ring name, up to 64 characters consisting of letters, digits, and underscores. The first and last characters cannot be underscores. If it is not specified, the statistics of all ERPS rings on the device are displayed.

<instance-id>: The ERPS ring instance ID, ranging from 1 to 48. If it is not specified, the statistics of all ERPS ring instances on the device are displayed.

Command Mode: Admin Mode.

Default: None.

Example:

Display ERPS ring instance statistics.

```
Switch#show erps statistics ring 1 instance 1
Statistics for ERPS ring ring1 instance 1 :
R-APS       Port0(Tx/Rx)         Port1(Tx/Rx)
--------------------------------------------------------------------------------
NR               3/0             3/0
NR,RB            0/0             0/0
SF           19129/0         19129/0
MS               0/0             0/0
FS               0/0             0/0
EVENT           0/0             0/0
--------------------------------------------------------------------------------
TOTOL       19132/0        19132/0
```

8.6.27 clear erps statistics [ring <ring-name> [instance <instance-id>]]

Command: clear erps statistics [ring <ring-name> [instance <instance-id>]]

Function: Clears ERPS statistics.

Parameters: <ring-name>: The ERPS ring name, up to 64 characters consisting of letters, digits, and underscores. The first and last characters cannot be underscores. If it is not specified, the statistics of all ERPS rings on the device are cleared.

<instance-id>: The ERPS ring instance ID, ranging from 1 to 48. If it is not specified, the statistics of all ERPS ring instances on the device are cleared.

Command Mode: Admin Mode.

Default: None.

Example: Clear the statistics of instance 1 of ERPS ring ring1.

```
Switch#clear erps statistics ring 1 instance 1
```

8.6.28 debug erps

Command: debug erps packet [detail] {send | receive] {[ring <ring-name> [instance <instance-id>]] | [port]}
debug erps fsm [ring <ring-name> [instance <instance-id>]]
debug erps timer [ring <ring-name> [instance <instance-id>]]
no debug eprs

Function: Enables ERPS debugging. The **no** form of this command disables it.

Parameters: packet: Enables packet debugging.

detail: Enables detailed packet debugging.

send: Enables debugging of sent packets.

receive: Enables debugging of received packets.

fsm: Enables state machine debugging.

timer: Enables timer debugging.

<ring-name>: The ERPS ring name, up to 64 characters consisting of letters, digits, and underscores. The first and last characters cannot be underscores.

<instance-id>: The ERPS ring instance ID, ranging from 1 to 48.

Command Mode: Admin Mode.

Default: Disabled.

8.6.29 debug erps error

Command: **`debug erps error`**
`no debug erps error`

Function: Displays ERPS error information. The **no** form of this command disables it.

Parameters: None.

Command Mode: Admin Mode.

Default: Disabled.

8.6.30 debug erps event

Command: **`debug erps event`**
`no debug erps event`

Function: Displays ERPS event information. The **no** form of this command disables it.

Parameters: None.

Command Mode: Admin Mode.

Default: Disabled.

8.6.31 no debug all

Command: **`no debug all`**

Function: Disables all debugging on the device.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: no debug all disables all debugging on the switch, including ERPS debugging.

8.6.32 show debugging

Command: **`show debugging`**

Function: Displays the debugging status of the modules.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: ERPS debugging status can also be displayed with **show debugging erps**.

Chapter 9 Commands for Debugging and Diagnosis

9.1 Monitor and Debug

9.1.1 clear history all-users

Command: `clear history all-users`

Function: Clears the command history of all users saved on the switch.

Command Mode: Admin Mode.

Usage Guidelines: Use this command to clear the command history of all users.

Example:

```
Switch#clear history all-users
```

9.1.2 history all-users max-length

Command: `history all-users max-length <count>`

Function: Sets the maximum number of command history entries of all users saved on the switch.

Parameters: <count>: The number of command history entries to save, ranging from 100 to 1000.

Command Mode: Global Mode.

Usage Guidelines: By default, the system saves up to the 100 most recent commands of all users. Use this command to change the maximum.

Example:

```
Switch(config)#history all-users max-length 500
```

9.1.3 ping

Command: `ping [[src <source-address> ] { <destination-address> | host <hostname> }]`

Function: Sends ICMP echo requests to a remote device to check whether it is reachable from the switch.

Parameters: <source-address> is the source IP address of the ping, in dotted decimal notation. **<destination-address>** is the destination IP address, in dotted decimal notation. **<hostname>** is the destination host name, up to 64 characters.

Default: Five ICMP echo requests are sent. The default packet size is 56 bytes, and the default timeout is 2 seconds.

Command Mode: Admin Mode.

Usage Guidelines: If the ping command is entered without parameters, interactive mode starts, in which the ping parameters can be entered.

Example:

Example 1: Ping with the default parameters.

```
Switch#ping 10.1.128.160
Type ^c to abort.
Sending 5 56-byte ICMP Echos to 10.1.128.160, timeout is 2 seconds.
...!!
Success rate is 40 percent (2/5), round-trip min/avg/max = 0/0/0 ms
```

In this example, the switch pings the device at 10.1.128.160. No ICMP echo reply is received for the first three requests within the default 2-second timeout, so the first three attempts fail; the last two

succeed, giving a success rate of 40%. On the switch, "." indicates a failed ping (unreachable), and "!" indicates a successful ping (reachable).

Example 2: Ping with a source address and default values for the other parameters.

```
Switch#ping src 10.1.128.161 10.1.128.160
Type ^c to abort.
Sending 5 56-byte ICMP Echos to 10.1.128.160, using source address
10.1.128.161, timeout is 2 seconds.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

In this example, 10.1.128.161 is the source address of the ICMP echo requests, and the destination device is 10.1.128.160. Replies are received for all five requests, so the success rate is 100%. On the switch, "." indicates a failed ping (unreachable), and "!" indicates a successful ping (reachable).

Example 3: Ping with parameters entered interactively.

```
Switch#ping
VRF name：
Target IP address：10.1.128.160
Use source address option[n]: y
Source IP address: 10.1.128.161
Repeat count [5]: 100
Datagram size in byte [56]：1000
Timeout in milli-seconds [2000]: 500
Extended commands [n]: n
```

Prompt	Description
VRF name	VRF name. If MPLS is not enabled, leave this field empty.
Target IP address :	IP address of the target device
Use source address option[n]	Whether to specify a source address for the ping
Source IP address	Source IP address of the ping
Repeat count [5]	Number of ping requests to send. The default is 5.
Datagram size in byte [56]	Size of the ICMP echo requests. The default is 56 bytes.
Timeout in milli-seconds [2000]:	Timeout in milliseconds. The default is 2 seconds.
Extended commands [n]:	Whether to use extended options

9.1.4 ping6

Command: ping6 [<dst-ipv6-address> | host <hostname> | src <src-ipv6-address> {<dst-ipv6-address > | host <hostname>}]

Function: Checks whether the destination network is reachable over IPv6.

Parameters: <dst-ipv6-address> is the destination IPv6 address. **<src-ipv6-address>** is the source IPv6 address of the ping. **<hostname>** is the destination host name, up to 64 characters.

Default: Five ICMPv6 echo requests are sent. The default size is 56 bytes, and the default timeout is 2 seconds.

Command Mode: User Mode.

Usage Guidelines: If ping6 is entered with only an IPv6 address, default values are used for the other parameters. If the IPv6 address is a link-local address, the VLAN interface name must be specified. If a source IPv6 address is specified, the ICMPv6 echo requests use that source address.

Example:

Example 1: Ping6 with the default parameters.

```
Switch>ping6 2001:1:2::4
Type ^c to abort.
```

```
Sending 5 56-byte ICMP Echos to 2001:1:2::4, timeout is 2 seconds.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/320/1600 ms
```

Example 2: Ping6 with a source IPv6 address.

```
switch>ping6 src 2001:1:2::3 2001:1:2::4
Type ^c to abort.
Sending 5 56-byte ICMP Echos to 2001:1:2::4, using src address 2001:1:2::3,
timeout is 2 seconds.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Example 3: Ping6 with parameters entered interactively.

```
switch>ping6
Target IPv6 address:fe80::2d0:59ff:feb8:3b27
Output Interface: vlan1
Use source address option[n]:y
Source IPv6 address: fe80::203:fff:fe0b:16e3
Repeat count [5]:
Datagram size in byte [56]:
Timeout in milli-seconds [2000]:
Extended commands [n]:
Type ^c to abort.
Sending 5 56-byte ICMP Echos to fe80::2d0:59ff:feb8:3b27, using src address
fe80::203:fff:fe0b:16e3, timeout is 2 seconds.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/16 ms
```

Prompt or output	Description
ping6	The ping6 command
Target IPv6 address	Target IPv6 address of the command
Output Interface	Name of the VLAN interface; required when the target address is a link-local address
Use source IPv6 address [n]:	Whether to use a source IPv6 address. Disabled by default.
Source IPv6 address	Source IPv6 address
Repeat count[5]	Number of ping packets
Datagram size in byte[56]	Packet size of the ping. The default is 56 bytes.
Timeout in milli-seconds[2000]	Timeout of the ping. The default is 2 seconds.
Extended commands[n]	Extended configuration. Disabled by default.
!	The network is reachable.
.	The network is unreachable.
Success rate is 100 percent(8/8), round-trip min/avg/max = 1/1/1ms	Statistics: the success rate of the ping packets is 100 percent.

9.1.5 show boot-files

Command: `show boot-files`

Function: Displays the primary and backup image files and the configuration file used for booting.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the boot order of the image files on the storage device, the image file currently used for booting, the configuration file on the storage device, and the configuration file currently used.

Example: Display the primary and backup image files and the configuration file used for booting.

```
Switch(config)#show boot-files
The primary img file at the next boot time:       mmc:/nos.img
The backup img file at the next boot time:        mmc:/nos.img
Current booted img file:                          mmc:/nos.img
Repair primary img by backup img:                 yes
The startup-config file at the next boot time:    flash:/initial.cfg
Current booted startup-config file:               flash:/vsf_startup.cfg
```

9.1.6 show debugging

Command: show debugging {bgp | dvmrp | igmp | ipv6 | mld | nsm | ospf | other | pim | rip | spanning-tree | vrrp}

Function: Displays the debugging status.

Usage Guidelines: Use **show debugging** to check which debugging functions are enabled.

Command Mode: Admin Mode.

Example: Check the enabled debugging functions.

```
Switch#show debugging ospf
OSPF debugging status:
  OSPF all IFSM debugging is on
  OSPF packet Hello detail debugging is on
  OSPF packet Database Description detail debugging is on
  OSPF packet Link State Request detail debugging is on
  OSPF packet Link State Update detail debugging is on
  OSPF packet Link State Acknowledgment detail debugging is on
  OSPF all LSA debugging is on
  OSPF all NSM debugging is on
  OSPF all events debugging is on
  OSPF all route calculation debugging is on
Switch#
```

Related Commands: **debug**

9.1.7 show fan

Command: show fan

Function: Displays the fan information of the switch.

Parameters: None.

Command Mode: All Modes.

Usage Guidelines: Checks the fan information of the switch.

Example: Display the current fan information of the switch.

```
Switch#show fan
Fan board information:
Fan No          Inserted        Status          Speed
1               NO              Abnormal        None
2               YES             Normal          Medium
3               YES             Normal          Medium
4               YES             Normal          Medium
```

9.1.8 show flash

Command: show flash

Function: Displays the files stored in the system flash memory and their sizes.

Command Mode: Admin Mode and Configuration Mode.

Example: List the files in the flash memory and their sizes.

```
Switch#show flash
boot.rom                                      329,828 1900-01-01 00:00:00 --SH
boot.conf                                          94 1900-01-01 00:00:00 --SH
nos.img                                       2,449,496 1980-01-01 00:01:06
----
startup-config                                  2,064 1980-01-01 00:30:12 ----
```

9.1.9 show history

Command: `show history`

Function: Displays the recent command history of the user.

Command Mode: Admin Mode.

Usage Guidelines: The system saves up to 20 commands entered by the user; use the Up/Down arrow keys (or Ctrl+P and Ctrl+N) to access the command history.

Example:

```
Switch#show history
enable
config
interface ethernet 1/0/3
enable
dir
show ftp
```

9.1.10 show history all-users

Command: `show history all-users [detail]`

Function: Displays the recent command history of all users.

Parameters: detail: Also displays the user name of each command; for commands entered through Telnet or SSH, the IP address of the user is also displayed.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the recent command history of all users, including the time, login type, and command.

Note: A user can view only the command history of users whose privilege level is not higher than the user's own.

Example:

```
Switch(config)#show history all-users detail
Time          Type        User       Command
0w 0d 0h 2m   Telnet/SSH  admin      show history all-users detail
192.168.1.2:1419
0w 0d 0h 1m   Telnet/SSH  admin      show history all-users 192.168.1.2:1419
0w 0d 0h 1m   Console     Null        show history all-users
0w 0d 0h 1m   Console     Null        end
0w 0d 0h 1m   Console     Null        ip address 192.168.1.1 255.255.255.0
0w 0d 0h 0m   Console     Null        in v 1
0w 0d 0h 0m   Console     Null        telnet-server enable
```

9.1.11 show memory usage

Command: `show memory [usage]`

Function: Displays the contents of memory.

Parameters: usage: Displays memory usage information.

Command Mode: Admin Mode.

Usage Guidelines: This command is used for switch debugging. It prompts the user for the start address in memory and the number of words to display. The output consists of three parts: the address, a hexadecimal view, and a character view.

Example:

```
Switch#show memory
start address : 0x2100
number of words[64]:
002100:  0000 0000 0000 0000  0000 0000 0000 0000   *................*
002110:  0000 0000 0000 0000  0000 0000 0000 0000   *................*
002120:  0000 0000 0000 0000  0000 0000 0000 0000   *................*
002130:  0000 0000 0000 0000  0000 0000 0000 0000   *................*
002140:  0000 0000 0000 0000  0000 0000 0000 0000   *................*
002150:  0000 0000 0000 0000  0000 0000 0000 0000   *................*
002160:  0000 0000 0000 0000  0000 0000 0000 0000   *................*
002170:  0000 0000 0000 0000  0000 0000 0000 0000   *................*
```

9.1.12 show running-config

Command: `show running-config`

Function: Displays the current active configuration of the switch.

Default: If the active configuration is the same as the default configuration, nothing is displayed.

Command Mode: Admin Mode.

Usage Guidelines: After completing a set of configuration changes, use **show running-config** to verify the current active configuration.

Example:

```
Switch#show running-config
```

9.1.13 show running-config current-mode

Command: `show running-config current-mode`

Function: Displays the configuration of the current mode.

Command Mode: All Configuration Modes.

Default: None.

Usage Guidelines: Enter this command in any configuration mode to display all configuration in that mode.

Example:

```
 Switch(config-if-ethernet1/0/1)#show run c
!
Interface Ethernet1/0/1
switchport access vlan 2
!
```

9.1.14 show startup-config

Command: `show startup-config`

Function: Displays the configuration saved in flash memory, which is normally the configuration used at the next startup.

Default: If the configuration read from flash memory is the same as the default configuration, nothing is displayed.

Command Mode: Admin Mode.

Usage Guidelines: After a set of configuration changes, **show running-config** displays the new configuration, but **show startup-config** does not. After the active configuration is saved to flash

memory with the **write** command, **show running-config** and **show startup-config** display the same configuration.

9.1.15 show switchport interface

Command: show switchport interface [ethernet <IFNAME>]

Function: Displays the VLAN mode, VLAN ID, and trunk information of switch ports.

Parameters: <IFNAME> is the port number.

Command Mode: Admin Mode.

Example: Display the VLAN information of port Ethernet 1/0/1.

```
Switch#show switchport interface ethernet 1/0/1
Ethernet1/0/1
Type :Universal
Mac addr num : No limit
Mode :Trunk
Port VID :1
Trunk allowed Vlan :ALL
```

Output	Description
Ethernet1/0/1	Ethernet interface number
Type	Current interface type
Mac addr num	Number of MAC addresses the interface can learn
Mode: Trunk	Current VLAN mode of the interface
Port VID :1	VLAN to which the interface belongs (PVID)
Trunk allowed Vlan :ALL	VLANs allowed on the trunk

9.1.16 show tcp

Command: show tcp

Function: Displays the current TCP connections to the switch.

Command Mode: Admin Mode.

Example:

```
Switch#show tcp
LocalAddress     LocalPort  ForeignAddress   ForeignPort     State
0.0.0.0           23        0.0.0.0          0              LISTEN
0.0.0.0           80        0.0.0.0          0              LISTEN
```

Output	Description
LocalAddress	Local address of the TCP connection
LocalPort	Local port number of the TCP connection
ForeignAddress	Remote address of the TCP connection
ForeignPort	Remote port number of the TCP connection
State	Current state of the TCP connection

9.1.17 show tcp ipv6

Command: show tcp ipv6

Function: Displays the current IPv6 TCP connections.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch#show tcp ipv6
LocalAddress                LocalPort  RemoteAddress        RemotePort  State
IF  VRF
```

```
::                          80          ::                  0           LISTEN
0   0
::                          23          ::                  0           LISTEN
0   0
```

Output	Description
LocalAddress	Local IPv6 address of the TCP connection
LocalPort	Local port of the TCP connection
RemoteAddress	Remote IPv6 address of the TCP connection
RemotePort	Remote port of the TCP connection
State	Current state of the TCP connection
IF	Index of the local interface of the TCP connection
VRF	VRF (virtual routing and forwarding instance)

9.1.18 show telnet login

Command: `show telnet login`

Function: Lists the Telnet clients currently connected to the switch.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Lists information about the Telnet clients currently connected to the switch.

Example:

```
Switch#show telnet login
Authenticate login by local.
Login user:
aa
```

9.1.19 show temperature

Command: `show temperature`

Function: Displays the current CPU temperature of the switch.

Parameters: None.

Command Mode: All Modes.

Usage Guidelines: Use this command to monitor the CPU temperature of the switch.

Example: Display the current CPU temperature of the switch.

```
Switch(Config)#show temperature
Temperature: 47.0625 ℃
```

9.1.20 show tech-support

Command: `show tech-support`

Function: Displays various information about the switch and its running tasks, for diagnosis by technical support.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: When a failure occurs on the switch, use this command to collect related information for diagnosis.

Example:

```
Switch#show tech-support
```

9.1.21 show udp

Command: show udp

Function: Displays the current UDP connections to the switch.

Command Mode: Admin Mode.

Example:

```
Switch#show udp
LocalAddress     LocalPort  ForeignAddress   ForeignPort     State
0.0.0.0          161        0.0.0.0          0               CLOSED
0.0.0.0          123        0.0.0.0          0               CLOSED
0.0.0.0          1985       0.0.0.0          0               CLOSED
```

Output	Description
LocalAddress	Local address of the UDP connection
LocalPort	Local port number of the UDP connection
ForeignAddress	Remote address of the UDP connection
ForeignPort	Remote port number of the UDP connection
State	Current state of the UDP connection

9.1.22 show udp ipv6

Command: show udp ipv6

Function: Displays the current IPv6 UDP connections.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
LocalAddress                LocalPort  RemoteAddress      RemotePort  State
::                          69         ::                 0           CLOSED
::                          1208       ::                 0           CLOSED
```

Output	Description
LocalAddress	Local IPv6 address of the UDP connection
LocalPort	Local port of the UDP connection
RemoteAddress	Remote IPv6 address of the UDP connection
RemotePort	Remote port of the UDP connection
State	Current state of the UDP connection

9.1.23 show version

Command: show version

Function: Displays the version information of the switch.

Command Mode: Admin Mode.

Usage Guidelines: Use this command to view the version information of the switch, including the hardware and software versions.

Example:

```
Switch#show version
```

9.1.24 traceroute

Command: traceroute [source <ipv4-addr>] vrf <vrfname> { <ip-addr> | host <hostname> |[ethernet target-mac <mac-address>| target-mep <1-4094> domain WORD server (WORD) (number <0-65535>) |(pvlan <1-4094 >) fdb-only|source|ttl] } [hops <hops>] [timeout <timeout>]

Function: Traces the gateways that packets pass through from the source device to the destination device. Use this command to test connectivity and locate a failed network segment.

Parameters: <ipv4-addr> is the source host IPv4 address, in dotted decimal notation. **<ip-addr>** is the destination host IP address, in dotted decimal notation. **<hostname>** is the host name of the remote host. **<hops>** is the maximum number of gateways that traceroute can pass through. **<timeout>** is the timeout of the test packets in milliseconds, ranging from 100 to 10000. **<vrfname>** is the VRF instance name.

Default: The maximum number of gateways is 30, and the timeout is 2000 ms.

Command Mode: Admin Mode.

Usage Guidelines: Traceroute is typically used to locate problems with unreachable network nodes.

9.1.25 traceroute6

Command: `traceroute6 [source <addr>] {<ipv6-addr> | host <hostname>} [hops <hops>] [timeout <timeout>]`

Function: Traces the gateways that packets pass through from the source device to the destination device over IPv6. Use this command to check network reachability and locate network failures.

Parameters: <addr> is the source host IPv6 address, in colon-hexadecimal notation. **<ipv6-addr>** is the IPv6 address of the destination host, in colon-hexadecimal notation. **<hostname>** is the name of the remote host. **<hops>** is the maximum number of gateways that traceroute6 can pass through, ranging from 1 to 255. **<timeout>** is the timeout of the packets in milliseconds, ranging from 100 to 10000.

Default: The maximum number of gateways is 30, and the timeout is 2000 ms.

Command Mode: Admin Mode.

Usage Guidelines: Traceroute6 is typically used to locate failures when a destination network is unreachable.

Example:

```
Switch# traceroute6 2004:1:2:3::4
```

Related Commands: ipv6 host

9.2 Logging

9.2.1 logging executed-commands

Command: `logging executed-commands {enable | disable}`

Function: Enables or disables logging of executed commands.

Parameters: None.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: When this function is enabled, commands executed by users from the console, Telnet, or SSH terminals are logged.

Example: Enable logging of executed commands.

```
Switch(Config)#logging executed-commands enable
```

9.2.2 show logging executed-commands state

Command: `show logging executed-commands state`

Function: Displays the state of executed-command logging.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Use this command to display whether executed-command logging is enabled or disabled.

Example:

```
Switch#show logging executed-commands state
Logging executed command state is enable
```

9.3 Reload Switch after Specified Time

9.3.1 reload after

Command: `reload after {[<HH:MM:SS>] [days <days>]}`

Function: Reloads the switch after a specified period of time.

Parameters: <HH:MM:SS> is the time to wait; HH (hours) ranges from 0 to 23, and MM (minutes) and SS (seconds) range from 0 to 59.

<days> is the number of days to wait, ranging from 1 to 30.

The time and days can be configured together or separately.

Command Mode: Admin Mode.

Usage Guidelines: Use this command to reboot the switch after a specified period of time without powering it off, typically when updating the switch software. The switch can then reboot at a later time instead of immediately after the update. This command is not saved in the configuration and takes effect only once. After this command is configured, users who log in to the switch through Telnet are prompted with the reboot information.

Example: Set the switch to reload automatically after 2 days, 10 hours, and 1 second.

```
Switch#reload after 10:00:01 days 2
Process with reboot after? [Y/N] y
```

Related Commands: reload, reload cancel, show reload

9.3.2 reload cancel

Command: `reload cancel`

Function: Cancels a scheduled reload of the switch.

Parameters: None.

Command Mode: Admin Mode.

Usage Guidelines: Use this command to cancel a reload scheduled with the **reload after** command. This command is not saved in the configuration.

Example: Cancel the scheduled reload of the switch.

```
Switch#reload cancel
Reload cancel successful.
```

Related Commands: reload, reload after, show reload

9.3.3 show reload

Command: `show reload`

Function: Displays the reload schedule configured with the **reload after** command.

Parameters: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Use this command to view the reload schedule configured with **reload after** and the time remaining before the switch reboots.

Example: Display the reload schedule. In this example, the switch is set to reboot after 10 hours and 1 second, and 9 hours, 59 minutes, and 48 seconds remain before it reboots.

```
Switch#show reload
 The original reload after configuration is 10:00:01.
 System will be rebooted after 09:59:48 from now.
```

Related Commands: reload, reload after, reload cancel

9.4 Debugging and Diagnosis for Packets Received and Sent by CPU

9.4.1 clear cpu-rx-stat protocol

Command: `clear cpu-rx-stat protocol[ <protocol-type> ]`

Function: Clears the statistics of packets of the specified protocol type received by the CPU.

Parameters: <protocol-type> is the protocol type of the packets, including dot1x, stp, snmp, arp, telnet, http, dhcp, igmp, ssh, bgp, bgp4plus, rip, ripng, ospf, ospfv3, pim, pimv6, unknown-mcast, unknown-mcast6, and mld.

Command Mode: Global Mode.

Usage Guidelines: This command clears the statistics of packets of the specified protocol type received by the CPU. Use it only with the help of technical support.

Example: Clear the statistics of ARP packets received by the CPU.

```
Switch#clear cpu-rx-stat protocol arp
```

9.4.2 cpu-rx-limitnotify enable interval

Command: `cpu-rx-limitnotify enable interval<180-86400>`
`no cpu-rx-limitnotify enable`

Function: Enables the CPU receive limit notification function and sets the notification interval. The **no** form of this command disables the function.

Parameters: interval: The notification interval in seconds, ranging from 180 to 86400. The default is 86400 seconds.

Command Mode: Global Mode.

Usage Guidelines: This command is used to diagnose protocol packets received by the switch. Use it only under the guidance of the manufacturer's technical support.

Example:

```
Switch(config)#cpu-rx-limitnotify enable interval 180
```

9.4.3 cpu-rx-limitnotify protocol (all|WORD)(enable|disable)

Command: `cpu-rx-limitnotify protocol (all|WORD)(enable|disable)`

Function: Enables or disables the notification for all protocols or a specified protocol. When enabled, if packets received by the CPU are denied during the interval, the switch sends the number of denied packets in that interval to users through an SNMP trap.

Command Mode: Global Mode.

Example:

Disable all protocols:

```
Switch(config)# cpu-rx-limitnotify protocol all disable
```

Enable all protocols:

```
Switch(config)# cpu-rx-limitnotify protocol all enable
```

Enable a specified protocol:

```
Switch(config)# cpu-rx-limitnotify protocol snmp enable
```

Disable a specified protocol:

```
Switch(config)# cpu-rx-limitnotify protocol snmp disable
```

9.4.4 cpu-rx-ratelimit enhanced

Command: `cpu-rx-ratelimit enhanced`
`no cpu-rx-ratelimit enhanced`

Function: Enables enhanced rate limiting for packets received by the CPU. The **no** form of this command disables it.

Parameters: None.

Command Mode: Global Mode.

Usage Guidelines: This command restricts the protocol packets received by the switch. Use it only under the guidance of the manufacturer's technical support.

Example: Enable enhanced rate limiting for packets received by the CPU.

```
Switch(config)#cpu-rx-ratelimit enhanced
```

9.4.5 cpu-rx-ratelimit protocol

Command: `cpu-rx-ratelimit protocol <protocol-type> <packets>`
`no cpu-rx-ratelimit protocol <protocol-type>`

Function: Sets the maximum rate at which the CPU receives packets of the specified protocol type. The **no** form of this command restores the default rate.

Parameters: <protocol-type> is the protocol type, including dot1x, stp, snmp, arp, telnet, http, dhcp, igmp, and ssh. **<packets>** is the maximum rate at which the CPU receives packets of that protocol type, ranging from 1 to 2000 pps.

Command Mode: Global Mode.

Default: The default rate differs by protocol type.

Usage Guidelines: The rate limit set by this command affects the packets received by the CPU. Use it only with the help of technical support.

Example: Set the rate of ARP packets to 500 pps.

```
Switch(config)#cpu-rx-ratelimit protocol arp 500
```

9.4.6 cpu-rx-ratelimit total

Command: `cpu-rx-ratelimit total <packets>`
`no cpu-rx-ratelimit total`

Function: Sets the total rate at which the CPU receives packets. The **no** form of this command restores the default total rate.

Parameters: <packets> is the maximum number of packets the CPU receives per second.

Command Mode: Global Mode.

Default: 1200 pps.

Usage Guidelines: The total rate set by this command affects the packets received by the CPU. Use it only with the help of technical support.

Example: Set the total rate of packets received by the CPU to 1500 pps.

```
Switch(config)#cpu-rx-ratelimit total 1500
```

9.4.7 debug driver

Command: debug driver {receive | send} [interface {<interface-name> | all}] [protocol {<protocol-type> | discard | all}] [detail]
no debug driver {receive | send}

Function: Enables display of information about packets received or sent by the CPU. The **no debug driver {receive | send}** command disables it.

Parameters: receive | send: Displays information about received or sent packets.

interface {<interface-list> | all}: **<interface-list>** is the Ethernet port number; **all** specifies all Ethernet ports.

protocol {<protocol-type> | discard | all}: **<protocol-type>** is the protocol type of the packets, including snmp, telnet, http, dhcp, igmp, hsrp, arp, bgp, rip, ospf, pim, ssh, vrrp, ripng, ospfv3, pimv6, icmpv6, bgp4plus, unknown-mcast, unknown-mcast6, ttl0-2cpu, isis, dot1x, gvrp, stp, lacp, cluster, mld, vrrpv3, ra, uldp, lldp, and eapou; **all** specifies all protocol types; **discard** specifies all discarded packets. **detail** displays detailed information.

Command Mode: Admin Mode.

Usage Guidelines: This command is used for debugging. Use it only with the help of technical support.

Example: Enable display of packets received by the CPU.

```
Switch#debug driver receive
```

9.4.8 protocol filter

Command: protocol filter {protocol-type}
no Protocol filter {protocol-type}

Function: Enables or disables processing of packets of the specified protocol.

Parameters: <protocol-type> is the protocol type: {arp|bgp|dhcp|dhcpv6|hsrp|http|igmp|ip|ldp|mpls|ospf|pim|rip|snmp|telnet|vrrp}.

Command Mode: Admin Mode.

Usage Guidelines: This command enables or disables processing of packets of the specified protocol and is used to debug and diagnose the switch. Use it only under the guidance of the manufacturer's technical support.

Example: Enable processing of ARP packets.

```
Switch#protocol filter arp
```

9.4.9 show cpu-rx protocol

Command: show cpu-rx protocol [<protocol-type>]

Function: Displays the statistics of packets of the specified protocol type received by the CPU.

Parameters: <protocol-type> is the protocol type of the packets. If no protocol type is specified, statistics for all packets are displayed.

Command Mode: Admin Mode and Configuration Mode.

Default: None.

Usage Guidelines: This command is used for debugging. Use it only with the help of technical support.

Example: Display the statistics of ARP packets received by the CPU.

```
Switch#show cpu-rx protocol arp
Type                Rate-limit    TotPkts        CurState
arp                 500           3              allowed
```

9.5 CPU-Protect

9.5.1 cpu-protect enable

Command: **`cpu-protect enable`**
`no cpu-protect enable`

Function: Enables the CPU protection function on the switch. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Use **cpu-protect enable** to enable the CPU protection function, and the **no** form to disable it.

Example: Enable the CPU protection function.

```
Switch(Config)# cpu-protect enable
```

9.5.2 cpu-protect log enable

Command: **`cpu-protect log enable`**
`no cpu-protect log enable`

Function: Enables CPU protection logging on the switch. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Use **cpu-protect log enable** to enable CPU protection logging, and the **no** form to disable it.

Example: Enable CPU protection logging.

```
Switch(Config)#cpu-protect log enable
```

9.5.3 cpu-protect trap enable

Command: **`cpu-protect trap enable`**
`no cpu-protect trap enable`

Function: Enables CPU protection trap alarms on the switch. The **no** form of this command disables them.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Use **cpu-protect trap enable** to enable CPU protection trap alarms, and the **no** form to disable them.

Example: Enable CPU protection trap alarms.

```
Switch(Config)# cpu-protect trap enable
```

9.5.4 cpu-protect interval

Command: `cpu-protect interval <time>`
`no cpu-protect interval`

Function: Sets the CPU protection sampling interval.

Parameters: <time> is the sampling interval, ranging from 1 to 10 seconds.

Default: 3 seconds.

Command Mode: Global Mode.

Usage Guidelines: Use **cpu-protect interval** to set the CPU protection sampling interval, and the **no** form to restore the default.

Example: Set the CPU protection sampling interval to 5 seconds.

```
Switch(Config)# cpu-protect interval 5
```

9.5.5 cpu-protect recovery-time

Command: `cpu-protect recovery-time <time>`
`no cpu-protect recovery-time`

Function: Sets the CPU protection policy recovery time.

Parameters: <time> is the recovery time, ranging from 1 to 3000 seconds.

Default: 60 seconds.

Command Mode: Global Mode.

Usage Guidelines: Use **cpu-protect recovery-time** to set the CPU protection policy recovery time, and the **no** form to restore the default.

Example: Set the CPU protection policy recovery time to 100 seconds.

```
Switch(config)#cpu-protect recovery-time 100
```

9.5.6 cpu-protect threshold

Command: `cpu-protect (protocol <WORD>|per-ip|per-mac) threshold <pps>`
`action (none|speed-limit)`
`no cpu-protect (protocol <WORD>|per-ip|per-mac) threshold`

Function: Sets the upper limit of the rate at which a stream (protocol type, IP address, or MAC address) is sent to the CPU.

Parameters: <WORD> is the protocol type. Supported protocol types are ARP, IP, ICMP, IGMP, and DHCP.

<pps> is the upper limit of the rate at which packets are sent to the CPU, in packets per second. See the Range column in the following table.

none: When the limit is exceeded, no rate limiting is applied; the switch only logs the event, sends a trap alarm, and records the attack source list. **speed-limit**: When the limit is exceeded, the switch applies rate limiting, logs the event, sends a trap alarm, and records the attack source list.

Default: See the Default column in the following table, in packets per second. The default action when the limit is exceeded is speed-limit.

Protocol	Default	Range
ARP	300	10/20～800
IP	300	10/20～800
ICMP	80	10/20～800
IGMP	150	10/20～800
DHCP	150	10/20～800
Specific host (IP)	400	10/20～800

Specific host (MAC)	400	10/20～800

Command Mode: Global Mode.

Usage Guidelines: Use **cpu-protect threshold** to set the upper limit of the rate at which a stream is sent to the CPU, and the **no** form to restore the default.

Example: Set the upper limit for ARP packets sent to the CPU to 500 pps, with no rate-limiting action when the limit is exceeded.

```
Switch(Config)# cpu-protect protocal arp threshold 500 action none
```

9.5.7 cpu-protect limit-speed

Command: cpu-protect (protocol <WORD>|per-ip|per-mac) limit-speed <pps>
no cpu-protect (protocol <WORD>|per-ip|per-mac) limit-speed

Function: Sets the rate limit applied to a stream (protocol type, IP address, or MAC address) sent to the CPU after the upper limit is exceeded.

Parameters: <WORD> is the protocol type. Supported protocol types are ARP, IP, ICMP, IGMP, and DHCP.

<pps> is the rate limit applied after the upper limit is exceeded, in packets per second. See the Range column in the following table.

Default: See the Default column in the following table, in packets per second.

Protocol	Default	Range
ARP	150/200	10/20～250
IP	150/200	10/20～250
ICMP	50/50	10/20～250
IGMP	80/100	10/20～250
DHCP	80/100	10/20～250
Specific host (IP)	200/250	10/20～300
Specific host (MAC)	200/250	10/20～300

Command Mode: Global Mode.

Usage Guidelines: Use **cpu-protect limit-speed** to set the rate limit applied after the upper limit is exceeded, and the **no** form to restore the default.

Example: Set the rate limit for ARP packets sent to the CPU to 100 pps after the upper limit is exceeded.

```
Switch(config)#cpu-protect protocal arp limit-speed 100
```

9.5.8 show cpu-protect attack-list

Command: show cpu-protect attack-list (detail|top)

Function: Displays the attack sources detected by the CPU protection module.

Parameters: detail displays all entries in the attack source table; **top** displays only the top 10 entries.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the attack sources detected by the CPU protection module.

Example: Display the top 10 entries in the attack source table.

```
Switch# show cpu-protect attack-list top
Attack Num Total:                1
Type       Item-Info   AttackTimes   Port        VLAN-LIST  Speed  State
Protocal    ARP       5          Ethernet1/0/1    1         64      Speed-
Limit
```

9.5.9 show cpu-protect running-config

Command: show cpu-protect running-config

Function: Displays the configuration and operating information of the CPU protection module.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the configuration and operating information of the CPU protection module.

Example: Display the configuration and operating information of the CPU protection module.

```
Switch# show cpu-protect running-config
Cpu-Protect Globle:          enable
Cpu-Protect trap :           enable
Cpu-Protect Log:             enable
Cpu-Protect Interval:        3
Cpu-Protect Recovery-Time:   60
Cap-Num   Ip-Num   Mac-Num   Protocal-Num
 0          0        0           0
Stream         Threshould     Limit-Speed    Action
IP              300            150           Speed-Limit
DHCP           150            80            Speed-Limit
IGMP           150             80            Speed-Limit
ARP            300             150           Speed-Limit
ICMP           80              50            Speed-Limit
PER-IP         400             200           Speed-Limit
PER-MAC       400             200          Speed-Limit
```

9.6 Info-Center

9.6.1 info-center enable

Command: info-center enable
no info-center enable

Function: Enables information center output.

Parameters: None.

Command Mode: Global Mode.

Default: Enabled.

Usage Guidelines: This command enables information center output. The information center can be configured whether or not output is enabled; this command only controls whether the information center outputs information. When output is disabled, the existing configuration remains and takes effect again when output is re-enabled.

Example:

```
Switch(config)#info-center enable
Switch(config)#no info-center enable
```

9.6.2 info-center prefix

Command: info-center (console | logbuffer | monitor | trapbuffer) prefix (on|off)
info-center (logfile <1-4> | loghost <1-8>) prefix (on|off) (member <1-16> |)

Function: Configures whether log records carry a prefix.

Parameters:

Parameter	Description
console | logbuffer | monitor | logfile <1-4> | loghost <1-8> | trapbuffer	The output direction to configure
on|off	Turns the log record prefix on or off
member <1-16>	Member ID

Command Mode: Global Mode.

Default: Enabled.

Usage Guidelines: This command turns the log record prefix on or off for each output direction. By default, the prefix is on for all directions.

Example:

```
Switch(config)# info-center console prefix on
```

9.6.3 info-center match

Command: info-center (console | logbuffer | monitor | trapbuffer) match level (emergencies | alerts | critical | errors | warnings | notifications | informational | debugging) (exact |) (keyword WORD |)
info-center (logfile <1-4> | loghost <1-8>) match level (emergencies | alerts | critical | errors | warnings | notifications | informational | debugging) (exact) (keyword WORD |) (member <1-16> |)
no info-center (console | logbuffer | monitor | trapbuffer) match
no info-center (logfile <1-4> | loghost <1-8>) match (member <1-16>)

Function: Configures the log matching conditions for an output direction.

Parameters:

Parameter	Description
console | logbuffer | monitor | logfile <1-4> | loghost <1-8> | trapbuffer	The output direction to configure
emergencies | alerts | critical | errors | warnings | notifications | informational | debugging	The severity level to match
exact	Strict level matching
keyword WORD	Regular expression used to filter logs
member <1-16>	Member ID

Command Mode: Global Mode.

Default: Enabled.

Usage Guidelines: This command sets the log matching conditions for each output direction. After **match**, specify the level of logs allowed in; exact level matching can also be specified. With **exact**, only logs of the specified level are matched. Without **exact**, levels are matched in the order emergencies, alerts, critical, errors, warnings, notifications, informational, and debugging. A regular expression can also be specified after **keyword**.

The **no** form of this command removes the matching conditions for the corresponding output direction.

Example:

```
Sysname(config)#info-center console match level warnings exact
Sysname(config)#info-center logfile 1 match level errors
```

9.6.4 info-center output-enable

Command: info-center (console | logbuffer | monitor | trapbuffer) match level (emergencies | alerts | critical | errors | warnings | notifications | informational | debugging) (exact |) (keyword WORD |)
info-center (logfile <1-4> | loghost <1-8>) match level (emergencies | alerts | critical | errors | warnings | notifications | informational | debugging) (exact) (keyword WORD |) (member <1-16> |)
no info-center (console | logbuffer | monitor | trapbuffer) match
no info-center (logfile <1-4> | loghost <1-8>) match (member <1-16>)

Function: Enables an output direction.

Parameters:

Parameter	Description
console | logbuffer | monitor | logfile <1-4> | loghost <1-8> | trapbuffer	The output direction to configure
member <1-16>	Member ID

Command Mode: Global Mode.

Default: Enabled.

Usage Guidelines: This command enables an output direction. It only enables or disables the direction and does not affect the matching conditions or other configuration. When the direction is enabled again, the previous configuration remains valid.

Note: console, monitor, logbuffer, trapbuffer, and logfile 4 are enabled by default; the other directions are disabled by default. logfile 4 is the default logfile output direction, so it is enabled by default.

Example:

```
Sysname(config)#info-center monitor output-enable
Sysname(config)#info-center logfile 1 output-enable
```

9.6.5 info-center record-cmd

Command: info-center (logbuffer | logfile <1-4> | loghost <1-8>) record-cmd
no info-center (logbuffer | logfile <1-4> | loghost <1-8>) record-cmd

Function: Logs the commands executed by users.

Parameters:

Parameter	Description
logbuffer | logfile <1-4> | loghost <1-8>	The output direction to configure

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: This command records the commands executed by users to the specified output direction. Command recording is not subject to the matching conditions of that direction; commands are recorded as long as the output direction is enabled. By default, user commands are not logged.

Example:

```
Sysname(config)#info-center logbuffer record-cmd
```

9.6.6 info-center loghost

Command: `info-center loghost <1-8> config (vrf <vrfname>|A.B.C.D | X:X::X:X) facility (local0|local1|local2|local3|local4|local5| local6|local7) (member <1-16> |)`
`no info-center loghost <1-8> config (member <1-16> |)`

Function: Configures the IP address and facility of a log host.

Parameters:

Parameter	Description
loghost <1-8>	The loghost output direction to configure
A.B.C.D | X:X::X:X	IP address of the log host
local0|local1|local2|local3| local4|local5|local6|local7	Facility, local0 to local7
member <1-16>	Member ID
<vrfname>	VRF instance name

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: This command configures the IP address and facility of a log host.

The **no** form of this command removes the IP address and facility configuration of the log host. In VSF mode, add **member** at the end of the command.

Example:

```
Sysname(config)#info-center loghost 1 config 192.168.1.1 facility local0
```

9.6.7 info-center logfile

Command: `info-center logfile <1-4> config count <1-40960> (flash|usb|mmc) WORD (member <1-16> |)`
`no info-center logfile <1-4> config (member <1-16> |)`

Function: Configures the number of log files and the storage path.

Parameters:

Parameter	Description
logfile <1-4>	The logfile output direction to configure
count <1-40960>	Number of log files
flash|usb|mmc	Storage location
WORD	Log file name
member <1-16>	Member ID

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: This command configures the number of log files and the storage path. The system uses logfile 4 as the default logfile output direction. If an MMC device is present, the default storage path is MMC; otherwise, it is flash. With the default configuration, the logs of a card from before a power failure can therefore still be viewed from the master card with **show info-center logfile** after the card restarts. In VSF mode, add **member** at the end of the command.

The **no** form of this command removes the logfile count and storage path configuration.

Example:

```
Sysname(config)#info-center logfile 1 config count 40960 flash logfile.log
```

9.6.8 info-center clear

Command: `info-center clear trapbuffer`
`info-center clear logbuffer (member <1-16> |)`

Function: Deletes all logs recorded in the logbuffer or trapbuffer of the information center.

Parameters:

Parameter	Description
logbuffer|trapbuffer	Output direction to clear
member <1-16>	Member ID

Command Mode: Global Mode.

Default: None.

Usage Guidelines: This command deletes all logs recorded in the logbuffer or trapbuffer of the information center.

Example:

```
Sysname(config)#info-center clear logbuffer
Sysname(config)#info-center clear trapbuffer
```

9.6.9 show info-center config

Command: `show info-center config`

Function: Displays the current configuration of the information center.

Parameters: None.

Command Mode: All Modes.

Default: None.

Usage Guidelines: This command displays the current configuration of the information center.

Example:

```
SW1(config)#show info-center config
info-center enable
info-center sync enable
info-center console output-enable
info-center monitor output-enable
info-center trapbuffer output-enable
info-center logbuffer output-enable
info-center logfile 4 config count 40960 mmc logfile.log
info-center logfile 4 output-enable
info-center console match level warnings
info-center console prefix on
info-center monitor match level debugging
info-center monitor prefix on
info-center trapbuffer prefix on
info-center logbuffer match level warnings
info-center logbuffer prefix on
info-center loghost 1 prefix on
info-center loghost 2 prefix on
info-center loghost 3 prefix on
info-center loghost 4 prefix on
info-center loghost 5 prefix on
info-center loghost 6 prefix on
info-center loghost 7 prefix on
info-center loghost 8 prefix on
```

```
info-center logfile 1 prefix on
info-center logfile 2 prefix on
info-center logfile 3 prefix on
info-center logfile 4 match level warnings
info-center logfile 4 prefix on
```

9.6.10 show info-center logbuffer

Command: show info-center logbuffer ((keyword WORD)|) (member <1-16> |)

Function: Displays the contents of the logbuffer output direction.

Parameters:

Parameter	Description
keyword WORD	Regular expression used to filter logs
member <1-16>	Member ID

Command Mode: All Modes.

Default: None.

Usage Guidelines: This command displays the contents of the logbuffer output direction. The output can be filtered with a regular expression.

Note: There is no separate command for displaying user commands. All user commands are logged with the string "CMD:", which can be used as a filter keyword. In VSF mode, add **member** at the end of the command.

Example:

```
Sysname(config)#show info-center logbuffer
severity: 1-emergencies 2-alerts 3-critical 4-errors 5-warnings 6-
notifications 7-informational 8-debugging
Allowed max messages:2000,Current messages:51
51 Jan 25 11:43:21:000 2019 Switch DEFAULT/5/:%LINEPROTO-5-UPDOWN: Line
protocol on Interface Vlan1,changed state to UP
50 Jan 25 11:43:20:000 2019 Switch MODULE_PORT/5/:%LINEPROTO-5-UPDOWN: Line
protocol on Interface Ethernet1/0/1, changed state to UP
49 Jan 25 11:43:07:000 2019 Switch DEFAULT/5/:%LINEPROTO-5-UPDOWN: Line
protocol on Interface Vlan1,changed state to DOWN
48 Jan 25 11:43:06:000 2019 Switch MODULE_PORT/5/:%LINEPROTO-5-UPDOWN: Line
protocol on Interface Ethernet1/0/1, changed state to DOWN
47 Jan 25 11:38:22:000 2019 Switch DEFAULT/5/:%LINEPROTO-5-UPDOWN: Line
protocol on Interface Vlan1,changed state to UP
46 Jan 25 11:38:21:000 2019 Switch MODULE_PORT/5/:%LINEPROTO-5-UPDOWN: Line
protocol on Interface Ethernet1/0/1, changed state to UP
45 Jan 25 11:38:08:000 2019 Switch DEFAULT/5/:%LINEPROTO-5-UPDOWN: Line
protocol on Interface Vlan1,changed state to DOWN
44 Jan 25 11:38:07:000 2019 Switch MODULE_PORT/5/:%LINEPROTO-5-UPDOWN: Line
protocol on Interface Ethernet1/0/1, changed state to DOWN
43 Jan 25 11:29:33:000 2019 Switch DEFAULT/2/:System cold restart...
42 Jan 25 11:28:36:000 2019 Switch DEFAULT/5/:%LINEPROTO-5-UPDOWN: Line
protocol on Interface Vlan1,changed state to UP
...
----finish show log buffer----
```

9.6.11 show info-center trapbuffer

Command: show info-center trapbuffer

Function: Displays the contents of the trapbuffer output direction.

Parameters:

Parameter	Description

keyword WORD	Regular expression used to filter logs

Command Mode: All Modes.

Default: None.

Usage Guidelines: This command displays the contents of the trapbuffer output direction. The output can be filtered with a regular expression.

Example:

```
Sysname(config)#show info-center trapbuffer
severity: 1-emergencies 2-alerts 3-critical 4-errors 5-warnings 6-
notifications 7-informational 8-debugging
Allowed max messages:2000,Current messages:44
44 Jan 25 11:43:21:000 2019 Switch DEFAULT/5/:%LINEPROTO-5-UPDOWN: Line
protocol on Interface Vlan1,changed state to UP
43 Jan 25 11:43:20:000 2019 Switch MODULE_PORT/5/:%LINEPROTO-5-UPDOWN: Line
protocol on Interface Ethernet1/0/1, changed state to UP
42 Jan 25 11:43:07:000 2019 Switch DEFAULT/5/:%LINEPROTO-5-UPDOWN: Line
protocol on Interface Vlan1,changed state to DOWN
41 Jan 25 11:43:06:000 2019 Switch MODULE_PORT/5/:%LINEPROTO-5-UPDOWN: Line
protocol on Interface Ethernet1/0/1, changed state to DOWN
40 Jan 25 11:38:22:000 2019 Switch DEFAULT/5/:%LINEPROTO-5-UPDOWN: Line
protocol on Interface Vlan1,changed state to UP
39 Jan 25 11:38:21:000 2019 Switch MODULE_PORT/5/:%LINEPROTO-5-UPDOWN: Line
protocol on Interface Ethernet1/0/1, changed state to UP
38 Jan 25 11:38:08:000 2019 Switch DEFAULT/5/:%LINEPROTO-5-UPDOWN: Line
protocol on Interface Vlan1,changed state to DOWN
37 Jan 25 11:38:07:000 2019 Switch MODULE_PORT/5/:%LINEPROTO-5-UPDOWN: Line
protocol on Interface Ethernet1/0/1, changed state to DOWN
36 Jan 25 11:29:33:000 2019 Switch DEFAULT/2/:System cold restart...
35 Jan 25 11:28:36:000 2019 Switch DEFAULT/5/:%LINEPROTO-5-UPDOWN: Line
protocol on Interface Vlan1,changed state to UP
......
----finish show trap buffer----
```

9.6.12 show info-center logfile

Command: `show info-center logfile`

Function: Displays the contents of the logfile output direction.

Parameters:

Parameter	Description
logfile <1-4>	Logfile output direction (optional)
keyword WORD	Regular expression used to filter logs
member <1-16>	Member ID

Command Mode: All Modes.

Default: None.

Usage Guidelines: This command displays the contents of the logfile output direction. The output can be filtered with a regular expression.

Note: There is no separate command for displaying user commands. All user commands are logged with the string "CMD:", which can be used as a filter keyword. In VSF mode, add **member** at the end of the command.

Example:

```
Sysname(config)#show info-center logfile 1
severity: 1-emergencies 2-alerts 3-critical 4-errors 5-warnings 6-
notifications 7-informational 8-debugging
55 Dec 18 14:47:22:000 2018 ECS8830F/ECS8854F
```

```
MODULE_UTILS_FILESYSTEM/2/:fs_write_file 2167: FS_DEV_UNLOCK Slot: 1
dev_name:flash: file_name:flash:/board_web_language
54 Dec 18 14:47:22:000 2018 ECS8830F/ECS8854F
MODULE_UTILS_FILESYSTEM/2/:fs_write_file 2149: FS_DEV_LOCK_NO_WAIT Slot: 1
dev_name:flash: file_name:flash:/board_web_language
53 Dec 18 14:47:16:000 2018 ECS8830F/ECS8854F
MODULE_MANAGEINTF/5/:%LINEPROTO-5-UPDOWN: Line protocol on Interface
Ethernet0, changed state to DOWN
52 Dec 18 14:47:16:000 2018 ECS8830F/ECS8854F
MODULE_MANAGEINTF/5/:%LINK-5-CHANGED: Interface Ethernet0, changed state to
UP
51 Dec 18 14:47:16:000 2018 ECS8830F/ECS8854F DEFAULT/3/:Clock between master
and slave has been synchronized!
50 Dec 18 14:47:15:000 2018 sysname MODULE_VSF_PROTO/2/:topo success! vsf
done 1 state ALIVE master 00-03-0f-aa-aa-ab seq 0 local seq 0
49 Dec 18 14:47:15:000 2018 sysname MODULE_VSF_PROTO/2/:disc success! cpu num
1 vsf done 0 state TOPO master 00-03-0f-aa-aa-ab seq 0 pri 0x4000207f local
seq 0 pri 0x4000207f
48 Dec 18 14:47:15:000 2018 sysname MODULE_VSF_PROTO/2/:Master 00-03-0f-aa-
aa-ab  mid 1 pri 0x4000207f seq 0
47 Dec 18 14:47:15:000 2018 sysname
MODULE_VSF_PROTO/2/:vsf_proto_handle_start 2448: vsf done 0 local seq 0 pri
0x207f
......
----finish show log file----
```

9.6.13 info-center list all disk

Command: `info-center list all disk`

Function: Displays the storage devices on which the information center can save files.

Parameters: None.

Command Mode: Global Mode.

Default: None.

Usage Guidelines: This command displays the storage devices on which the information center can save files. Supported devices are flash, USB, and MMC.

Example:

```
Sysname(config)# info-center list all disk
flash:
usb:
mmc:
```

9.6.14 info-center save all

Command: `info-center save all ((flash|usb|mmc) WORD)`

Function: Collects all information center data in one step.

Parameters:

Parameter	Description
flash|usb|mmc	Storage location of the file (optional)
WORD	File name

Command Mode: Global Mode.

Default: None.

Usage Guidelines: This command collects all information center data in one step: the information center configuration and the logs recorded in logbuffer and trapbuffer. If no file path and name are

specified, the data is saved to the default location with the default file name. If an MMC device is present, the default location is MMC; otherwise, it is flash. The default file name is icsaveall.txt.

Example:

```
Sysname(config)# info-center save all flash saveall.log
*****Now saving Master card(member 1)*****
Now saving infocenter all configuration, please wait..
Now saving infocenter logbuffer content, please wait..
Now saving infocenter trapbuffer content, please wait..
*****Master card(member 1) saving finished!*****
```

9.7 Mirror

9.7.1 monitor session source interface

Command: monitor session <session> source {interface <interface-list>} {rx| tx| both}
no monitor session <session> source {interface <interface-list>}

Function: Specifies the source interfaces of a mirror session. The **no** form of this command removes the configuration.

Parameters: <session> is the mirror session number, ranging from 1 to 7. **<interface-list>** is the list of source interfaces, which can be separated with "-" and ";". **rx** mirrors the frames received on the interface, **tx** mirrors the frames sent from the interface, and **both** mirrors frames in both directions.

Command Mode: Global Mode.

Usage Guidelines: This command configures the source interfaces of a mirror session. The switch does not restrict which interfaces can be mirror sources; the source can be one interface or multiple interfaces. Received and sent frames can both be mirrored, or only one direction can be mirrored. If **rx**, **tx**, or **both** is not specified, **both** is used by default. When multiple interfaces are mirrored, each can use a different direction, but they must be configured separately.

Example: Mirror the frames sent from interfaces 1/0/1-4 and the frames received on interface 1/0/5.

```
Switch(config)#monitor session 1 source interface ethernet 1/0/1-4 tx
Switch(config)#monitor session 1 source interface ethernet1/0/5 rx
```

9.7.2 monitor session source interface access-list

Command: monitor session <session> source {interface <interface-list>} access-list <num> {rx|tx|both}
no monitor session <session> source {interface <interface-list>} access-list <num>

Function: Specifies an access list for filtering the mirror source traffic. The **no** form of this command removes the configuration.

Parameters: <session> is the mirror session number, ranging from 1 to 7. **<interface-list>** is the list of source interfaces, which can be separated with "-" and ";". **<num>** is the access list number. **rx** mirrors the frames received on the interface, **tx** mirrors the frames sent from the interface, and **both** mirrors frames in both directions.

Command Mode: Global Mode.

Usage Guidelines: This command configures the source interfaces of a mirror session with access list filtering. The switch does not restrict which interfaces can be mirror sources; the source can be one interface or multiple interfaces. For flow mirroring, only received frames can be mirrored. The direction parameter can be **rx**, **tx**, or **both**. Configure the access list before using this command; for details, see the ACL configuration. The flow mirror can be created only after the destination interface of the session is configured.

Example: In session 2, mirror the traffic on interface 1/0/6 filtered by access list 120.

```
Switch(config)#monitor session 2 source interface 1/0/6 access-list 120 rx
```

9.7.3 monitor session destination interface

Command: monitor session <session> destination interface <interface-number>
no monitor session <session> destination interface <interface-number>

Function: Specifies the destination interface of a mirror session. The **no** form of this command removes the configuration.

Parameters: <session> is the mirror session number, ranging from 1 to 7. **<interface-number>** is the destination interface of the mirror.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: The switch supports seven mirror destination interfaces. The destination interface must not be a member of a port trunk. The maximum throughput of the destination interface should be greater than the total throughput of the mirrored interfaces. If the destination of a session is removed, the mirror paths configured in the session are removed at the same time; if the destination interface is configured again, the mirror paths are restored. Flow mirroring is restored only after the destination interface is configured again.

Example: Configure interface 1/0/7 as the mirror destination.

```
Switch(config)#monitor session 1 destination interface ethernet 1/0/7
```

9.7.4 show monitor

Command: show monitor

Function: Displays the source and destination ports of all mirror sessions.

Command Mode: Admin Mode.

Usage Guidelines: This command displays the source and destination ports of the configured mirror sessions. For port mirroring and flow mirroring, the mirror direction of each source is displayed. For MAC mirroring, the MAC mirror configuration is displayed on switch cards that support it.

Example:

```
Switch#show monitor
```

9.8 RSPAN

9.8.1 remote-span

Command: remote-span
no remote-span

Function: Configures a VLAN as the RSPAN VLAN. The **no** form of this command removes the RSPAN VLAN configuration.

Parameters: None.

Command Mode: VLAN Mode.

Default: Not configured.

Usage Guidelines: This command configures an existing VLAN as the RSPAN VLAN. A dedicated RSPAN VLAN must be configured before RSPAN can work. Special VLANs, such as the default VLAN, dynamic VLANs, private VLANs, multicast VLANs, and VLANs with a Layer 3 interface, must

not be configured as the RSPAN VLAN. If RSPAN is disabled while sessions are running, those sessions keep working regardless of the configuration change. However, if a Layer 3 interface is configured in the VLAN after RSPAN is disabled, the existing RSPAN sessions stop.

Example:

```
Switch(Config-Vlan5)#remote-span
```

9.8.2 monitor session remote vlan

Command: monitor session <session> remote vlan <vid>
no monitor session <session> remote vlan

Function: Changes a local mirror session to an RSPAN session. The **no** form of this command changes the RSPAN session back to a local mirror session.

Parameters: <session>: The session ID, ranging from 1 to 7. **<vid>**: The RSPAN VLAN ID.

Command Mode: Global Mode.

Default: Not configured.

Usage Guidelines: This command changes a local mirror session to an RSPAN session. The VLAN ID is the RSPAN VLAN. Mirrored frames are tagged with the RSPAN VLAN tag.

Example:

```
Switch(config)#monitor session 1 remote vlan 5
```

9.8.3 monitor session reflector-port

Command: monitor session <session> reflector-port <interface-number>
no monitor session <session> reflector-port <interface-number>

Function: Configures the reflector port. The **no** form of this command removes the reflector port.

Parameters: <session>: The session ID, ranging from 1 to 7. **<interface-number>**: The interface number.

Command Mode: Global Mode.

Default: Not configured.

Usage Guidelines: This command configures the reflector port for the mirrored frames and disables MAC learning on the specified port. Configuring a reflector port changes the local port from destination port mode to reflector mode, so the reflector port and the destination port are mutually exclusive. The **no** form restores the reflector port to a normal port. A source port in access or trunk mode must not be added to the RSPAN VLAN. When the reflector port is used to relay mirroring of CPU-sent (TX) traffic, it must be a trunk port that allows the RSPAN VLAN, and the native VLAN must not be the RSPAN VLAN. After RSPAN is configured, a VLAN tag is added to egress-mirrored frames, which can cause oversize frame errors on the reflector port; therefore, increase the default MTU of the switch.

Example:

```
Switch(config)#monitor session 1 reflector-port inter ethernet 1/0/3
```

9.9 ERSPAN

9.9.1 monitor session destination tunnel

Command: **monitor session <session> destination tunnel <tunnel-number> reflector-port <interface-number>**
no monitor session <session> destination tunnel <tunnel-number> reflector-port <interface-number>

Function: Specifies a tunnel as the mirror destination. The **no** form of this command removes the configuration.

Parameters: **<session>** is the mirror session number, ranging from 1 to 4. **<tunnel-number>** is the tunnel number. **<interface-number>** is the reflector port number of the mirror destination.

Default: Not configured.

Command Mode: Global Mode.

Usage Guidelines: The switch supports four destination tunnels. The destination tunnel, whether configured as physical ports or a tunnel, must not be a member of a port aggregation group, and the reflector port number of the mirror destination must be specified. The maximum throughput of the port should be greater than the total throughput of the mirrored source ports. If the destination tunnel of a session is removed, the mirror paths configured in the session are removed at the same time; if the destination tunnel is configured again, the port mirror paths are restored. Flow mirroring is restored only after the destination port is configured again. The destination tunnel must be fully configured beforehand and must be a GRE tunnel.

Example:

```
Switch(config)#monitor session 4 destination tunnel 1 reflector-port
ethernet1/0/3
```

9.10 sFlow

9.10.1 sflow agent-address

Command: **sflow agent-address <agent-address>**
no sflow agent-address

Function: Configures the sFlow agent address. The **no** form of this command deletes the agent address.

Parameters: **<agent-address>** is the IP address of the sFlow agent, in dotted decimal notation.

Command Mode: Global Mode.

Default: None.

Usage Guidelines: The agent address identifies the sFlow agent, similar to the router ID in OSPF or BGP. It is not required for the sFlow agent to work properly.

Example: Configure the sFlow agent address in Global Mode.

```
switch (config)#sflow agent-address 192.168.1.200
```

9.10.2 sflow analyzer

Command: **sflow analyzer sflowtrend**
no sflow analyzer sflowtrend

Function: Configures the analyzer used by sFlow. The **no** form of this command deletes the analyzer.

Parameters: sflowtrend specifies the sFlowTrend analyzer from InMon.

Command Mode: Global Mode.

Default: Not configured.

Usage Guidelines: Configure this command when sFlowTrend is used.

Example:

```
Switch(config)#sflow analyzer sflowtrend
```

9.10.3 sflow counter-interval

Command: `sflow counter-interval <interval-value>`
`no sflow counter-interval`

Function: Configures the maximum sFlow counter sampling interval. The **no** form of this command deletes the counter sampling interval.

Parameters: <interval-value> is the interval in seconds, ranging from 20 to 120.

Command Mode: Port Mode.

Default: None.

Usage Guidelines: If no counter sampling interval is configured, no counter sampling is performed on the interface.

Example: Set the counter sampling interval on interface Ethernet 1/1/1 to 20 seconds.

```
Switch(Config-If-Ethernet1/1/1)#sflow counter-interval 20
```

9.10.4 sflow data-len

Command: `sflow data-len <length-value>`
`no sflow data-len`

Function: Configures the maximum data length of sFlow packets. The **no sflow data-len** command restores the default.

Parameters: <length-value> is the length in bytes, ranging from 500 to 1470.

Command Mode: Port Mode.

Default: 1400.

Usage Guidelines: When several samples are combined into one sFlow datagram, the datagram length, excluding the MAC and IP headers, cannot exceed the configured value.

Example: Set the maximum data length of sFlow packets to 1000.

```
switch (Config-If-Ethernet1/1/2)#sflow data-len 1000
```

9.10.5 sflow destination

Command: `sflow destination <collector-address> [<collector-port>]`
`no sflow destination`

Function: Configures the IP address and port number of the host running the sFlow analysis software (collector). If an address is configured on the port, the port configuration is used; otherwise, the global configuration is used. The **no** form of this command restores the default port and deletes the IP address.

Parameters: <collector-address> is the IP address of the collector, in dotted decimal notation. **<collector-port>** is the destination port of the sFlow packets.

Command Mode: Global Mode and Port Mode.

Default: The destination port of sFlow packets is 6343. The collector has no default address.

Usage Guidelines: If a collector address is configured in Port Mode, the address and port configured in Port Mode are used when sample packets are sent; otherwise, the address and port configured in Global Mode are used. A collector address must be configured for the sFlow agent to work properly.

Example: Configure the collector address and port in Global Mode.

```
switch (config)#sflow destination 192.168.1.200 1025
```

9.10.6 sflow header-len

Command: `sflow header-len <length-value>`
`no sflow header-len`

Function: Configures the length of the packet header copied in sFlow data sampling. The **no** form of this command restores the default.

Parameters: <length-value> is the length in bytes, ranging from 32 to 256.

Command Mode: Port Mode.

Default: 128.

Usage Guidelines: If a sampled packet sent to the CPU cannot be identified as IPv4 or IPv6, a portion of its header is copied into the sFlow packet and sent. This command configures the length of the copied portion.

Example: Set the length of the packet header copied in sFlow data sampling to 50.

```
Switch(Config-If-Ethernet1/1/2)#sflow header-len 50
```

9.10.7 sflow priority

Command: `sflow priority <priority-value>`
`no sflow priority`

Function: Configures the priority of packets that sFlow receives from the hardware. The **no** form of this command restores the default.

Parameters: <priority-value> is the priority, ranging from 0 to 3.

Command Mode: Global Mode.

Default: 0.

Usage Guidelines: When sampled packets are sent to the CPU, do not assign them a high priority, so that the normal sending and receiving of other protocol packets is not affected. A higher value means a higher priority.

Example: Configure the priority of packets that sFlow receives from the hardware in Global Mode.

```
switch (config)#sflow priority 1
```

9.10.8 sflow rate

Command: `sflow rate { input <input-rate> | output <output-rate >}`
`no sflow rate [input | output]`

Function: Configures the sFlow hardware sampling rate. The **no** form of this command deletes the sampling rate.

Parameters: <input-rate> is the ingress packet sampling rate, ranging from 1000 to 16383500.

<output-rate> is the egress packet sampling rate, ranging from 1000 to 16383500.

Command Mode: Port Mode.

Default: None.

Usage Guidelines: If no sampling rate is configured on the port, no traffic sampling is performed. A sampling rate of 10000 for ingress traffic means that one packet is sampled out of every 10000 ingress packets.

Example: Set the ingress sampling rate on port Ethernet 1/1/1 to 10000 and the egress sampling rate to 20000.

```
Switch(Config-If-Ethernet1/1/1)#sflow rate input 10000
Switch(Config-If-Ethernet1/1/1)#sflow rate output 20000
```

9.10.9 sflow version

Command: `sflow version<version>`
`no sflow version`

Function: Configures the global sFlow version. The **no** form of this command restores the default.

Parameters: <version>: The sFlow version. Versions 4 and 5 are supported.

Default: 4.

Command Mode: Global Mode.

Usage Guidelines: This command configures the global sFlow version. Versions 4 and 5 are supported.

Example: Set the sFlow version to 5.

```
Switch (config)#sflow version 5
```

9.10.10 show sflow

Command: `show sflow`

Function: Displays the sFlow configuration and status.

Parameters: None.

Command Mode: All Modes.

Usage Guidelines: Use this command to check the operating status of sFlow.

```
Switch#show sflow
Sflow version 1.2
Agent address is 172.16.1.100
Collector address have not configured
Collector port is 6343
Sampler priority is 2
Sflow DataSource: type 2, index 194(Ethernet1/1/2)
  Collector address is 192.168.1.200
  Collector port is 6343
  Counter interval is 0
  Sample rate is input 0, output 0
  Sample packet max len is 1400
  Sample header max len is 50
  Sample version is 4
```

Output	Description
Sflow version 1.2	The sFlow version is 1.2.
Agent address is 172.16.1.100	The sFlow agent address is 172.16.1.100.
Collector address have not configured	The global sFlow collector address is not configured.
Collector port is 6343	The global sFlow destination port is the default, 6343.
Sampler priority is 2	The priority of packets that sFlow receives from the hardware is 2.
Sflow DataSource: type 2, index 194(Ethernet1/1/1)	One data source of the sFlow agent is interface Ethernet 1/1/1, of type 2 (Ethernet), with interface index 194.

Collector address is 192.168.1.200	The collector address for sampling on interface Ethernet 1/1/1 is 192.168.1.200.
Collector port is 6343	The sampling destination port on interface Ethernet 1/1/1 is the default, 6343.
Counter interval is 20	The counter sampling interval on interface Ethernet 1/1/1 is 20 seconds.
Sample rate is input 10000, output 0	The ingress sampling rate on interface Ethernet 1/1/1 is 10000; no egress sampling is performed.
Sample packet max len is 1400	The length of sFlow datagrams sent for interface Ethernet 1/1/1 cannot exceed 1400 bytes.
Sample header max len is 50	The length of the packet header copied in data sampling on interface Ethernet 1/1/1 is 50 bytes.
Sample version is 4	The version of sFlow datagrams sent for interface Ethernet 1/1/1 is 4.

9.11 NQA

9.11.1 nqa agent

Command: `nqa agent`
`no nqa agent`

Function: Enables the NQA client. The **no** form of this command disables the NQA client.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Configure this command to use the NQA client.

Example: Enable the NQA client.

```
Switch#config terminal
Switch(config)#nqa agent
```

9.11.2 nqa entry type icmp-echo

Command: `nqa entry <1-64> type icmp-echo dest-ip A.B.C.D (src-ip A.B.C.D |)`
`(nexthop-ip A.B.C.D |) (vrf WORD |)`
`no nqa entry <1-64>`

Function: Sets the probe type of the NQA entry to icmp-echo. The **no** form of this command deletes the NQA entry.

Parameters: <1-64>: The NQA entry ID.

dest-ip A.B.C.D: The destination IP address.

src-ip A.B.C.D: The source IP address.

nexthop-ip A.B.C.D: The next-hop IP address.

vrf WORD: The VRF name.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: Use this command to configure a icmp-echo probe.

Example: Set the probe type of the NQA entry to icmp-echo.

```
Switch#config terminal
```

```
Switch(config)#nqa entry 1 type icmp-echo dest-ip 1.1.1.1 src-ip 2.2.2.2
nexthop-ip 3.3.3.3 vrf 1
```

9.11.3 nqa entry type icmp-jitter

Command: nqa entry <1-64> type icmp-jitter dest-ip A.B.C.D (src-ip A.B.C.D |)
(nexthop-ip A.B.C.D |) (vrf WORD |)
no nqa entry <1-64>

Function: Sets the probe type of the NQA entry to icmp-jitter. The **no** form of this command deletes the NQA entry.

Parameters: <1-64>: The NQA entry ID.

dest-ip A.B.C.D: The destination IP address.

src-ip A.B.C.D: The source IP address.

nexthop-ip A.B.C.D: The next-hop IP address.

vrf WORD: The VRF name.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: Use this command to configure a icmp-jitter probe.

Example: Set the probe type of the NQA entry to icmp-jitter.

```
Switch#config terminal
Switch(config)#nqa entry 1 type icmp-jitter dest-ip 1.1.1.1 src-ip 2.2.2.2
nexthop-ip 3.3.3.3 vrf 1
```

9.11.4 nqa entry type udp-echo

Command: nqa entry <1-64> type udp-echo dest-ip A.B.C.D dest-port <1-65535>
(src-ip A.B.C.D |) (nexthop-ip A.B.C.D |) (vrf WORD |)
no nqa entry <1-64>

Function: Sets the probe type of the NQA entry to udp-echo. The **no** form of this command deletes the NQA entry.

Parameters: <1-64>: The NQA entry ID.

dest-ip A.B.C.D: The destination IP address.

dest-port <1-65535>: The destination port.

src-ip A.B.C.D: The source IP address.

nexthop-ip A.B.C.D: The next-hop IP address.

vrf WORD: The VRF name.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: Use this command to configure a udp-echo probe.

Example: Set the probe type of the NQA entry to udp-echo.

```
Switch#config terminal
Switch(config)#nqa entry 1 type udp-echo dest-ip 1.1.1.1 dest-port 1500 src-
ip 2.2.2.2 nexthop-ip 3.3.3.3 vrf 1
```

9.11.5 nqa entry type udp-jitter

Command: nqa entry <1-64> type udp-jitter dest-ip A.B.C.D dest-port <1-65535>
(src-ip A.B.C.D |) (nexthop-ip A.B.C.D |) (vrf WORD |)
no nqa entry <1-64>

Function: Sets the probe type of the NQA entry to udp-jitter. The **no** form of this command deletes the NQA entry.

Parameters: <1-64>: The NQA entry ID.

dest-ip A.B.C.D: The destination IP address.

dest-port <1-65535>: The destination port.

src-ip A.B.C.D: The source IP address.

nexthop-ip A.B.C.D: The next-hop IP address.

vrf WORD: The VRF name.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: Use this command to configure a udp-jitter probe.

Example: Set the probe type of the NQA entry to udp-jitter.

```
Switch#config terminal
Switch(config)#nqa entry 1 type udp-jitter dest-ip 1.1.1.1 dest-port 1500
src-ip 2.2.2.2 nexthop-ip 3.3.3.3 vrf 1
```

9.11.6 nqa entry type tcp

Command: nqa entry <1-64> type tcp dest-ip A.B.C.D dest-port <1-65535>
(src-ip A.B.C.D |) (nexthop-ip A.B.C.D |) (vrf WORD |)
no nqa entry <1-64>

Function: Sets the probe type of the NQA entry to tcp. The **no** form of this command deletes the NQA entry.

Parameters: <1-64>: The NQA entry ID.

dest-ip A.B.C.D: The destination IP address.

dest-port <1-65535>: The destination port.

src-ip A.B.C.D: The source IP address.

nexthop-ip A.B.C.D: The next-hop IP address.

vrf WORD: The VRF name.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: Use this command to configure a tcp probe.

Example: Set the probe type of the NQA entry to tcp.

```
Switch#config terminal
Switch(config)#nqa entry 1 type tcp dest-ip 1.1.1.1 dest-port 1500 src-ip
2.2.2.2 nexthop-ip 3.3.3.3 vrf 1
```

9.11.7 nqa entry type dhcp

Command: nqa entry <1-64> type dhcp interface vlan <1-4094>
no nqa entry <1-64>

Function: Sets the probe type of the NQA entry to dhcp. The **no** form of this command deletes the NQA entry.

Parameters: <1-64>: The NQA entry ID.

vlan <1-4094>: The VLAN ID.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: Use this command to configure a dhcp probe.

Example: Set the probe type of the NQA entry to dhcp.

```
Switch#config terminal
Switch(config)#nqa entry 1 type dhcp interface vlan 1
```

9.11.8 nqa entry description

Command: nqa entry <1-64> description TEXT
no nqa entry <1-64> description

Function: Configures the description of the NQA entry. The **no** form of this command deletes the description.

Parameters: <1-64>: The NQA entry ID.

description TEXT: The description.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: Use this command to configure a description for the NQA entry.

Example: Set the description of the NQA entry to icmp-test.

```
Switch#config terminal
Switch(config)#nqa entry 1 description icmp-test
```

9.11.9 nqa entry frequency

Command: nqa entry <1-64> frequency <3-60>
no nqa entry <1-64> frequency

Function: Configures the probe frequency of the NQA entry. The **no** form of this command restores the default.

Parameters: <1-64>: The NQA entry ID.

frequency <3-60>: The probe interval, ranging from 3 to 60 seconds.

Default: 40 seconds for icmp-jitter and udp-jitter probes; 3 seconds for other probes.

Command Mode: Global Mode.

Usage Guidelines: Use this command to change the probe interval of the NQA entry.

Example: Set the probe interval of the NQA entry to 10 seconds.

```
Switch#config terminal
Switch(config)#nqa entry 1 frequency 10
```

9.11.10 nqa entry probe-count

Command: nqa entry <1-64> probe-count <1-5>
no nqa entry <1-64> probe-count

Function: Configures the number of probes sent in each probe interval of the NQA entry. The **no** form of this command restores the default.

Parameters: <1-64>: The NQA entry ID.

probe-count <1-5>: The number of probes, ranging from 1 to 5.

Default: 20 for icmp-jitter and udp-jitter probes; 1 for other probes.

Command Mode: Global Mode.

Usage Guidelines: Use this command to change the number of probes sent in each probe interval of the NQA entry.

Example: Send three probes in each probe interval of the NQA entry.

```
Switch#config terminal
Switch(config)#nqa entry 1 probe-count 3
```

9.11.11 nqa entry probe-timeout

Command: nqa entry <1-64> probe-timeout <1-5>
no nqa entry <1-64> probe-timeout

Function: Configures the probe timeout of the NQA entry. The **no** form of this command restores the default.

Parameters: <1-64>: The NQA entry ID.

probe-timeout <1-5>: The probe timeout, ranging from 1 to 5 seconds.

Default: 2 seconds.

Command Mode: Global Mode.

Usage Guidelines: Use this command to change the probe timeout of the NQA entry.

Example: Set the probe timeout of the NQA entry to 3 seconds.

```
Switch#config terminal
Switch(config)#nqa entry 1 probe-timeout 3
```

9.11.12 nqa entry datasize

Command: nqa entry <1-64> datasize <1-8100>
no nqa entry <1-64> datasize

Function: Configures the packet data size of the NQA entry. The **no** form of this command restores the default.

Parameters: <1-64>: The NQA entry ID.

datasize <1-8100>: The packet data size, ranging from 1 to 8100 bytes.

Default: 56 bytes.

Command Mode: Global Mode.

Usage Guidelines: Use this command to change the packet data size of the NQA entry.

Example: Set the packet data size of the NQA entry to 1500 bytes.

```
Switch#config terminal
Switch(config)#nqa entry 1 datasize 1500
```

9.11.13 nqa entry ttl

Command: nqa entry <1-64> ttl <1-255>
no nqa entry <1-64> ttl

Function: Configures the TTL of NQA entry packets. The **no** form of this command restores the default.

Parameters: <1-64>: The NQA entry ID.

ttl <1-255>: The packet TTL, ranging from 1 to 255.

Default: 30.

Command Mode: Global Mode.

Usage Guidelines: Use this command to change the TTL of NQA entry packets.

Example: Set the TTL of NQA entry packets to 100.

```
Switch#config terminal
Switch(config)#nqa entry 1 ttl 100
```

9.11.14 nqa entry tos

Command: **nqa entry <1-64> tos <0-255>**
no nqa entry <1-64> tos

Function: Configures the ToS of NQA entry packets. The **no** form of this command restores the default.

Parameters: <1-64>: The NQA entry ID.

tos <0-255>: The packet ToS, ranging from 0 to 255.

Default: 0.

Command Mode: Global Mode.

Usage Guidelines: Use this command to change the ToS of NQA entry packets.

Example: Set the ToS of NQA entry packets to 100.

```
Switch#config terminal
Switch(config)#nqa entry 1 tos 100
```

9.11.15 nqa entry fail-percent

Command: **nqa entry <1-64> fail-percent <1-100>**
no nqa entry <1-64> fail-percent

Function: Configures the failure percentage of the NQA entry. The **no** form of this command restores the default.

Parameters: <1-64>: The NQA entry ID.

fail-percent <1-100>: The failure percentage, ranging from 1 to 100.

Default: 100.

Command Mode: Global Mode.

Usage Guidelines: Use this command to change the failure percentage of the NQA entry.

Example: Set the failure percentage of the NQA entry to 10%.

```
Switch#config terminal
Switch(config)#nqa entry 1 fail-percent 10
```

9.11.16 nqa entry records-result

Command: **nqa entry <1-64> records-result <1-10>**
no nqa entry <1-64> records-result

Function: Configures the maximum number of result records of the NQA entry. The **no** form of this command restores the default.

Parameters: <1-64>: The NQA entry ID.

records-result <1-10>: The maximum number of result records, ranging from 1 to 10.

Default: 5.

Command Mode: Global Mode.

Usage Guidelines: Use this command to change the maximum number of result records of the NQA entry.

Example: Set the maximum number of result records of the NQA entry to 10.

```
Switch#config terminal
```

```
Switch(config)#nqa entry 1 records-result 10
```

9.11.17 nqa entry probe-threshold

Command: nqa entry <1-64> probe-threshold <50-5000>
no nqa entry <1-64> probe-threshold

Function: Configures the probe threshold of the NQA entry. The **no** form of this command restores the default.

Parameters: <1-64>: The NQA entry ID.

probe-threshold <50-5000>: The probe threshold, ranging from 50 to 5000 ms.

Default: 2000 ms.

Command Mode: Global Mode.

Usage Guidelines: Use this command to change the probe threshold of the NQA entry.

Example: Set the probe threshold of the NQA entry to 3000 ms.

```
Switch#config terminal
Switch(config)#nqa entry 1 probe-threshold 3000
```

9.11.18 nqa entry start

Command: nqa entry <1-64> start (|forever|time-range WORD)
no nqa entry <1-64> start

Function: Starts the NQA entry. The **no** form of this command restores the default.

Parameters: <1-64>: The NQA entry ID.

forever: Probes continuously.

time-range WORD: The probe running time.

Default: The NQA entry does not probe.

Command Mode: Global Mode.

Usage Guidelines: If no probe time is specified, the entry stops after one probe cycle.

Example: Start the NQA entry and probe continuously.

```
Switch#config terminal
Switch(config)#nqa entry 1 start forever
```

9.11.19 nqa alarm enable

Command: nqa alarm enable
no nqa alarm enable

Function: Enables global NQA alarms. The **no** form of this command disables global NQA alarms.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Configure this command to enable global NQA alarms.

Example: Enable global NQA alarms.

```
Switch#config terminal
Switch(config)#nqa alarm enable
```

9.11.20 nqa traps enable

Command: **`nqa traps enable`**
`no nqa traps enable`

Function: Enables global NQA traps. The **no** form of this command disables global NQA traps.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Configure this command to enable global NQA traps.

Example: Enable global NQA traps.

```
Switch#config terminal
Switch(config)#nqa traps enable
```

9.11.21 nqa entry alarm enable

Command: **`nqa entry <1-64> alarm enable`**
`no nqa entry <1-64> alarm enable`

Function: Enables alarms for the NQA entry. The **no** form of this command disables them.

Parameters: **<1-64>**: The NQA entry ID.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Configure this command to use alarms for the NQA entry.

Example: Enable alarms for the NQA entry.

```
Switch#config terminal
Switch(config)#nqa entry 1 alarm enable
```

9.11.22 nqa entry traps enable

Command: **`nqa entry <1-64> traps enable`**
`no nqa entry <1-64> traps enable`

Function: Enables traps for the NQA entry. The **no** form of this command disables them.

Parameters: **<1-64>**: The NQA entry ID.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Configure this command to use traps for the NQA entry.

Example: Enable traps for the NQA entry.

```
Switch#config terminal
Switch(config)#nqa entry 1 traps enable
```

9.11.23 nqa server

Command: **`nqa server`**
`no nqa server`

Function: Enables the NQA server. The **no** form of this command disables the NQA server.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Configure this command to enable the NQA server.

Example: Enable the NQA server.

```
Switch#config terminal
Switch(config)#nqa server
```

9.11.24 nqa server tcp-port

Command: nqa server tcp-port <1-65535> (vrf WORD |)
no nqa server tcp-port (vrf WORD |)

Function: Configures the TCP listening port of the NQA server. The **no** form of this command disables TCP listening on the NQA server.

Parameters: tcp-port <1-65535>: The TCP listening port number.

vrf WORD: The VRF name.

Default: The TCP listening port is 2000.

Command Mode: Global Mode.

Usage Guidelines: Configure this command for the NQA server to listen on a TCP port.

Example: Configure the NQA server to listen on TCP port 3000 in VRF a.

```
Switch#config terminal
Switch(config)#nqa server tcp-port 3000 vrf a
```

9.11.25 nqa server udp-port

Command: nqa server udp-port <1-65535> (vrf WORD |)
no nqa server udp-port (vrf WORD |)

Function: Configures the UDP listening port of the NQA server. The **no** form of this command disables UDP listening on the NQA server.

Parameters: udp-port <1-65535>: The UDP listening port number.

vrf WORD: The VRF name.

Default: The UDP listening port is 2000.

Command Mode: Global Mode.

Usage Guidelines: Configure this command for the NQA server to listen on a UDP port.

Example: Configure the NQA server to listen on UDP port 3000 in VRF a.

```
Switch#config terminal
Switch(config)#nqa server udp-port 3000 vrf a
```

9.11.26 track nqa

Command: track <1-32> nqa <1-64>
no track <1-32> (nqa <1-64>|)

Function: Associates a track with an NQA entry. The **no** form of this command removes the association.

Parameters: track <1-32>: The track ID.

nqa <1-64>: The NQA entry ID.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: Configure this command to associate an NQA entry with a track.

Example: Associate an NQA entry with a track.

```
Switch#config terminal
Switch(config)#track 1 nqa 1
```

9.11.27 track list boolean

Command: `track <1-32> list boolean (and|or)`
`no track <1-32> list boolean`

Function: Configures the Boolean relationship among multiple NQA entries associated with a track. The **no** form of this command removes the Boolean relationship.

Parameters: track <1-32>: The track ID.

boolean (and|or): The Boolean relationship (AND or OR) among multiple NQA entries.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: Configure this command when multiple NQA entries are associated with a track. With **and**, the track fails if any probe fails. With **or**, the track succeeds if any probe succeeds.

Example: Associate a track with multiple NQA entries using the AND relationship.

```
Switch#config terminal
Switch(config)#track 1 list boolean and
```

9.11.28 ip route track

Command: `ip route (A.B.C.D A.B.C.D | A.B.C.D/M) A.B.C.D track <1-32>`
`no ip route (A.B.C.D A.B.C.D | A.B.C.D/M) (A.B.C.D|) (track <1-32>|)`

Function: Associates a static route with a track. The **no** form of this command deletes the static route.

Parameters: A.B.C.D: The destination IP address.

A.B.C.D: The subnet mask.

A.B.C.D/M: The IP address prefix.

A.B.C.D: The next-hop IP address.

<1-32>: The track ID.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: Configure this command to associate a static route with a track.

Example: Associate a static route with a track.

```
Switch#config terminal
Switch(config)#ip route 1.1.1.1/32 2.2.2.2 track 1
```

9.11.29 rip track

Command: `rip track <1-32>`
`no rip track <1-32>`

Function: Associates RIP with a track. The **no** form of this command removes the association.

Parameters: <1-32>: The track ID.

Default: None.

Command Mode: Interface Mode.

Usage Guidelines: Configure this command to associate RIP with a track.

Example: Associate RIP with a track.

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#rip track 1
```

9.11.30 ospf track

Command: ip ospf track <1-32>
no ip ospf track <1-32>

Function: Associates OSPF with a track. The **no** form of this command removes the association.

Parameters: <1-32>: The track ID.

Default: None.

Command Mode: Interface Mode.

Usage Guidelines: Configure this command to associate OSPF with a track.

Example: Associate OSPF with a track.

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#ip ospf track 1
```

9.11.31 bgp track

Command: neighbor {<ip-address>|<TAG>} track <1-32>
no neighbor {<ip-address>|<TAG>} track <1-32>

Function: Associates a BGP neighbor with a track. The **no** form of this command removes the association.

Parameters: <ip-address>: The IP address of the neighbor.

<TAG>: The name of the peer group.

<1-32>: The track ID.

Default: None.

Command Mode: BGP Mode.

Usage Guidelines: Configure this command to associate BGP with a track.

Example: Associate BGP neighbor 1.1.1.1 with a track.

```
Switch#config terminal
Switch(config)#router bgp 1
Switch(config-router)#neighbor 1.1.1.1 track 1
```

9.11.32 show nqa results

Command: show nqa (entry <1-64>|) results

Function: Displays the probe results of NQA entries.

Parameters: <1-64>: The NQA entry ID.

Default: None.

Command Mode: All Modes.

Usage Guidelines: After an NQA entry completes a probe, use this command to display the probe results. If no NQA entry ID is specified, the probe results of all NQA entries are displayed.

Example: Display the probe results of NQA entry 1.

```
switch#show nqa entry 1 results
------------------------------------------------------------
NQA entry(test probe-type, icmp-echo)
        1, Test 17 result   The test is finished.
         Send operation times: 1 Receive response times: 1
         Min/Max/Avg/Sum RTT: 0/0/0/0
         RTT Square Sum: 0
         Start probe Time: 2023-11-10 11:26:55
         Lost packet ratio: 0%
```

Output	Description
probe-type	Probe type
Send operation times	Number of probes sent
Receive response times	Number of responses received
Min/Max/Avg/Sum RTT	Minimum, maximum, average, and total round-trip time
RTT Square Sum	Sum of the squares of the round-trip times
Start probe Time	Time when the probe started
Lost packet ratio	Packet loss ratio

9.11.33 show track status

Command: `show track (all|<1-32>) status`

Function: Displays the track status.

Parameters: all: Displays the status of all tracks.

<1-64>: The track ID.

Default: None.

Command Mode: All Modes.

Usage Guidelines: After a track is created, use this command to view its status.

Example: Display the status of track 1.

```
switch#show track 1 status
Track ID: 1
Notification delay: Positive 0, Negative 0 (in milliseconds)
Logical mode: Default
  Remote-ip: *                   probe-status: positive
    protocal: NQA 1               status: success
```

Chapter 10 Commands for Network Time Management

10.1 NTP

10.1.1 clock timezone

Command: **`clock timezone WORD {add | subtract} <0-23> [<0-59>]`**
`no clock timezone WORD`

Function: Configures the time zone. The **no** form of this command deletes the configured time zone.

Parameters: **WORD**: The time zone name, up to 16 characters.

add | subtract: Whether the offset is added to or subtracted from UTC.

<0-23>: The hour offset.

<0-59>: The minute offset.

Command Mode: Global Mode.

Default: None.

Usage Guidelines: The time zone name cannot contain spaces. The hour and minute values must be within the specified ranges.

Example: Configure a time zone named aaa with an offset of +8 hours.

```
Switch(config)#clock timezone aaa add 8
```

10.1.2 debug ntp adjust

Command: **`debug ntp adjust`**
`no debug ntp adjust`

Function: Enables or disables debugging of local time adjustment information.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example: Enable debugging of local time adjustment information.

```
Switch# debug ntp adjust
```

10.1.3 debug ntp authentication

Command: **`debug ntp authentication`**
`no debug ntp authentication`

Function: Enables display of NTP authentication information. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: When this debugging is enabled, the key identifier is printed if a packet sent or received carries authentication information.

Example: Enable display of NTP authentication information.

```
Switch# debug ntp authentication
```

10.1.4 debug ntp events

Command: `debug ntp events`
`no debug ntp events`

Function: Enables or disables debugging of NTP events.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: When this debugging is enabled, events such as a server changing between available and unavailable, and received illegal packets, are printed.

Example: Enable debugging of NTP events.

```
Switch# debug ntp events
```

10.1.5 debug ntp packet

Command: `debug ntp packet [send | receive]`
`no debug ntp packet [send | receive]`

Function: Enables or disables debugging of NTP packet information.

Parameters: send: Debugs sent NTP packets.

receive: Debugs received NTP packets.

If no parameter is specified, debugging is enabled for both sent and received NTP packets.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example: Enable debugging of NTP packet information.

```
Switch# debug ntp packet
```

10.1.6 debug ntp sync

Command: `debug ntp sync`
`no debug ntp sync`

Function: Enables or disables debugging of local time synchronization information.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example: Enable debugging of local time synchronization information.

```
Switch# debug ntp sync
```

10.1.7 ntp access-group

Command: `ntp access-group server <acl>`
`no ntp access-group server <acl>`

Function: Configures or removes the access control list of the NTP server.

Parameters: <acl>: The ACL number, ranging from 1 to 99.

Default: Not configured.

Command Mode: Global Mode.

Usage Guidelines: None.

Example: Apply access control list 2 to the NTP server.

```
Switch(config)#ntp access-group server 2
```

10.1.8 ntp authenticate

Command: **`ntp authenticate`**
`no ntp authenticate`

Function: Enables or disables NTP authentication.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: None.

Example: Enable NTP authentication.

```
Switch(config)#ntp authenticate
```

10.1.9 ntp authentication-key

Command: **`ntp authentication-key <key-id> md5 <value>`**
`no ntp authentication-key <key-id>`

Function: Defines or removes an NTP authentication key.

Parameters: **<key-id>**: The key ID, ranging from 1 to 4294967295.

<value>: The key value, 1 to 16 ASCII characters.

Default: No NTP authentication key is configured.

Command Mode: Global Mode.

Usage Guidelines: None.

Example: Define an NTP authentication key with key ID 20 and MD5 key value abc.

```
Switch(config)# ntp authentication-key 20 md5 abc
```

10.1.10 ntp broadcast client

Command: **`ntp broadcast client`**
`no ntp broadcast client`

Function: Enables or disables the receiving of NTP broadcast packets on the specified interface.

Parameters: None.

Default: Disabled.

Command Mode: VLAN Interface Mode.

Usage Guidelines: None.

Example: Enable the VLAN 1 interface to receive NTP broadcast packets.

```
Switch(config)# interface vlan 1
Switch(Config-if-Vlan1)#ntp broadcast client
```

10.1.11 ntp broadcast server count

Command: **`ntp broadcast server count <number>`**
`no ntp broadcast server count`

Function: Sets the maximum number of broadcast or multicast servers supported by the NTP client. The **no** form of this command restores the default.

Parameters: <number>: The maximum number of broadcast servers, ranging from 1 to 100.

Default: 50.

Command Mode: Global Mode.

Example: Set the maximum number of broadcast servers to 70.

```
Switch(config)#ntp broadcast server count 70
```

10.1.12 ntp disable

Command: **`ntp disable`**
`no ntp disable`

Function: Disables or enables NTP on the interface.

Parameters: None.

Default: NTP is enabled on all interfaces.

Command Mode: VLAN Interface Mode.

Usage Guidelines: None.

Example: Disable NTP on the VLAN 1 interface.

```
Switch(config)# interface vlan 1
Switch(Config-if-Vlan1)#ntp disable
```

10.1.13 ntp enable

Command: **`ntp enable`**
`ntp disable`

Function: Enables or disables NTP globally.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: None.

Example: Enable NTP.

```
Switch(config)#ntp enable
```

10.1.14 ntp ipv6 multicast client

Command: **`ntp ipv6 multicast client`**
`no ntp ipv6 multicast client`

Function: Enables the specified interface to receive IPv6 NTP multicast packets. The **no** form of this command disables it.

Parameters: None.

Command Mode: VLAN Interface Mode.

Default: The interface does not receive IPv6 NTP multicast packets.

Usage Guidelines: None.

Example: Enable the VLAN 1 interface to receive IPv6 NTP multicast packets.

```
Switch(Config)# interface vlan 1
Switch(Config-if-Vlan1)#ntp ipv6 multicast client
```

10.1.15 ntp multicast client

Command: **`ntp multicast client`**
`no ntp multicast client`

Function: Enables the specified interface to receive NTP multicast packets. The **no** form of this command disables it.

Parameters: None.

Command Mode: VLAN Interface Mode.

Default: The interface does not receive NTP multicast packets.

Usage Guidelines: None.

Example: Enable the VLAN 1 interface to receive NTP multicast packets.

```
Switch(Config)# interface vlan 1
Switch(Config-if-Vlan1)#ntp multicast client
```

10.1.16 ntp server

Command: **`ntp server {vrf <vrfname>|host <hostname>|<ip-address> | <ipv6-address>} [version <version_no>] [key <key-id>]`**
`no ntp server {vrf <vrfname>|host <hostname>|<ip-address>|<ipv6-address>}`

Function: Specifies an NTP server as the time source. The **no** form of this command removes the server.

Parameters: **<ip-address>**: The IPv4 address of the time server.

<ipv6-address>: The IPv6 address of the time server.

version: Specifies the NTP version for the server.

<version_no>: The NTP version number of the server, ranging from 1 to 4. The default is 4.

key: Specifies a key for the server.

<key-id>: The key ID.

<vrfname>: The VRF instance name.

<hostname>: The host name of the server.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: None.

Example: Configure 1.1.1.1 as the time server.

```
Switch(config)#ntp server 1.1.1.1
```

10.1.17 ntp syn-interval

Command: **`ntp syn-interval <1-3600>`**
`no ntp syn-interval`

Function: Sets the interval at which the NTP client sends request packets, from 1 to 3600 seconds. The **no** form of this command restores the default of 64 seconds.

Default: 64 seconds.

Command Mode: Global Mode.

Usage Guidelines: To reduce the risk of incorrect time adjustment on high-latency networks, the NTP client sends eight time requests and uses the response with the lowest latency to synchronize the system time. With the default configuration, the client sends a request every 64 seconds and

adjusts the time after eight requests, that is, about every 8 minutes. To adjust the time once per hour, for example, set the interval to 450 seconds (3600/8).

Example: Adjust the system time once per hour by setting the request interval to 450 seconds.

```
Switch(config)#ntp syn-interval 450
```

10.1.18 ntp trusted-key

Command: `ntp trusted-key <key-id>`
`no ntp trusted-key <key-id>`

Function: Configures a trusted key. The **no** form of this command removes the trusted key.

Parameters: <key-id>: The key ID, ranging from 1 to 4294967295.

Default: No trusted key is configured.

Command Mode: Global Mode.

Usage Guidelines: None.

Example: Configure key 20 as a trusted key.

```
Switch(config)# ntp trusted-key 20
```

10.1.19 show ntp status

Command: `show ntp status`

Function: Displays the time synchronization status, including whether the clock is synchronized, the stratum, and the address of the time source.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: None.

Example:

```
Switch# show ntp status
Clock status: synchronized
Clock stratum: 3
Reference clock server: 1.1.1.2
Clock offset: 0.010 s
Root delay: 0.012 ms
Root dispersion: 0.000 ms
Reference time: TUE JAN 03 01:27:24 2006
```

10.1.20 show ntp session

Command: `show ntp session [<ip-address> | <ipv6-address>]`

Function: Displays information about all NTP sessions or a specific session, including the server ID, server stratum, and local offset from the server. An asterisk (*) marks the server selected as the local time source.

Parameters: <ip-address>: The IPv4 address of a configured time server.

<ipv6-address>: The IPv6 address of a configured time server.

If no parameter is specified, session information for all servers, including broadcast and multicast servers, is displayed.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: None.

Example:

```
(Switch)# show ntp session
   server       stream      type     rootdelay     rootdispersion
trustlevel
*  1.1.1.2        2         unicast    0.010s          0.002s       10
   2.2.2.2        3         unicast    0.005s          0.000s       10
```

10.2 SNTP

10.2.1 clock timezone

Command: `clock timezone WORD {add | subtract} <0-23> [<0-59>]`
`no clock timezone WORD`

Function: Configures the time zone. The **no** form of this command deletes the configured time zone.

Parameters: WORD: The time zone name, up to 16 characters.

add | subtract: Whether the offset is added to or subtracted from UTC.

<0-23>: The hour offset.

<0-59>: The minute offset.

Command Mode: Global Mode.

Default: None.

Usage Guidelines: The time zone name cannot contain spaces. The hour and minute values must be within the specified ranges.

Example: Configure a time zone named aaa with an offset of +8 hours.

```
Switch(config)#clock timezone aaa add 8
```

10.2.2 debug sntp

Command: `debug sntp {adjust | packet | select|config }`
`no debug sntp {adjust | packet | select|config}`

Function: Enables or disables SNTP debugging.

Parameters: adjust: SNTP clock adjustment information. **packet**: SNTP packets. **select**: SNTP clock selection. **config**: SNTP configuration information.

Command Mode: Admin Mode.

Example: Enable debugging of SNTP packets.

```
Switch#debug sntp packet
```

10.2.3 sntp polltime

Command: `sntp polltime <interval>`
`no sntp polltime`

Function: Sets the interval at which the SNTP client sends requests to the NTP/SNTP server. The **no sntp polltime** command restores the default.

Parameters: <interval> is the interval in seconds, ranging from 16 to 16284.

Default: 64 seconds.

Command Mode: Global Mode.

Example: Set the client to send a request to the server every 128 seconds.

```
Switch#config
Switch(config)#sntp polltime128
```

10.2.4 sntp server

Command: sntp server {vrf <vrfname>|host <hostname> |<ip-address> | <ipv6-address>} [source {vlan <vlan no> | loopback <loopback no>}] [version <version_no>]
no sntp server {vrf <vrfname>|host <hostname>|<ip-address> | <ipv6-address>} [source {vlan <vlan no> | loopback <loopback no>}] [version <version_no>]

Function: Specifies a time server as the clock source. The **no** form of this command deletes the specified time server.

Parameters: <ip-address>: The IPv4 address of the time server.

<ipv6-address>: The IPv6 address of the time server.

source: Specifies the interface that provides the source address.

vlan: Specifies a VLAN interface.

<vlan no>: The VLAN number, ranging from 1 to 4094.

loopback: Specifies a loopback interface.

<loopback no>: The loopback interface ID, ranging from 1 to 1024.

version: Specifies the version for the server.

<version_no>: The version number, ranging from 1 to 4. The default is 4.

<vrfname>: The VRF instance name.

<hostname>: The host name of the server.

Default: No time server is configured.

Command Mode: Global Mode.

Usage Guidelines: None.

Example:

Configure 1.1.1.1 as the time server, with the VLAN 1 interface as the source address interface:

```
Switch(config)#sntp server 1.1.1.1 source vlan 1
```

Delete time server 1.1.1.1, whose source address interface is VLAN 1:

```
Switch(config)#no sntp server 1.1.1.1 source vlan 1
```

10.2.5 show sntp

Command: show sntp

Function: Displays the current SNTP client configuration and server status.

Parameters: None.

Command Mode: Admin Mode and Configuration Mode.

Example: Display the current SNTP configuration.

```
Switch#show sntp
SNTP server     Version    Last Receive
2.1.0.2           1              6
```

10.3 DNSv4/v6

10.3.1 clear dynamic-host

Command: clear dynamic-host {<ip-address> | <ipv6-address> | all}

Function: Deletes the domain name entries of the specified address, or of all addresses, from the dynamic cache.

Parameters: <ip-address> is the IP address, in dotted decimal notation. **<ipv6-address>** is the IPv6 address. **all** deletes the domain name entries of all addresses from the dynamic cache.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Use this command to manually delete domain name and address entries from the dynamic cache. This is useful when a domain name entry has remained in the cache for a long time.

Example: Delete the domain name entry of address 202.108.22.5.

```
Switch# clear dynamic-host 202.108.22.5
```

10.3.2 debug dns

Command: debug dns {all | packet [send | recv] | events | relay}
no debug dns {all | packet [send | recv] | events | relay}

Function: Enables display of DNS domain name resolution debugging information. The **no** form of this command disables it.

Parameters: None.

Command Mode: Admin Mode.

Example:

```
Switch# debug dns all
Switch# ping host www.google.com
%Jan 01 00:03:13 2006 domain name www.google.com is to be parsed!
%Jan 01 00:03:13 2006 Dns query type is A!
 %Jan 01 00:03:13 2006 Connect dns server 10.1.120.241 ......
ping www.google.com [104.244.42.197]
Type ^c to abort.
Sending 5 56-byte ICMP Echos to 104.244.42.197, timeout is 2 seconds.
%Jan 01 00:03:15 2006 Host:www.google.com    Address: 104.244.42.197
.....
Success rate is 0 percent (0/5), round-trip min/avg/max = 0/0/0 ms
```

10.3.3 dns-server

Command: dns-server {<ip-address>|<ipv6-address>} [priority <value>]
no dns-server {<ip-address>|<ipv6-address>}

Function: Configures or deletes a DNS server.

Parameters: <ip-address> is the IP address, in dotted decimal notation. **<ipv6-address>** is the IPv6 address. **<value>** is the priority of the DNS server, ranging from 0 to 255. The default is 0.

Command Mode: Global Mode.

Default: Not configured.

Usage Guidelines: Use this command to configure or delete a DNS server. When dynamic domain name resolution is needed, the switch sends domain name query requests to the configured DNS servers. Up to six DNS servers can be configured. The priority is optional. If priorities are configured, the DNS servers are queried in order of priority, from highest to lowest; the switch sends the query to the server with the highest priority first. Therefore, assign the highest priority to DNS servers that respond quickly and are used frequently. If no priority is configured, DNS servers are queried in the order in which they were configured. When the switch acts as a DNS server, queries are not sent according to these priority rules; instead, requests are sent to all configured servers at the same time.

Example: Configure DNS server 10.1.120.241 with priority 200.

```
Switch(config)# dns-server 10.1.120.241 priority 200
```

10.3.4 dns lookup

Command: `dns lookup {ipv4 | ipv6} <hostname>`

Function: Performs DNS dynamic domain name resolution.

Parameters: {ipv4 | ipv6} specifies IPv4 or IPv6 address lookup. **<hostname>** is the host name to resolve, less than 63 characters.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: Use this command to look up the address of the specified host name. Both IPv4 and IPv6 addresses can be looked up. This command is used only for domain name resolution and has no other function. While the command is running, it cannot be interrupted. If many servers and domain name suffixes are configured, resolution takes longer.

Example: Look up the IPv4 address of www.google.com.

```
Switch(config)# dns lookup ipv4 www.google.com
```

10.3.5 show dns name-server

Command: `show dns name-server`

Function: Displays information about the configured DNS servers.

Parameters: None.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch# show dns name-server
DNS NAME SERVER:
Address                                  Priority
10.1.120.231                              100
10.1.180.85                               80
2001::1                                   20
```

10.3.6 show dns domain-list

Command: `show dns domain-list`

Function: Displays the configured DNS domain name suffixes.

Parameters: None.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch# show dns domain-list
DNS DOMAIN LIST:
com
```

10.3.7 show dns hosts

Command: `show dns hosts`

Function: Displays the dynamic domain name entries resolved by the switch.

Parameters: None.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch# show dns hosts
Total number of dynamic host is 2
DNS HOST LIST:
```

```
Hostname              Address                  Time to live      Type
www.google.com       104.244.42.197            168000          dynamic
www.ipv6.org          2001:6b0:1:               168060           dynamic
```

10.3.8 show dns config

Command: `show dns config`

Function: Displays the global DNS configuration of the switch.

Parameters: None.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch(config)#show dns config
ip dns server enable
ip domain-lookup enable
the maximum of dns client in cache is 3000, timeout is 5
dns client number in cache is 0
dns dynamic host in cache is 0
dns name server number is 1
dns domain-list number is 0
```

10.3.9 show dns client

Command: `show dns client`

Function: Displays the DNS client information maintained by the switch.

Parameters: None.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch(config)#show dns client
DNS REQUEST LIST:
Total number of dns request is 2
Address                                          Request Id
192.168.11.141                                    1
192.168.11.138                                    2
```

10.3.10 ip domain-lookup

Command: `ip domain-lookup`
`no ip domain-lookup`

Function: Enables or disables DNS dynamic lookup, that is, whether the switch sends dynamic DNS queries to the DNS server.

Parameters: None.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: Use this command to enable or disable DNS dynamic lookup on the switch. When it is enabled, the DNS server resolves host names and domain names to IPv4 or IPv6 addresses for client requests. When it is disabled, client applications cannot send DNS requests to the DNS server, and only static address resolution is available. Address mappings previously learned through DNS in the resolution cache become invalid after they age out.

Example: Enable DNS so that domain names can be resolved dynamically.

```
Switch(config)# ip domain-lookup
```

10.3.11 ip domain-list

Command: `ip domain-list <WORD>`
`no ip domain-list <WORD>`

Function: Configures or deletes a domain name suffix.

Parameters: <WORD> is the domain name suffix string, less than 63 characters.

Command Mode: Global Mode.

Default: None.

Usage Guidelines: Use this command to configure or delete a domain name suffix. When an incomplete domain name is entered (such as google), the switch automatically appends a suffix and then performs address resolution. Up to six domain name suffixes can be configured. The first configured suffix is appended first.

Example: Configure the domain name suffix com.

```
Switch(config)# ip domain-list com
```

10.3.12 ip dns server

Command: `ip dns server`
`no ip dns server`

Function: Enables or disables the DNS server function.

Parameters: None.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: When the DNS server function is enabled, the switch can receive DNS requests from clients and handle them by looking up locally or forwarding them to the DNS server.

Example: Enable the DNS server function of the switch.

```
Switch(config)#ip dns server
```

10.3.13 ip dns server queue maximum

Command: `ip dns server queue maximum <1-5000>`
`no ip dns server queue maximum`

Function: Configures the maximum number of client entries in the switch queue.

Parameters: <1-5000>: The maximum number of client entries, ranging from 1 to 5000.

Command Mode: Global Mode.

Default: 3000.

Usage Guidelines: When the switch receives a DNS request from a client, it caches the client information. The number of client entries in the queue cannot exceed the configured maximum; otherwise, the client request is not handled.

Example: Set the maximum number of client entries in the switch queue to 2000.

```
Switch(config)#ip dns server queue maximum 2000
```

10.3.14 ip dns server queue timeout

Command: `ip dns server queue timeout <1-100>`
`no ip dns server queue timeout`

Function: Configures the timeout for cached client information on the switch.

Parameters: <1-100>: The timeout, ranging from 1 to 100 seconds.

Command Mode: Global Mode.

Default: 5 seconds.

Usage Guidelines: When the switch receives a DNS request from a client, it caches the client information. If the client information is kept longer than the configured timeout, it is cleared.

Example: Set the timeout for cached client information on the switch to 10 seconds.

```
Switch(config)#ip dns server queue timeout 10
```

10.4 Summer Time

10.4.1 clock summer-time absolute

Command: clock summer-time <word> absolute <HH:MM> <YYYY.MM.DD> <HH:MM> <YYYY.MM.DD> [<offset>]
no clock summer-time

Function: Configures an absolute summer time range; time within this range is summer time. The **no** form of this command deletes the configuration.

Parameters: <word> is the name of the summer time zone. **<HH:MM>** is the start time, in the format hour (0 to 23):minute (0 to 59). **<YYYY.MM.DD>** is the start date, in the format year (2001 to 2037).month (1 to 12).day (1 to 31). The second **<HH:MM>** is the end time, and the second **<YYYY.MM.DD>** is the end date, in the same formats. **<offset>** is the time offset in minutes, ranging from 1 to 1440. The default is 60 minutes.

Default: No summer time range is configured.

Command Mode: Global Mode.

Usage Guidelines: This command sets the absolute start and end times of summer time. When the system time reaches the start of summer time, the clock is advanced by **<offset>** and summer time begins. When the system time reaches the end of summer time, **<offset>** is subtracted from the clock and summer time ends. The end time must be later than the start time.

Example: Configure summer time named aaa from 12:10 on April 6, 2010, to 12:10 on August 6, 2010, with an offset of 70 minutes.

```
Switch(config)#clock summer-time aaa absolute 12:10 2010.4.6 12:10 2010.8.6
70
```

10.4.2 clock summer-time recurring

Command: clock summer-time <word> recurring <HH:MM> <MM.DD> <HH:MM> <MM.DD> [<offset>]
no clock summer-time

Function: Configures a recurring summer time range; time within this range is summer time.

Parameters: <word> is the name of the summer time zone. **<HH:MM>** is the start time, in the format hour (0 to 23):minute (0 to 59). **<MM.DD>** is the start date, in the format month (1 to 12).day (1 to 31). The second **<HH:MM>** is the end time, and the second **<MM.DD>** is the end date, in the same formats. **<offset>** is the time offset in minutes, ranging from 1 to 1440. The default is 60 minutes.

Default: No summer time range is configured.

Command Mode: Global Mode.

Usage Guidelines: This command sets the start and end times of recurring summer time. When the system time reaches the start of summer time, the clock is advanced by **<offset>** and summer time begins. When the system time reaches the end of summer time, **<offset>** is subtracted from the clock and summer time ends. Recurring summer time does not depend on the year; the clock

changes at the start and end times every year. Summer time in the Southern Hemisphere is supported.

Example: Configure recurring summer time named aaa from 12:10 on April 6 to 12:10 on August 6 every year, with an offset of 70 minutes.

```
Switch(config)# clock summer-time aaa recurring 12:10 4.6 12:10 8.6 70
```

10.4.3 clock summer-time recurring

Command: clock summer-time <word> recurring <HH:MM> <week> <day> <month> < HH:MM > <week> <day> <month> [<offset>]
no clock summer-time

Function: Configures a recurring summer time range by week and day; time within this range is summer time.

Parameters: <word> is the name of the summer time zone. **<HH:MM>** is the start time, in the format hour (0 to 23):minute (0 to 59). **<week>** is the week of the month: 1 to 4, first, or last. **<day>** is the day of the week: Sun, Mon, Tue, Wed, Thu, Fri, or Sat. **<month>** is the month: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, or Dec. The second set of **<HH:MM>**, **<week>**, **<day>**, and **<month>** specifies the end, in the same formats. **<offset>** is the time offset in minutes, ranging from 1 to 1440. The default is 60 minutes.

Default: No summer time range is configured.

Command Mode: Global Mode.

Usage Guidelines: This command sets the start and end times of recurring summer time flexibly. When the system time reaches the start of summer time, the clock is advanced by **<offset>** and summer time begins. When the system time reaches the end of summer time, **<offset>** is subtracted from the clock and summer time ends. Recurring summer time does not depend on the year; the clock changes at the start and end times every year. Summer time in the Southern Hemisphere is supported.

Example: Configure recurring summer time named aaa from 12:10 on the first Monday of April to 12:10 on the last Saturday of August every year, with an offset of 70 minutes.

```
Switch(config)#clock summer-time aaa recurring 12:10 1 mon apr 12:10 last sat
aug 70
```

Chapter 11 Commands for Virtualization

11.1 VSF

11.1.1 Basic VSF

11.1.1.1 switch convert mode

Command: `switch convert mode ( stand-alone | vsf )`

Function: Switches the device from stand-alone mode to VSF mode, or from VSF mode to stand-alone mode.

Parameters: stand-alone: Stand-alone mode. **vsf**: VSF mode.

Default: The device determines which mode to enter from the VSF configuration file vsf.cfg.

Command Mode: Global Mode.

Operation Mode: Independent Operation Mode, VSF Operation Mode.

VSF Role: VSF Master.

Usage Guidelines: The device supports two modes: stand-alone mode and VSF mode. In stand-alone mode, the device operates alone. In VSF mode, the device can form a VSF with other devices. Use this command to switch between the two modes.

Example: Switch the device from stand-alone mode to VSF mode.

```
Switch#config
Switch(config)#switch convert mode vsf
```

11.1.1.2 write

Command: `write`

Function: In stand-alone mode, the **write** command saves the current running configuration and writes the current VSF-related configuration to vsf.cfg. In VSF mode, the **write** command saves the current running configuration to vsf_startup.cfg and the current VSF-related configuration to vsf.cfg.

Parameters: None.

Default: The running configuration and VSF-related configuration are not saved.

Command Mode: Admin Mode.

Operation Mode: Independent Operation Mode, VSF Operation Mode.

VSF Role: VSF Master.

Usage Guidelines: When saving the configuration, a device with the VSF function writes the current configuration to startup.cfg and vsf.cfg respectively.

Example: Save the configuration.

```
Switch#write
```

11.1.1.3 vsf port-group

Command: `vsf port-group <port-number>`
`no vsf port-group <port-number>`

Function: Configures a logical VSF port. The **no** form of this command deletes the VSF port.

Parameters: <port-number>: The logical VSF port number, 1 or 2.

Default: Not configured.

Command Mode: Global Mode.

Operation Mode: Independent Operation Mode, VSF Operation Mode.

VSF Role: VSF Master.

Usage Guidelines: This command configures a logical VSF port. Up to two VSF port groups can be configured on a device: vsf port-group 1 and vsf port-group 2.

Example: Configure a logical VSF port.

```
Switch(config)#vsf port-group 1
```

11.1.1.4 vsf port-group interface ethernet

Command: `vsf port-group interface Ethernet <interface-list>`
`no vsf port-group interface Ethernet <interface-list>`

Function: After a logical VSF port is created, binds physical ports to it in VSF Port Mode. The **no** form of this command removes the binding.

Parameters: <interface-list>: The physical port numbers.

Default: No physical port is bound.

Command Mode: VSF Port Mode.

Operation Mode: Independent Operation Mode, VSF Operation Mode.

VSF Role: VSF Master.

Usage Guidelines: A VSF port group can bind up to eight physical ports, and the mode of the ports in the group is **on**. If more than eight ports are bound, the user is notified that the binding is not allowed. The bound physical ports do not need to be contiguous. Currently, only 10G ports can be bound to a logical VSF port.

Example: Create a logical VSF port, enter VSF Port Mode, and bind physical port 1/0/1 to the logical VSF port.

```
Switch(config)# vsf port-group 1
Switch(config)# vsf port-group interface ethernet 1/0/1
```

11.1.1.5 vsf domain

Command: `vsf domain <domain-id>`
`no vsf domain`

Function: Configures the VSF domain of the device. The **no** form of this command restores the default of 1. In stand-alone mode, the VSF domain configuration takes effect immediately. In VSF mode, the new configuration appears in the running configuration but takes effect only after it is saved and the device restarts.

Parameters: <domain-id>: The domain number, ranging from 1 to 32.

Default: The device is in domain 1.

Command Mode: Global Mode.

Operation Mode: Independent Operation Mode, VSF Operation Mode.

VSF Role: VSF Master.

Usage Guidelines: A domain is a logical concept. Devices connected through VSF links form a VSF, and the set of these member devices is a VSF domain. To suit various network applications, multiple VSFs can be deployed in the same network, and the domain number distinguishes them. Only devices in the same domain can form a VSF; devices or VSF groups in different domains cannot. Domain number conflicts are checked before the VSF is formed. The default domain number is 1.

Note: This command is not supported by the switch.

11.1.1.6 vsf member

Command: `vsf member <member-id>`
`no vsf member <member-id>`

Function: Configures the VSF member number of the device. The **no** form of this command deletes the member number.

Parameters: <member-id>: The member number, ranging from 1 to 16.

Default: The device has no member number.

Command Mode: Global Mode.

Operation Mode: Independent Operation Mode.

Usage Guidelines: The member number identifies each device; each device in a VSF group has a unique member number. Configure the member number before entering VSF mode. If the command is configured multiple times, the last configuration takes effect. There is no member number in the initial state. After the device enters VSF mode, the port numbering format changes according to the member number. If member numbers conflict, the VSF cannot be formed.

Note: This command is not supported by the switch.

11.1.1.7 vsf non-wait port-inactive

Command: `vsf non-wait port-inactive`
`no vsf non-wait port-inactive`

Function: Enables fast detection of VSF link status changes to discover VSF splits. The **no** form of this command restores the default detection method.

Parameters: None.

Default: Fast detection of VSF link status is not configured.

Command Mode: Global Mode.

Operation Mode: VSF Operation Mode.

Usage Guidelines: After this command is configured, the system immediately receives and confirms VSF link status changes and detects VSF topology changes. The command takes effect immediately. Use this command when the physical VSF links are stable.

Example: Enable fast detection of VSF link status changes.

```
Switch(config)# vsf non-wait port-inactive
```

11.1.1.8 vsf priority

Command: `vsf priority <priority>`
`no vsf priority`

Function: Configures the priority of a VSF member in the VSF group. The **no** form of this command restores the default of 1. In stand-alone mode, the member priority takes effect immediately. In VSF mode, the new configuration appears in the running configuration but takes effect only after it is saved and the device restarts.

Parameters: <priority>: The priority of the VSF member, ranging from 1 to 32.

Default: 1.

Command Mode: Global Mode.

Operation Mode: Independent Operation Mode.VSF Operation Mode.

VSF Role: VSF Master.

Usage Guidelines: Configure the member priority in stand-alone mode. The member priority is used in role election; a larger value means a higher priority. A device with a higher priority is more likely to

be elected master. Configure different priorities on different devices to designate one device as the VSF master.

Note: This command is not supported by the switch.

11.1.1.9 vsf auto-merge enable

Command: **`vsf auto-merge enable`**
`no vsf auto-merge enable`

Function: Enables automatic merging of VSF groups. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guidelines: When two VSF groups are correctly connected through their VSF ports and there is no VSF domain or member ID conflict, the port coming up, VSF creation, and binding trigger the two VSF groups to merge automatically. During the merge, priorities and member IDs are compared; the VSF group that loses the election restarts and joins the VSF group that wins.

Note: This command is not supported by the switch.

11.1.1.10 vsf member description

Command: **`vsf member <member-id> description <text>`**
`no vsf member <member-id> description`

Function: Configures a description for a VSF member. The description is written only to the master configuration. The **no** form of this command deletes the description.

Parameters: **<member-id>**: The VSF member number. **<text>**: The description entered by the user.

Default: No description is configured.

Command Mode: Global Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guidelines: In VSF mode, descriptions make management easier; for example, they help distinguish VSFs when a network contains more than one VSF or when a VSF has split.

Note: This command is not supported by the switch.

11.1.1.11 vsf link delay

Command: **`vsf link delay<interval>`**
`no vsf link delay`

Function: Configures the delay before a VSF link down event is reported, to prevent the VSF from splitting and merging because of short-term link changes. The **no** form of this command restores the default delay.

Parameters: **<interval>**: The delay before a VSF link down event is reported. The default is 0, which means the event is reported immediately.

Default: 0.

Command Mode: Global Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guidelines: After the VSF link delay is configured, when a VSF link goes from up to down, the port does not report the change to the system immediately. If the VSF link is still down after the configured time, the port reports the change and the system acts on it. When a VSF link goes from down to up, the link layer reports the change to the system immediately. The command takes effect immediately.

Note: This command is not supported by the switch.

11.1.1.12 vsf mac-address persistent

Command: **`vsf mac-address persistent <timer | always>`**
`no vsf mac-address persistent`

Function: Configures how long the VSF bridge MAC address is retained after the VSF splits. The **no** form of this command deletes the retention time.

Parameters: **<timer>**: Retains the VSF bridge MAC address for 6 minutes. After the master leaves the VSF, the VSF bridge MAC address stays unchanged for 6 minutes; if the master does not return within 6 minutes, the bridge MAC address of the newly elected master becomes the VSF bridge MAC address. **<always>**: Retains the bridge MAC address permanently; the VSF bridge MAC address never changes, whether or not the master leaves.

Default: No bridge MAC retention time is configured.

Command Mode: Global Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guidelines: A VSF communicates with other devices as a single virtual device and has a unique bridge MAC address, the VSF bridge MAC address. Usually, the bridge MAC address of the master becomes the VSF bridge MAC address. A bridge MAC address conflict disrupts communication, and a bridge MAC address change interrupts traffic. Configure the bridge MAC retention time so that, when a split occurs, the user decides whether and for how long the VSF bridge MAC address is retained. With the timer, after the master leaves the VSF, the VSF bridge MAC address stays unchanged for 6 minutes; if the master does not return within 6 minutes, the CPU MAC address of the newly elected master becomes the VSF bridge MAC address. With **always**, the VSF does not restart when the master leaves and keeps using the original CPU MAC address as the VSF MAC address. If the VSF restarts, the CPU MAC address of the newly elected master is used. The command does not persist after a restart and must be configured again.

Note: This command is not supported by the switch.

11.1.2 Configuration and Debugging of VSF Conflict Detection

11.1.2.1 vsf mad lacp enable

Command: **`vsf mad lacp enable`**
`no vsf mad lacp enable`

Function: Enables LACP MAD detection on the specified port channel. The **no** form of this command disables LACP MAD on the port channel.

Parameters: None.

Default: Disabled.

Command Mode: Port-Channel Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guidelines: This command can be used only in VSF mode. It configures the specified port channel as an LACP MAD detection group; the group members send MAD TLV messages.

Example: Enable LACP MAD detection on port-channel 1.

```
Switch(config)#interface port-channel 1
Switch(config-if-port-channel1)# vsf mad lacp enable
```

Note: This command is not supported by the switch.

11.1.2.2 vsf mad bfd enable

Command: **`vsf mad bfd enable`**
`no vsf mad bfd enable`

Function: Enables BFD MAD detection on the interface. The **no** form of this command disables BFD MAD detection on the interface.

Parameters: None.

Default: Disabled.

Command Mode: Interface Mode.

Operation Mode: VSF Operation Mode and Network Management Port Configuration Mode.

VSF Role: VSF Master.

Usage Guidelines: This command can be used only in VSF mode. It enables BFD MAD detection on the specified interface.

Example: Enable BFD MAD detection on interface VLAN 2.

```
Switch(config)# interface vlan 2
Switch(config-if-vlan2)# vsf mad bfd enable
```

11.1.2.3 vsf mad ip address

Command: **`vsf mad ip address <ip-address> <ip-mask> member <member-number>`**
`no vsf mad ip address <ip-address> <ip-mask> member <member-number>`

Function: Specifies the member device for a BFD MAD session.

Parameters: **<ip-address>**: The IP address. **<ip-mask>**: The subnet mask. **<member-number>**: The member device number, ranging from 1 to 16.

Default: No MAD address is configured.

Command Mode: Interface Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guidelines: This command can be used only in VSF mode. It configures the address used by the member device to establish a BFD session with the peer address.

Example: Create BFD MAD sessions for member devices on interface VLAN 2.

```
Switch(config)# interface vlan 2
Switch(config-if-vlan2)# vsf mad ip address 2.1.1.1 255.255.255.0 member 1
Switch(config-if-vlan2)# vsf mad ip address 2.1.1.2 255.255.255.0 member 2
```

11.1.2.4 vsf mad exclude

Command: **`vsf mad exclude`**
`no vsf mad exclude`

Function: Configures a port that is not shut down when the device enters the Recovery state, so that it continues forwarding. The **no** form of this command deletes the MAD reserved port configuration.

Parameters: None.

Default: No MAD reserved port is configured.

Command Mode: Port Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guidelines: When a VSF splits, the network contains two devices with the same global configuration, which can disrupt the network. To prevent this, the system performs multi-active detection (MAD); only one device remains Active and the others enter the Recovery state, in which all their service ports are shut down. Use this command to specify ports that are not shut down.

Example: Configure port 2/1/4 as a MAD reserved port.

```
Switch(config)# inte e 2/1/4
Switch (config-if-ethernet2/1/4)#vsf mad exclude
```

11.1.2.5 vsf mad restore

Command: `vsf mad restore`

Function: Restores a VSF in the Recovery state to normal operation.

Parameters: None.

Default: None.

Command Mode: Global Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guidelines: When a VSF link fails, an active conflict occurs and the original VSF splits into two active VSFs. To prevent conflicts in the network, the VSF system uses multi-active detection to keep one VSF Active (it continues working) and put the other VSFs in the Recovery state (they cannot process service traffic). If the Active VSF fails, use this command to restore the VSF in the Recovery state to normal operation.

Example: Restore the VSF in the Recovery state to normal operation.

```
Switch(config)#vsf mad restore
```

11.1.2.6 show mad config

Command: `show mad config`

Function: Displays the VSF MAD configuration, including the LACP MAD and BFD MAD configuration.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guidelines: None.

11.1.3 VSF Debugging

11.1.3.1 show running-config

Command: `show running-config`

Function: Displays the entire current configuration.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Operation Mode: Independent Operation Mode.VSF Operation Mode.

VSF Role: VSF Master.

Usage Guidelines: When VSF is enabled, this command displays the VSF-related configuration together at the top of the output.

Example:

```
Switch#show running-config
```

11.1.3.2 show vsf

Command: `show vsf`

Function: Displays information about all devices in the VSF, including the VSF master, backup master, VSF CPU MAC address, VSF bridge MAC address, device descriptions, member priorities, version consistency check, bridge MAC address retention configuration, whether auto-merge is enabled, and VSF domain.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guidelines: This command can be used only in VSF mode. Role election information is obtained through the VSF protocol, and configuration information such as the bridge MAC and CPU MAC addresses is obtained by reading the vsf.cfg file of each device.

Example:

```
Switch# sho vsf
Switch   SlotID   Role   Priority   CPU-Mac             Description
------------------------------------------------------------------------------
2        M1       M      1          00-03-0f-0f-66-b4   (null)
2        7         S      1          00-03-0f-0f-66-b4   (null)
The Bridge Mac of the VSF is: 00-03-0f-0f-66-b4
Auto Merge: yes
Mac Persistent: off
Domain ID: 1
```

11.1.3.3 show vsf topology

Command: `show vsf topology`

Function: Displays the current VSF topology.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guidelines: A VSF merge or a member leaving the VSF triggers protocol operation and a new topology calculation. Use this command to view the current topology.

Example:

```
Switch# show vsf topology
Switch    VSF-Port1            Neighbor   VSF-Port2         Neighbor
2     Ethernet2/7/3(inactive)  --         --                --
```

11.1.3.4 show vsf-config

Command: `show vsf-config`

Function: Displays the VSF configuration in order of device, including member ID, member priority, and VSF port information of each member.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guidelines: When a stand-alone VSF device forms, it collects its own VSF configuration. If the VSF contains several devices, it sends collection requests to the other devices and collects the configuration of the entire VSF.

Example:

```
Switch# show vsf config
MemberID  Priority      VSF-Port1         VSF-Port2
2         1           Ethernet2/7/3       --
```

11.1.3.5 show mad config

Command: `show mad config`

Function: Displays the current VSF MAD detection configuration.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guidelines: This command can be used only in VSF mode. It displays whether LACP MAD and BFD MAD are enabled and on which ports.

Example:

```
Switch# show mad config
Current lacp MAD status: Disable
Current bfd MAD status: Detecting
Reserved ports:
Reserved ports(defaults):
 interface Ethernet2/7/3
MAD lacp enabled aggregation port:
MAD BFD enabled interface:
 Interface Vlan10
 vsf mad ip address 10.1.1.1 255.255.255.0 member 1
 vsf mad ip address 10.1.1.2 255.255.255.0 member 2
```

Output	Description
Current lacp MAD status	Current status of LACP MAD
Current bfd MAD status	Current status of BFD MAD
Reserved ports	Reserved ports configured by the user
Reserved ports(defaults)	Default reserved ports (no configuration needed)
MAD lacp enabled aggregation port	Aggregation ports with LACP MAD enabled
MAD BFD enabled interface	Interfaces with BFD MAD enabled

11.1.3.6 show vsf cpu-database all-member brief-information

Command: show vsf cpu-database all-member brief-information

Function: Displays brief information about all members in the CPU database.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guidelines: Displays brief information about all members in the CPU database.

Example:

```
Switch# show vsf cpu-database all-member brief-information
Vsf cpu database include 1 member:
Member 2 : cpu key:00-03-0f-0f-66-b4, PRI:1
Master is : 2, Standby is : 0
```

11.1.3.7 show vsf cpu-database member basic-information

Command: show vsf cpu-database [member <1-16>| basic information]

Function: Displays the CPU database basic information for the entire VSF or for a specified member.

Parameters: member <1-16>: The VSF member ID.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guidelines: Displays the CPU database basic information for the entire VSF or for a specified member.

Example:

```
Switch# show vsf cpu-database member 2 basic-information
Vsf cpu database member 2 basic information:
Key: 00-03-0f-0f-66-b4
CPU-MAC: 00-03-0f-0f-66-b4
Member ID: 2
Domain ID: 1
Sequence Num: 4
Master Prioriy: 1
Units Num: 1
Dest unit: 1
Dest port: 0
Unit prefer module id: 2
Unit require module id num: 1
Vsf port num: 1
Flags: 131072
Vsf port index 1:
     Unit: 0
     port: 1
     Weight: 0
     Bflag: 1
```

11.1.3.8 show vsf cpu-database member running-information

Command: show vsf cpu-database [member <1-16>| running-information]

Function: Displays the CPU database running information for the entire VSF or for a specified member.

Parameters: member <1-16>: The VSF member ID.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guidelines: Displays the CPU database running information for the entire VSF or for a specified member.

Example:

```
Switch# show vsf cpu-database member 1 running-information
%Member 1 not exist in the cpu-database!
Switch# show vsf cpu-database member 2 running-information
Vsf cpu database member 2 running information:
Flags: 1
Tx unit: 0
Tx port: 0
Dest module: 2
Dest port: 0
Module ID: 2
Topo index:  0
Vsf port index 1 link info:
Flags: 0
Tx cpu key:
Tx port-group: 0
Rx cpu key:
Rx port-group: 0
```

11.1.3.9 show vsf cpu-database member port-information

Command: show vsf cpu-database [member <1-16>| port-information]

Function: Displays the CPU database VSF port information for the entire VSF or for a specified member.

Parameters: member <1-16>: The VSF member ID.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guidelines: Displays the CPU database VSF port information for the entire VSF or for a specified member.

Example:

```
Switch# show vsf cpu-database member 2 port-information
Vsf cpu database member 2 port information:
Vsf port index 1:
     Unit: 0
     port: 1
     Weight: 0
     Bflag: 1
```

11.1.3.10 show vsf cpu-database member port-link-information

Command: show vsf cpu-database [member <1-16>| port-link-information]

Function: Displays the CPU database VSF port link information for the entire VSF or for a specified member.

Parameters: member <1-16>: The VSF member ID.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Operation Mode: VSF Operation Mode.

VSF Role: VSF Master.

Usage Guidelines: None.

Example:

```
Switch# show vsf cpu-database port-link-information
Vsf cpu database member 1 include 2 vsf port:
Vsf port index 1 link info:
Flags:1
Tx cpu key:00-01-05-11-11-11
Tx stk idx:1
Rx cpu key: 00-01-05-11-11-11
Rx cpu key:1
Vsf port index 2 link info:
Flags:1
Tx cpu key:00-01-05-11-11-12
Tx stk idx:2
Rx cpu key: 00-01-05-11-11-12
Rx cpu key:2
```

11.1.3.11 show slot

Command: show [member <member-id>] slot <slot-id>

Function: Displays basic information about each chip.

Parameters: <member-id> is the member device number in VSF mode, ranging from 1 to 16. **<slot-id>** is the number of the slot in which the chip resides; for box devices, the slot number is always 1.

Default: If no member ID and slot ID are specified, information about all chips is displayed.

Command Mode: Admin Mode.

Example:

```
Switch#show member 13 slot 1
--------------------member :13--------------------
Inserted : YES
Module type : Switch
Work mode : STANDBY MASTER
Work state : RUNNING
Software package version : 7.0.3.0(R0075.0011)
Bootrom version : 7.2.2
CPLD version : N/A
Hardware version : 1.0.1
Part number : N110900062
Manufacture date : 2011/03/10
Temperature : 39C/102F
Uptime : 0 weeks, 0 days, 1 hours, 37 minutes
```

11.1.3.12 debug vsf packet detail <alive | all | config | member-infor | probe | routing | topo>

Command: **debug vsf packet detail <alive | all | config | member-infor | probe | routing | topo>**
no debug vsf packet detail <alive | all | config | member-infor | probe | r routing | topo>

Function: Enables display of VSF protocol packets of various types. The **no** form of this command disables it.

Parameters: **alive**: Keepalive packets. **all**: All VSF protocol packets. **config**: Configuration information packets, exchanged in the configuration stage, in which VSF members obtain the information required for master election and elect the master and standby master. **member-infor**: Member information packets. **probe**: VSF member detection packets, used to detect the connection information of all VSF ports. **routing**: VSF member information distribution packets, which carry the local VSF port information, the required module IDs, the number of chips, the master election priority, CPU database status, and the chip and port numbers through which this CPU is reached. **topo**: Topology analysis packets. In the topology analysis stage, the master calculates a loop-free network from the topology information, assigns module IDs to all members, calculates the relationship between each member VSF port and destination module ID, and distributes the results to each member.

Default: Disabled.

Command Mode: Admin Mode.

VSF Role: VSF Master, member and line card.

Usage Guidelines: A VSF group goes through discovery and topology analysis stages while forming, and the device is in a different state in each stage. Discovery consists of the probe, routing, and config sub-stages. Use this command to view the details of the protocol packets in each stage.

11.1.3.13 debug vsf packet

Command: **debug vsf packet <all | receive | send> vsf-port <vsf-port-number>**
no debug vsf packet <all | receive | send> vsf-port <vsf-port-number>

Function: Enables VSF packet debugging. The **no** form of this command disables it.

Parameters: **receive**: Debugs received VSF packets. **send**: Debugs sent VSF packets. **all**: Debugs both received and sent VSF packets. **<vsf-port-number>**: The VSF port number.

Default: Disabled.

Command Mode: Admin Mode.

VSF Role: VSF Master, Member and Slave.

Usage Guidelines: When VSF packet debugging is enabled, received VSF protocol messages are displayed.

11.1.3.14 debug vsf event

Command: **debug vsf event**
no debug vsf event

Function: Enables VSF event debugging. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

VSF Role: VSF Master, Member and Slave.

Usage Guidelines: When VSF event debugging is enabled, feedback is displayed for the defined events in all VSF stages.

11.1.3.15 debug vsf error

Command: **`debug vsf error`**
`no debug vsf error`

Function: Enables VSF error debugging. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

VSF Role: VSF Master, Member and Slave.

Usage Guidelines: When this debugging is enabled, error messages from all VSF stages are displayed.

Chapter 12 Commands for DataCenter

12.1 Commands for MC-LAG

12.1.1 evpn nve mac-address

Command: **`evpn nve mac-address FF-FF-FF-FF-FF-FF`**
`no evpn nve mac-address`

Function: Configures the VTEP MAC address globally.

Parameters: **FF-FF-FF-FF-FF-FF**: The VTEP MAC address.

Command Mode: Global Mode.

Default: The CPU MAC address of the MC-LAG master.

Usage Guidelines: When a VXLAN distributed gateway is built with BGP EVPN and MC-LAG is used for VXLAN dual-homing access, configure the same VTEP MAC address on the two dual-homing devices so that the gateway forwards traffic normally in the VXLAN network. The **no** form of this command restores the default VTEP MAC address.

Example: Set the VTEP MAC address to 00-01-02-03-04-05.

```
Switch(config)#evpn nve mac-address 00-01-02-03-04-05
```

12.1.2 mac-address

Command: **`mac-address XX-XX-XX-XX-XX-XX`**
`no mac-address`

Function: Configures the MAC address of the gateway interface.

Parameters: **XX-XX-XX-XX-XX-XX**: The MAC address of the gateway interface.

Command Mode: VLAN Interface Mode and NVI Interface Mode.

Default: None.

Usage Guidelines: When MC-LAG devices act as a Layer 3 gateway, configure the same MAC address on the gateway interfaces of the two devices in the same network segment. The **no** form of this command deletes the configured MAC address.

Example: Set the MAC address of gateway interface VLAN 10 to 02-02-02-02-02-02.

```
switch(config)#interface vlan 10
switch(config-if-vlan10)#mac-address 02-02-02-02-02-02
```

12.1.3 mclag

Command: **`[no] mclag`**

Function: Enters MC-LAG Mode.

Parameters: None.

Command Mode: Global Mode.

Default: None.

Usage Guidelines: Run **mclag** to enter MC-LAG Mode. The **no** form of this command deletes the configuration in MC-LAG Mode and exits the mode.

Example: Enter MC-LAG Mode.

```
switch(config)#mclag
switch(config-mclag)#
```

12.1.4 mclag domain-id

Command: `mclag domain-id <1-128>`
`no mclag domain-id`

Function: Configures the MC-LAG domain ID.

Parameters: <1-128>: The domain ID, ranging from 1 to 128.

Command Mode: MC-LAG Mode.

Default: None.

Usage Guidelines: The two MC-LAG devices must use the same domain ID. The **no** form of this command deletes the domain ID.

Example: Set the MC-LAG domain ID to 10.

```
Switch(config-mclag)#mclag domain-id 10
```

12.1.5 mclag priority

Command: `mclag priority <1-256>`
`no mclag priority`

Function: Configures the MC-LAG domain priority.

Parameters: <1-256>: The domain priority, ranging from 1 to 256.

Command Mode: MC-LAG Mode.

Default: 128.

Usage Guidelines: This command configures the MC-LAG domain priority. A smaller value means a higher priority. The device with the higher priority becomes the MC-LAG master. The **no** form of this command restores the default priority.

Example: Set the MC-LAG domain priority to 100.

```
switch(config-mclag)#mclag priority 100
```

12.1.6 mclag enable

Command: `[no] mclag enable`

Function: Enables MC-LAG.

Parameters: None.

Command Mode: MC-LAG Mode.

Default: None.

Usage Guidelines: This command enables MC-LAG. The **no** form of this command disables MC-LAG.

Example: Enable MC-LAG.

```
switch(config-mclag)#mclag enable
```

12.1.7 mclag group

Command: `[no] mclag group`

Function: Adds a port group to the MC-LAG group.

Parameters: None.

Command Mode: Port-Channel Mode.

Default: None.

Usage Guidelines: This command adds a port group to the MC-LAG group. The **no** form of this command removes the port group from the MC-LAG group.

Example: Add port group 10 to the MC-LAG group.

```
switch(config-if-port-channel10)#mclag group
```

12.1.8 mclag local-ip

Command: **`mclag local-ip A.B.C.D`**
`no mclag local-ip`

Function: Configures the IP address of the local Layer 3 interface of the MC-LAG control link.

Parameters: **A.B.C.D**: The IP address.

Command Mode: MC-LAG Mode.

Default: None.

Usage Guidelines: This command configures the IP address of the local Layer 3 interface of the MC-LAG control link. The **no** form of this command removes the local IP address.

Example: Set the IP address of the local Layer 3 interface of the MC-LAG control link to 20.4.4.4.

```
switch(config-mclag)#mclag local-ip 20.4.4.4
```

12.1.9 mclag peer-ip

Command: **`mclag peer-ip A.B.C.D`**
`no mclag peer-ip`

Function: Configures the IP address of the peer Layer 3 interface of the MC-LAG control link.

Parameters: **A.B.C.D**: The IP address.

Command Mode: MC-LAG Mode.

Default: None.

Usage Guidelines: This command configures the IP address of the peer Layer 3 interface of the MC-LAG control link. The **no** form of this command removes the peer IP address.

Example: Set the IP address of the peer Layer 3 interface of the MC-LAG control link to 20.2.2.2.

```
switch(config-mclag)#mclag peer-ip 20.2.2.2
```

12.1.10 ip address

Command: **`ip address <ipaddress> <mask> [secondary] [mc-lag]`**
`no ip address <ipaddress> <mask> [secondary] [mc-lag]`

Function: Configures an independent IPv4 address for an MC-LAG Layer 3 gateway.

Parameters: **<ipaddress>**: The IP address, in dotted decimal notation. **<mask>**: The subnet mask. **[secondary]**: Specifies that the IP address is a secondary IP address. **[mc-lag]**: Specifies that the secondary address is the independent external IPv4 address of the MC-LAG Layer 3 gateway.

Command Mode: VLAN Interface Mode.

Default: None.

Usage Guidelines: Only one MC-LAG IP address can be configured on a VLAN interface. The MC-LAG secondary IP address must be in the same network segment as the primary IP address. The **no** form of this command removes the configuration.

Example: Set the independent external MC-LAG IPv4 address of the VLAN 10 interface to 10.10.1.3.

```
Switch(config-if-vlan10)#ip address 10.10.1.3 255.255.255.0 secondary mclag
```

12.1.11 ipv6 address

Command: `ipv6 address <ipv6address | prefix-length> [eui-64] [mc-lag]`
`no ipv6 address <ipv6address | prefix-length> [eui-64] [mc-lag]`

Function: Configures an independent IPv6 address for an MC-LAG Layer 3 gateway.

Parameters: <ipv6-address> is the IPv6 address prefix. **<prefix-length>** is the prefix length, ranging from 3 to 128. **eui-64** specifies that the IPv6 address is generated automatically from the EUI-64 interface identifier. **[mc-lag]** specifies that the address is the independent external IPv6 address of the MC-LAG Layer 3 gateway.

Command Mode: VLAN Interface Mode.

Default: None.

Usage Guidelines: Only one MC-LAG IPv6 global unicast address and one MC-LAG link-local address can be configured on a VLAN interface. The MC-LAG IPv6 address must be in the same network segment as one of the other IPv6 addresses of the interface. The **no** form of this command removes the configuration.

Example: Set the independent external MC-LAG IPv6 unicast address of the VLAN 10 interface to 2022::3.

```
Switch(config-if-vlan10)#ipv6 address 2022::3/64 mclag
```

Set the independent external MC-LAG IPv6 link-local address of the VLAN 10 interface to fe80::3:

```
Switch(config-if-vlan10)#ipv6 address fe80::3/64 mclag
```

12.1.12 mclag dad link

Command: `mclag dad link local <X.X.X.X> peer < X.X.X.X >`
`no mclag dad link local <X.X.X.X> peer < X.X.X.X >`

Function: Configures the local interface IP address of the dual-active detection link and the IP address of the peer device.

Parameters: local <X.X.X.X>: The local interface IP address. **peer <X.X.X.X>**: The IP address of the peer device.

Command Mode: MC-LAG Mode.

Default: None.

Usage Guidelines: Dual-active detection requires that the peer address be reachable by routing.

Example: Set the local interface IP address of the dual-active detection link to 24.24.1.1 and the peer device IP address to 24.24.1.2.

```
Switch(config-mclag)#mclag dad link local 24.24.1.1 peer 24.24.1.2
```

12.1.13 error-down exclude

Command: `error-down exclude`
`no error-down exclude`

Function: Excludes the local physical port or port group from error-down.

Parameters: error-down: Disables the ports of the slave device when MC-LAG detects dual-active. **exclude**: Excludes this port.

Command Mode: Port Mode.

Default: None.

Usage Guidelines: Ports on the slave device configured with **error-down exclude** are not placed in the error-down state when MC-LAG detects dual-active.

Example: Exclude port Ethernet 1/0/1 from error-down.

```
Switch(config-if-ethernet1/0/1)#error-down exclude
```

12.1.14 mclag up-delay

Command: `mclag up-delay <interval>`
`no mc-lag up-delay <interval>`

Function: Configures the delay before MC-LAG ports come up.

Parameters: up-delay: The delay before MC-LAG ports come up. **<interval>**: The delay, in seconds.

Command Mode: MC-LAG Mode.

Default: 120 seconds.

Usage Guidelines: For recovery from control link failures, configure the delay before MC-LAG ports come up to improve failback performance.

Example: Set the MC-LAG up-delay to 60 seconds.

```
Switch(config-mclag)#mclag up-delay 60
```

12.1.15 mclag probe-interval

Command: `mclag probe-interval <interval>`
`no mclag probe-interval <interval>`

Function: Configures the MC-LAG probe interval.

Parameters: probe-interval: The interval for sending MC-LAG keepalive packets. **<interval>**: The interval, ranging from 2 to 90 seconds.

Command Mode: MC-LAG Mode.

Default: 60 seconds.

Usage Guidelines: This command configures the MC-LAG probe interval. If no echo or control packet is received within two probe intervals, MC-LAG changes to the INACTIVE state.

Example: Set the MC-LAG probe interval to 30 seconds.

```
Switch(config-mclag)#mclag probe-interval 30
```

12.1.16 show mclag

Command: `show mclag`

Function: Displays MC-LAG configuration and status information.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: None.

Example: Display MC-LAG configuration and status information.

```
Switch#show mclag
mclag domain_id  : 10
mclag priority     : 128
mclag local system_id  : 90-3c-b3-95-0e-d7
mclag peer system_id  : 90-3c-b3-95-10-eb
mclag domain state  : MDS_READY
mclag ctrlink state  : MCLAG_CTL_ACTIVE
mclag tunlink state  : MCLAG_TUN_UP
mclag master    : LOCAL
```

12.1.17 show mclag group

Command: `show mclag group (<1-128> | )`

Function: Displays MC-LAG group configuration and status information.

Parameters: <1-128>: The group ID, ranging from 1 to 128.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: None.

Example: Display MC-LAG group configuration and status information.

```
Switch#show mclag group
*********mclag group info   :*********
group id:1
group state:ACTIVE
local link num:1
portname              status
Ethernet1/0/21         aggregate
peer link num:1
peer-portname         status
Ethernet1/0/21         aggregate
```

12.1.18 switchport mclag data link

Command: `[no] switchport mclag data link`

Function: Configures the local MC-LAG data link port.

Parameters: None.

Command Mode: Port Mode and Port-Channel Mode.

Default: None.

Usage Guidelines: This command configures the local MC-LAG data link port. The **no** form of this command removes the configuration.

Example: Configure Ethernet 1/6/1 as the local MC-LAG data link port.

```
Switch(config-if-ethernet1/6/1)#switchport mclag data link
```

12.1.19 virtual-equipment-group ID

Command: `[no] virtual-equipment-group <ID>`

Function: Configures a virtual equipment group (VEG).

Parameters: <ID>: The VEG ID; the only valid value is 1.

Command Mode: Global Mode.

Default: None.

Usage Guidelines: This command configures a VEG. MC-LAG must be associated with the VEG to synchronize MAC, ARP, and ND entries. The **no** form of this command deletes the VEG.

Example: Configure VEG 1.

```
Switch(config)#virtual-equipment-group 1
```

12.1.20 virtual-equipment-group ID

Command: `[no] virtual-equipment-group <ID>`

Function: Associates a VEG with MC-LAG.

Parameters: <ID>: The VEG ID; the only valid value is 1.

Command Mode: MC-LAG Mode.

Default: None.

Usage Guidelines: This command associates a VEG with MC-LAG; the VEG function synchronizes MAC, ARP, and ND entries between the two MC-LAG devices. At the same time, the source IP and remote IP configured in the VEG are deleted, and the local IP and peer IP configured for MC-LAG are associated automatically. The **no** form of this command removes the association.

Example: Associate VEG 1 with MC-LAG.

```
Switch(config-mclag)#virtual-equipment-group 1
```

12.1.21 virtual-equipment-group ID

Command: `[no] virtual-equipment-group <ID>`

Function: Binds the gateway interface to a VEG.

Parameters: <ID>: The VEG ID; the only valid value is 1.

Command Mode: VLAN Interface Mode and NVI Interface Mode.

Default: None.

Usage Guidelines: This command binds the gateway interface to a VEG. The **no** form of this command unbinds the gateway interface from the VEG.

Example: Bind interface VLAN 4 to VEG 1.

```
Switch(config)#interface vlan 4
Switch(config-if-vlan4)#virtual-equipment-group 1
```

12.2 Commands for NETCONF

12.2.1 netconf server enable

Command: `netconf server enable`
`no netconf server enable`

Function: Enables NETCONF. The **no** form of this command disables NETCONF.

Command Mode: Global Mode.

Default: Not configured.

Usage Guidelines: None.

Example: Enable NETCONF.

```
Switch(config)# netconf server enable
netconf server is enabled
```

12.2.2 show netconf session

Command: `show netconf session`

Function: Displays NETCONF session information.

Command Mode: Admin Mode and Configuration Mode.

Default: None.

Usage Guidelines: NETCONF must be enabled and a client connected before the current session information can be viewed. Make sure the network between the NETCONF server and client is reachable.

Example: Display NETCONF session information.

```
Switch(config)# show netconf session
session_id:1
transport:netconf-ssh
```

```
username:test
source-host:172.30.8.120
login-time:2021-07-20T15:46:40+02:00
in-rpcs:0
in-bad-rpcs:0
out-rpc-errors:0
out-notifications:0
```

12.2.3 show netconf tcp

Command: `show netconf tcp`

Function: Displays information about users connected to NETCONF.

Command Mode: Admin Mode and Configuration Mode.

Default: None.

Usage Guidelines: NETCONF must be enabled and a client connected before the current user information can be viewed. Make sure the network between the NETCONF server and client is reachable.

Example: Display information about users connected to NETCONF.

```
Switch(config)# show netconf tcp
LocalAddress     LocalPort  ForeignAddress   ForeignPort     State       IF
VRF
0.0.0.0          830        0.0.0.0          *               LISTEN      0
0
172.17.100.34    830        172.30.8.120     57924           ESTABLISHED 3527
0
```

12.3 Commands for Telemetry

12.3.1 Telemetry

Command: `telemetry`

Function: Enters Telemetry Mode.

Default: Telemetry is not configured.

Command Mode: Global Mode.

Usage Guidelines: Enter Telemetry Mode to configure the telemetry function.

Example: Enter Telemetry Mode.

```
Switch(config)#telemetry
Switch(config-telemetry)#exit
```

12.3.2 grpc server

Command: `grpc server x.x.x.x port <10000-57999>`
`no grpc server`

Function: Configures the server address and TCP listening port for dynamic subscriptions.

Parameters: x.x.x.x: The IPv4 address.

<10000-57999>: The TCP listening port.

Default: Telemetry is not configured.

Command Mode: Telemetry Mode.

Usage Guidelines: This command can be configured only in Telemetry Mode. The IP address must be a local IP address reachable by the client.

Example:

```
Switch(config-telemetry)#grpc server 192.168.1.1 port 10002
Switch(config-telemetry)#no grpc server
```

12.3.3 destination-group

Command: `destination-group WORD`
`no destination-group WORD`

Function: Configures the name of a destination group for static subscriptions.

Parameters: WORD: A string of up to 64 characters.

Default: Telemetry is not configured.

Command Mode: Telemetry Mode.

Usage Guidelines: This command can be configured only in Telemetry Mode. The name can be up to 64 characters, and up to five groups can be configured.

Example:

```
Switch(config-telemetry)#destination-group abcdefgh
Switch(config-telemetry-dest-group-abcdefgh)#
Switch(config-telemetry)#no destination-group abcdefgh
```

12.3.4 destination-group ipv4-address

Command: `ipv4-address x.x.x.x port <1-65535>`
`no ipv4-address x.x.x.x port <1-65535>`

Function: Configures the IP address and TCP port of the target collector in a static-subscription destination group.

Parameters: x.x.x.x: The IPv4 address.

<1-65535>: The TCP listening port.

Default: Telemetry is not configured.

Command Mode: Destination Group Mode.

Usage Guidelines: This command can be configured only in Telemetry Mode.

Example:

```
Switch(config-telemetry)#destination-group abcdefgh
Switch(config-telemetry-dest-group-abcdefgh)#ipv4-address 172.17.30.96 port
50002
Switch(config-telemetry-dest-group-abcdefgh)#no ipv4-address 172.17.30.96
port 50002
```

12.3.5 sensor-group

Command: `sensor-group WORD`
`no sensor-group WORD`

Function: Configures the name of a sensor (sampling) group.

Parameters: WORD: A string of up to 64 characters.

Default: Telemetry is not configured.

Command Mode: Telemetry Mode.

Usage Guidelines: This command can be configured only in Telemetry Mode. The name can be up to 64 characters, and up to five groups can be configured.

Example:

```
Switch(config-telemetry)#sensor-group abcdefgh
```

```
Switch(config-telemetry-sen-group-abcdefgh)#
Switch(config-telemetry)#no sensor-group abcdefgh
```

12.3.6 sensor-group path memoryInfo

Command: sensor-path memoryInfo (| (op-type (eq | ge | gt | le | lt) op-value <1-100> (| ((and | or) op-type (eq | ge | gt | le | lt) op-value <1-100>))))
no sensor-path memoryInfo

Function: Configures the sensor path and constraints in a static-subscription sensor group.

Parameters: op-type: The constraint operator of the sensor path.

op-value: The constraint value of the sensor path.

Default: Telemetry is not configured.

Command Mode: Sensor Group Mode.

Usage Guidelines: This command can be configured only in Sensor Group Mode within Telemetry Mode. Constraints can be combined. To configure a new constraint, delete the original constraint first. **and** means AND, **or** means OR, **eq** means equal to, **ge** means greater than or equal to, **gt** means greater than, **le** means less than or equal to, and **lt** means less than.

Example:

```
Switch(config-telemetry)#sensor-group abcdefgh
Switch(config-telemetry-sen-group-abcdefgh)#sensor-pathMemoryInfo op-type
   le op-value 10 or op-type ge op-value 19
Switch(config-telemetry-sen-group-abcdefgh)#no sensor-path memoryInfo
```

12.3.7 sensor-group path cpuInfo

Command: sensor-path cpuInfo (| (op-type (eq | ge | gt | le | lt) op-value <1-100> (| ((and | or) op-type (eq | ge | gt | le | lt) op-value <1-100>))))
no sensor-path cpuInfo

Function: Configures the sensor path and constraints in a static-subscription sensor group.

Parameters: op-type: The constraint operator of the sensor path.

op-value: The constraint value of the sensor path.

Default: Telemetry is not configured.

Command Mode: Sensor Group Mode.

Usage Guidelines: This command can be configured only in Sensor Group Mode within Telemetry Mode. Constraints can be combined. To configure a new constraint, delete the original constraint first. **and** means AND, **or** means OR, **eq** means equal to, **ge** means greater than or equal to, **gt** means greater than, **le** means less than or equal to, and **lt** means less than.

Example:

```
Switch(config-telemetry)#sensor-group abcdefgh
Switch(config-telemetry-sen-group-abcdefgh)#sensor-pathcpuInfo   op-type
   le op-value 10 or op-type ge op-value 19
Switch(config-telemetry-sen-group-abcdefgh)#no sensor-path cpuInfo
```

12.3.8 sensor-group path ifStatistics

Command: sensor-path ifStatistics ((ethernet | port-channel) IFNAME|)
no sensor-path ifStatistics ((ethernet | port-channel) IFNAME|)

Function: Configures the interface statistics sensor path in a static-subscription sensor group.

Parameters: ethernet: Specifies an Ethernet port in the sensor path.

port-channel: Specifies a LAG port in the sensor path.

IFNAME: The port name.

Default: Telemetry is not configured.

Command Mode: Sensor Group Mode.

Usage Guidelines: This command can be configured only in Sensor Group Mode. If no interface is specified, all Layer 2 ports and LAG ports are sampled.

Example:

```
Switch(config-telemetry)#sensor-group abcdefgh
Switch(config-telemetry-sen-group-abcdefgh)#sensor-path ifStatistics ethernet
1/0/1
Switch(config-telemetry-sen-group-abcdefgh)#sensor-path ifStatistics port-
channel 1
Switch(config-telemetry-sen-group-abcdefgh)#sensor-path ifStatistics
Switch(config-telemetry-sen-group-abcdefgh)#no sensor-path ifStatistics
Switch(config-telemetry-sen-group-abcdefgh)#no sensor-path ifStatistics
ethernet 1/0/1
Switch(config-telemetry-sen-group-abcdefgh)#no sensor-path ifStatistics port-
channel 1
```

12.3.9 subscription

Command: `subscription WORD`
`no subscription WORD`

Function: Configures a subscription group.

Parameters: WORD: A string of up to 64 characters.

Default: Telemetry is not configured.

Command Mode: Telemetry Mode.

Usage Guidelines: This command can be configured only in Telemetry Mode. The name can be up to 64 characters, and up to five groups can be configured.

Example:

```
Switch(config-telemetry)#subscription abcdefgh
Switch(config-telemetry-sub-group-abcdefgh)#
Switch(config-telemetry)#no subscription abcdefgh
```

12.3.10 subscription destination-group

Command: `destination-group WORD`
`no destination-group WORD`

Function: Configures the destination group associated with the subscription.

Parameters: WORD: The destination group name.

Default: Telemetry is not configured.

Command Mode: Subscription Mode.

Usage Guidelines: This command can be configured only in Telemetry Mode. The name can be up to 64 characters. The destination group must be configured before it can be bound to the subscription group.

Example:

```
Switch(config-telemetry)#destination-group 1
Switch(config-telemetry-dest-group-1)#exit
Switch(config-telemetry)#subscription 2
```

```
Switch(config-telemetry-sub-group-2)#destination-group 1
Switch(config-telemetry-sub-group-2)#no destination-group 1
```

12.3.11 subscription sensor-group

Command: `sensor-group WORD sample-interval <10000-1800000>`
`no sensor-group WORD`

Function: Configures the associated sensor group and sampling interval.

Parameters: WORD: The sensor group name.

sample-interval: The sampling interval, from 10000 to 1800000 ms.

Default: Telemetry is not configured.

Command Mode: Subscription Mode.

Usage Guidelines: This command can only be configured in telemetry mode, the string length does not exceed 64, and the sensor group needs to be configured in advance before it can be bound to the subscription group. The actual configurable values of the sampling interval are 10s, 30s, 60s, 180s, 300s, 900s, 1800s.

Example:

```
Switch(config-telemetry)#sensor-group 1
Switch(config-telemetry-sen-group-1)#exit
Switch(config-telemetry)#subscription 2
Switch(config-telemetry-sub-group-2)#sensor-group 1 sample-interval 10000
Switch(config-telemetry-sub-group-2)#no sensor-group 1
```

12.3.12 tun interface vlan

Command: `tun interface vlan <vlan-id | WORD>`
`no tun interface vlan <vlan-id | WORD>`

Function: When a service port of the device is used as a management port, enables the tun function on the VLAN of that service port.

Parameters: <vlan-id> is the ID of an existing VLAN, ranging from 1 to 4094.

WORD is a list or range of VLANs, such as 100, 200, 300-400.

Command Mode: Global Mode.

Default: Not configured.

Usage Guidelines: Enable the tun function when a service port is used as the telemetry management port.

Example: Use IP address 192.168.60.100 of interface VLAN 100 as the telemetry management IP address and enable the tun function.

```
Switch(config)#interface Vlan100
Switch(config)#ip address 192.168.60.100 255.255.255.0
Switch(config)#interface ethernet 3/0/1
Switch(config-if-ethernet3/0/1)#switchport access vlan 100
Switch(config-if-ethernet3/0/1)#exit
Switch(config)#tun interface vlan 100
Switch(Config)#
```

12.3.13 show telemetry subscription

Command: `show telemetry subscription`

Function: Displays all static subscription configuration of telemetry.

Parameters: None.

Default: None.

Command Mode: All Modes.

Usage Guidelines: This command displays the configuration of all destination groups, sensor groups, and subscription groups in the current static subscriptions.

Example:

```
Switch(config)#telemetry
Switch(config-telemetry)#destination-group 1
Switch(config-telemetry-dest-group-1)#ipv4-address 172.17.9.26 port 50002
Switch(config-telemetry-dest-group-1)#exit
Switch(config-telemetry)#sensor-group 2
Switch(config-telemetry-sen-group-2)#sensor-path ifStatistics
Switch(config-telemetry-sen-group-2)#sensor-path cpuInfo
Switch(config-telemetry-sen-group-2)#sensor-path memoryInfo
Switch(config-telemetry-sen-group-2)#exit
Switch(config-telemetry)#subscription 3
Switch(config-telemetry-sub-group-3)#destination-group 1
Switch(config-telemetry-sub-group-3)#sensor-group 2 sample-interval 10000
Switch(config-telemetry-sub-group-3)#
Switch(config-telemetry-sub-group-3)#
Switch(config-telemetry-sub-group-3)#show telemetry subscription
-----------------------------------------------------
destination_group: 1
destination_ip_addr: 172.17.9.26:50002
-----------------------------------------------------
-----------------------------------------------------
sensor_group: 2
sensor_group_path: ifStatistics
sensor_group_path: MemoryInfo
sensor_group_path: CpuInfo
-----------------------------------------------------
-----------------------------------------------------
subscription_group: 3
subscription_destination_group: 1
subscription_sensor_group: 2
subscription_sample_interval: 10000 ms
-----------------------------------------------------
Switch(config-telemetry-sub-group-3)#
```

12.3.14 show telemetry dynamic-subscription

Command: `show telemetry dynamic-subscription`

Function: Displays all dynamic subscription information of telemetry.

Parameters: None.

Default: None.

Command Mode: All Modes.

Usage Guidelines: This command displays information about all clients connected in the current dynamic subscriptions.

Example:

```
Switch(config)#telemetry
Switch(config-telemetry)#grpc server 172.17.100.235 port 50002
Switch(config-telemetry)#show telemetry dynamic-subscription
-------------------------------------------------------------------------------
--
grpc server 172.17.100.235 port 50002
-------------------------------------------------------------------------------
--
-------------------------------------------------------------------------------
--
```

```
Ip-port :172.30.9.26:50002
Sensor-path:CpuInfo;MemoryInfo;IfStatistics
Sample-interval:10000 ms
```

12.4 VXLAN Commands

12.4.1 arp proxy-answer enable

Command: `[no] arp proxy-answer enable`

Function: Enables ARP proxy reply.

Parameters: None.

Command Mode: NVI Mode.

Default: Disabled.

Usage Guidelines: This configuration takes effect only after ARP suppression is enabled. With this function, the device replies on behalf of the target to ARP requests that match the suppression table, reducing ARP flooding and transmission to remote sites.

Example: Enable ARP proxy reply in NVI 10.

```
Switch(config)# nvi 10
Switch(config-nvi)#arp proxy-answer enable
```

12.4.2 arp suppression enable

Command: `[no] arp suppression enable`

Function: Enables ARP flood suppression.

Parameters: None.

Command Mode: NVI Mode.

Default: Disabled.

Usage Guidelines: This function reduces the flooding of broadcast ARP packets.

Example: Enable ARP flood suppression in NVI 10.

```
Switch(config)# nvi 10
Switch(config-nvi)# arp suppression enable
```

12.4.3 arp suppress-drop

Command: `[no] arp suppress-drop`

Function: Drops ARP packets suppressed by ARP flood suppression.

Parameters: None.

Command Mode: NVI Mode.

Default: Disabled.

Usage Guidelines: This function reduces the flooding of broadcast ARP packets and drops the suppressed ARP packets.

Example: Enable ARP flood suppression in NVI 10.

```
Switch(config)# nvi 10
Switch(config-nvi)# arp suppression enable
```

12.4.4 arp suppression table kat

Command: `[no] arp suppression table kat <1-3600>`

Function: Configures the lifetime of ARP suppression table entries.

Parameters: <1-3600>: The lifetime, in seconds.

Command Mode: Global Mode.

Default: 1100 seconds.

Usage Guidelines: The lifetime starts from the time the entry was created or last updated; the entry is deleted when it expires.

Example: Set the lifetime of ARP suppression table entries to 1000 seconds.

```
Switch(config)# arp suppression table kat 1000
```

12.4.5 clear nvi statistics

Command: clear nvi [<nvi-id>] statistics

Function: Clears the packet statistics of network virtual instances (NVIs).

Parameters: <nvi-id>: The NVI ID.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: This command clears the packet statistics of NVIs. By default, the statistics of all NVIs are cleared; an NVI ID can be specified.

Example: Clear the packet statistics of NVI 10.

```
Switch# clear nvi 10 statistics
```

12.4.6 description

Command: [no] description <NAME>

Function: Configures a description for an NVI.

Parameters: <NAME>: The description of the NVI.

Command Mode: NVI Mode.

Default: None.

Usage Guidelines: Configure a description for an NVI to make it easier to identify.

Example: Set the description of NVI 10 to school.

```
Switch(config)# nvi 10
Switch(config-nvi)# description school
```

12.4.7 description

Command: [no] description <NAME>

Function: Configures a description for an NVE tunnel.

Parameters: <NAME>: The description of the NVE tunnel.

Command Mode: NVE Interface Mode.

Default: None.

Usage Guidelines: Configure a description for an NVE tunnel to make it easier to identify.

Example: Set the description of NVE tunnel 1 to group1.

```
Switch(config)# interface nve 1
Switch(config-if-nve1)# description group1
```

12.4.8 destination

Command: [no]destination <ip-address>

Function: Configures the destination address of a VXLAN tunnel.

Parameters: <ip-address>: The destination IP address of the VTEP (VXLAN tunnel endpoint).

Command Mode: NVE Interface Mode.

Default: None.

Usage Guidelines: Manually specify the tunnel destination IP address (remote VTEP); use it with the **source** command to establish a VXLAN tunnel. The address of a VLAN interface or loopback interface can be specified; the loopback interface address is recommended.

Example: In NVE tunnel 1, set the source IP address to 1.1.1.1 and the destination IP address to 2.2.2.2.

```
Switch(config)# interface nve 1
Switch(config-if-nve1)# source 1.1.1.1
Switch(config-if-nve1)# destination 2.2.2.2
```

12.4.9 flooding disable

Command: [no] flooding disable

Function: Disables flooding on the VXLAN tunnels in the NVI.

Parameters: None.

Command Mode: NVI Mode.

Default: Flooding is enabled on all tunnels in the NVI.

Usage Guidelines: By default, when a VTEP receives a unicast frame with an unknown destination MAC address from the local site, it floods the frame on all VXLAN tunnels in the VXLAN network except the receiving interface, sending it to all sites. To prevent flooding into VXLAN tunnels, disable flooding with this command.

Example: Disable flooding in NVI 10.

```
Switch(config)# nvi 10
Switch(config-nvi)# flooding disable
```

12.4.10 interface nve

Command: [no] interface nve <nve-id>

Function: Creates an NVE tunnel interface.

Parameters: <nve-id>: The NVE tunnel interface ID, ranging from 1 to 400.

Command Mode: Global Mode.

Default: No NVE tunnel interface exists.

Usage Guidelines: This command creates an NVE tunnel interface and enters NVE Interface Mode. The **no** form of this command deletes the specified NVE interface and all its configuration.

Example: Create NVE tunnel interface 1.

```
Switch(config)# interface nve 1
Switch(config-if-nve1)#
```

12.4.11 interface nvi-interface

Command: [no] interface nvi-interface <nvi-interface-id>

Function: Creates an NVI virtual interface.

Parameters: <nvi-interface-id>: The NVI ID, ranging from 1 to 2048.

Command Mode: Global Mode.

Default: No NVI virtual interface exists.

Usage Guidelines: This command creates the NVI virtual interface associated with a virtual switching instance (NVI). The NVI must be created before the interface.

Example: Create NVI virtual interface 10.

```
Switch(config)#interface nvi-interface 10
Switch(config-if-nvi-interface10)#
```

12.4.12 ip address

Command: [no] ip address ip-address mask (secondary|)

Function: Configures the IP address of the NVI virtual interface.

Parameters: ip-address: The IP address of the NVI virtual interface.

mask: The subnet mask.

secondary: Configures the address as a secondary address.

Command Mode: NVI Interface Mode.

Default: No IP address is configured.

Usage Guidelines: This command configures the IP address of the NVI virtual interface, which serves as the gateway address when the device acts as a VXLAN IP gateway.

Example: Configure IP address 10.1.1.1 on NVI virtual interface 10.

```
Switch(config)# interface nvi-interface 10
Switch(config-if-nvi-interface10)# ip address 10.1.1.1 255.255.255.0
```

12.4.13 ipv6 address

Command: [no] ipv6 address X:X::X:X/M

Function: Configures the IPv6 address of the NVI virtual interface.

Parameters: X:X::X:X/M: The IPv6 address of the NVI virtual interface.

Command Mode: NVI Interface Mode.

Default: No IPv6 address is configured.

Usage Guidelines: This command configures the IPv6 address of the NVI virtual interface, which serves as the gateway address when the device acts as a VXLAN IPv6 gateway.

Example: Configure IPv6 address 2010::1/64 on NVI virtual interface 10.

```
Switch(config)# interface nvi-interface 10
Switch(config-if-nvi-interface10)# ipv6 address 2010::1/64
```

12.4.14 join nvi

Command: [no] join nvi <nvi-id>

Function: Associates the VXLAN tunnel interface with an NVI.

Parameters: <nvi-id>: The NVI ID, ranging from 1 to 3838.

Command Mode: NVE Interface Mode.

Default: The VXLAN tunnel interface does not belong to any NVI.

Usage Guidelines: A VXLAN tunnel interface can join multiple NVIs, and an NVI can be associated with multiple VXLAN tunnel interfaces. The NVIs at the two ends of a tunnel can differ, but the VXLAN IDs bound to them must be the same.

Example: Bind tunnel interface NVE 1 to NVI 10.

```
Switch(config)# interface nve 1
Switch(config-if-nve1)# join nvi 10
```

12.4.15 mac-address

Command: [no] mac-address FF-FF-FF-FF-FF-FF

Function: Configures the MAC address of the NVI virtual interface.

Parameters: FF-FF-FF-FF-FF-FF: The MAC address of the NVI virtual interface.

Command Mode: NVI Interface Mode.

Default: The default MAC address of the device.

Usage Guidelines: For distributed gateways, configure the same MAC address on all gateway interfaces in the same network segment.

Example: Set the MAC address of NVI virtual interface 10 to 02-02-02-02-02-02.

```
Switch(config)# interface nvi-interface 10
Switch(config-if-nvi-interface10)# mac-address 02-02-02-02-02-02
```

12.4.16 mac-address-table static address nvi

Command: [no] mac-address-table static address {mac-address} nvi <nvi-id> interface nve <nve-id>

Function: Configures a remote static MAC address.

Parameters: mac-address: The MAC address.

nvi-id: The NVI ID.

nve-id: The VXLAN tunnel interface corresponding to the remote MAC address.

Command Mode: Global Mode.

Default: None.

Usage Guidelines: This command configures a remote static MAC address on the specified NVI and tunnel interface. The tunnel interface must be a statically created VXLAN tunnel interface. When the tunnel is deleted or changed to another tunnel type, this configuration is deleted.

Example: Configure remote static MAC address 00-00-00-00-00-01 on NVI 10 and tunnel interface NVE 1.

```
Switch(config)# mac-address-table static address 00-00-00-00-00-01 nvi 10
interface nve 1
```

12.4.17 nd proxy-answer enable

Command: [no] nd proxy-answer enable

Function: Enables ND proxy reply.

Parameters: None.

Command Mode: NVI Mode.

Default: Disabled.

Usage Guidelines: This configuration takes effect only after ND suppression is enabled. With this function, the device replies on behalf of the target to NS packets that match the suppression table, reducing the flooding of multicast ND packets and transmission to remote sites.

Example: Enable ND proxy reply in NVI 10.

```
Switch(config)# nvi 10
Switch(config-nvi)#nd proxy-answer enable
```

12.4.18 nd suppression enable

Command: [no] nd suppression enable

Function: Enables ND flood suppression.

Parameters: None.

Command Mode: NVI Mode.

Default: Disabled.

Usage Guidelines: This function reduces the flooding of multicast ND packets.

Example: Enable ND flood suppression in NVI 10.

```
Switch(config)# nvi 10
Switch(config-nvi)# nd suppression enable
```

12.4.19 nd suppress-drop

Command: `[no] nd suppress-drop`

Function: Drops ND packets suppressed by ND flood suppression.

Parameters: None.

Command Mode: NVI Mode.

Default: Disabled.

Usage Guidelines: This function reduces the flooding of multicast ND packets and drops the suppressed ND packets.

Example: Enable ND flood suppression in NVI 10.

```
Switch(config)# nvi 10
Switch(config-nvi)# nd suppression enable
```

12.4.20 nd suppression table kat

Command: `[no] nd suppression table kat <1-3600>`

Function: Configures the lifetime of ND suppression table entries.

Parameters: <1-3600>: The lifetime, in seconds.

Command Mode: Global Mode.

Default: 1100 seconds.

Usage Guidelines: The lifetime starts from the time the entry was created or last updated; the entry is deleted when it expires.

Example: Set the lifetime of ND suppression table entries to 1000 seconds.

```
Switch(config)# nd suppression table kat 1000
```

12.4.21 nve mode

Command: `nve mode vxlan`

Function: Configures the mode of the NVE tunnel interface.

Parameters: None.

Command Mode: NVE Interface Mode.

Default: None.

Usage Guidelines: Only VXLAN mode is supported.

Example: Set tunnel interface NVE 1 to VXLAN mode.

```
Switch(config)# interface nve 1
Switch(config-if-nve1)#nve mode vxlan
```

12.4.22 nvi

Command: `[no] nvi <nvi-id>`

Function: Configures a network virtual instance (NVI).

Parameters: <nvi-id>: The NVI ID, ranging from 1 to 2048.

Command Mode: Global Mode.

Default: No NVI exists.

Usage Guidelines: This command creates an NVI and enters NVI Mode, or enters NVI Mode of an existing NVI. The **no** form of this command deletes the NVI and all its related dynamic data and configuration. If an NVE tunnel interface is manually bound to the NVI, unbind the NVE tunnel interface before deleting the NVI.

Example: Create NVI 10 and enter NVI Mode.

```
Switch(config)# nvi 10
Switch(config-nvi)#
```

12.4.23 remote ip

Command: `[no] remote ip <ip-address>`

Function: Specifies the IP address of the remote device for VEG communication.

Parameters: <ip-address>: The IP address for VEG communication (IPv4 only).

Command Mode: VEG Mode.

Default: None.

Usage Guidelines: This command configures the communication IP address of a remote device in the VEG. Up to five addresses can be configured.

Example: Set the communication IP address of the remote device to 2.2.2.2.

```
Switch(config)#virtual-equipment-group 1
Switch(config-veg1)#remote ip 2.2.2.2
```

12.4.24 show interface nve

Command: `show interface nve [<nve-id>]`

Function: Displays NVE tunnel interface information and statistics of sent and received packets and bytes.

Parameters: <nve-id>: The NVE tunnel interface ID, ranging from 1 to 400.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: This command displays NVE tunnel interface information and packet and byte statistics. By default, all NVE interfaces are displayed; an NVE ID can be specified.

Example:

```
Switch# show interface nve 200
NVE200 is up(0), line protocol is up, dev index is 16001
Device flag 0x91(UP P2P NOARP)
Time since last status change:0w-1d-20h-4m-19s  (158659 seconds)
Tunnel source 3.3.3.3, destination 2.2.2.2
  Input unicast packets statistics:
        0 input packets, 0 bytes
  Output unicast packets statistics:
        0 output packets, 0 bytes
```

12.4.25 show interface nvi-interface

Output	Description
source	Tunnel source IP address
destination	Tunnel destination IP address
Input unicast packets statistics	Number of packets and bytes received
Output unicast packets statistics	Number of packets and bytes sent

Command: show interface nvi-interface <nvi-interface-id>

Function: Displays information about the NVI virtual interface.

Parameters: <nvi-interface-id>: The NVI virtual interface number, ranging from 1 to 3838.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Displays information about the NVI virtual interface.

Example:

```
Switch# show interface nvi-interface 10
Nvi-interface is up(0), line protocol is up, dev index is 11012
  Device flag 0x1003(UP BROADCAST MULTICAST)
  Time since last status change:0w-1d-22h-2m-40s  (165760 seconds)
  IPv4 address is:
    12.0.0.1         255.255.255.0     (Primary)
  VRF Bind: Not Bind
  Hardware is EtherSVI, address is 00-22-2d-00-00-01
  MTU is 1500 bytes , BW is 0 Kbit
```

12.4.26 show ipv6 interface nvi-interface

Command: show ipv6 interface nvi-interface <nvi-interface-id>

Function: Displays IPv6 information about the NVI virtual interface.

Parameters: <nvi-interface-id>: The NVI virtual interface number, ranging from 1 to 3838.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Displays IPv6 information about the NVI virtual interface.

Example:

```
Switch# show ipv6 interface nvi-interface 10
Nvi-interface is up(0), line protocol is up, dev index is 11012
  Device flag 0x1003(UP BROADCAST MULTICAST)
  IPv6 is enabled
Link-local address(es):
 fe80::222:2dff:fe00:1  PERMANENT
Site-local address(es):
Global unicast address(es):
Joined group address(es):
 ff02::1
 ff02::1:ff00:1
MTU is 1500 bytes
ND DAD is enabled,    number of DAD attempts is 1
ND managed_config_flag is unset
ND other_config_flag is unset
ND NS interval is 1 second(s)
ND router advertisements is disabled
ND RA min-interval is 200 second(s)
ND RA max-interval is 600 second(s)
ND RA hoplimit is 64
ND RA lifetime is 1800 second(s)
```

```
ND RA MTU is 1500
ND advertised reachable time is 30000 millisecond(s)
ND advertised retransmit time is 1000 millisecond(s)
ND advertised default router preference is Medium
```

12.4.27 show nvi arp suppression

Command: show nvi [<nvi-id>] arp suppression

Function: Displays the ARP suppression entries in network virtual instances.

Parameters: <nvi-id>: The NVI ID, ranging from 1 to 3838.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Displays the ARP suppression entries in NVIs. By default, all NVIs are displayed; an NVI ID can be specified.

Example:

```
Switch# show nvi arp suppression
Address    Hardware Addr              Port    svid      Age-time(sec)
10.1.1.1   00-00-00-00-00-08        nve1    10        10s
20.1.1.1   00-00-00-00-00-09        Local   0         static
30.1.1.1   00-00-00-00-00-0f         nve2    20        12s
```

Output	Description
Address	IP address
Hardware Addr	MAC address
Port	nveX: Tunnel interface name Local: Local port
svid	VLAN ID
Age-time(sec)	Aging time; static means the entry does not age

12.4.28 show nvi detail

Command: show nvi [<nvi-id>] detail

Function: Displays detailed information about network virtual instances.

Parameters: <nvi-id>: The NVI ID, ranging from 1 to 3838.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Displays detailed information about NVIs. By default, all NVIs are displayed; an NVI ID can be specified.

Example:

```
Switch# show nvi 10 detail
NVI: 10
description:
vxlan-id: 10
udp destination-port number：4789
split-horizon: enable
flooding tunnel: enable
tunnel list:
Nve name    state      source           destination
Nve1        UP         12.0.0.1         12.0.0.2
```

12.4.29 show nvi nd suppression

Output	Description
NVI	NVI ID
description	Description of the NVI
vxlan-id	VXLAN ID
udp destination-port number	Destination UDP port number in the VXLAN packet header
split-horizon	Whether split horizon is enabled
flooding tunnel	Whether flooding on VXLAN tunnels is enabled
Nve name	Tunnel interface name
state	Tunnel interface status
source	Tunnel source address
destination	Tunnel destination address

Command: `show nvi [<nvi-id>] nd suppression`

Function: Displays the ND suppression entries in network virtual instances.

Parameters: <nvi-id>: The NVI ID, ranging from 1 to 3838.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Displays the ND suppression entries in NVIs. By default, all NVIs are displayed; an NVI ID can be specified.

Example:

```
Switch# show nvi nd suppression
Address    Hardware Addr           Port    svid      Age-time(sec)
2010::1    00-00-00-00-00-08        nve1    10        10s
2020::1    00-00-00-00-00-09        Local    0         static
2030::1    00-00-00-00-00-0f         nve2    20        12s
```

Output	Description
Address	IPv6 address
Hardware Addr	MAC address
Port	nveX: Tunnel interface name Local: Local port
svid	VLAN ID
Age-time(sec)	Aging time; static means the entry does not age

12.4.30 show nvi nve tunnel

Command: `show nvi [<nvi-id>] nve tunnel`

Function: Displays tunnel information of virtual switching instances.

Parameters: <nvi-id>: The NVI ID, ranging from 1 to 3838.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Displays tunnel information of NVIs. By default, all NVIs are displayed; an NVI ID can be specified.

Example:

```
Switch# show nvi nve tunnel
```

```
NVI 10 : vxlan-id 10
Nve name    state    source     destination
Nve1           up       1.1.1.1    2.2.2.2
Nve2           up       1.1.1.1    3.3.3.3
NVI 20 : vxlan-id 20
Nve name    state    source     destination
Nve1           up       1.1.1.1    2.2.2.2
Nve3           up       1.1.1.1    4.4.4.4
Nve4           up       5.5.5.5    6.6.6.6
```

Output	Description
NVI	NVI ID
vxlan-id	VXLAN ID
Nve name	Tunnel interface name
state	Tunnel interface status
source	Tunnel source address
destination	Tunnel destination address

12.4.31 show nvi statistics

Command: `show nvi [<nvi-id>] statistics`

Function: Displays packet statistics of network virtual instances.

Parameters: <nvi-id>: The NVI ID, ranging from 1 to 3838.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Displays packet statistics of NVIs. By default, all NVIs are displayed; an NVI ID can be specified.

Example:

```
Switch# show nvi 10 statistics
nvi 10 vxlan-id 10:
Item            Packets                 Bytes
Input            0                       0
Output          0                       0
```

Output	Description
NVI	NVI ID
vxlan-id	VXLAN ID
Input Packets Bytes	Number of packets and bytes received
Output Packets Bytes	Number of packets and bytes sent

12.4.32 show virtual-equipment-group ID

Command: `show virtual-equipment-group <ID>`

Function: Displays virtual equipment group (VEG) information.

Parameters: <ID>: The VEG ID; the only valid value is 1.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Displays the IP addresses and connection status of VEG members.

Example:

```
Switch(config-veg1)#show virtual-equipment-group 1
Virtual equipment group 1
  source ip 1.1.1.1
  remote ip 2.2.2.2 not connected
```

12.4.33 show virtual-equipment-group ID service

Command: show virtual-equipment-group <ID> service [interface nvi-interface <nvi-interface-id> (arp|nd)]

Function: Displays the services synchronized by the VEG.

Parameters: <ID>: The VEG ID; the only valid value is 1.

<nvi-interface-id>: The NVI virtual interface number, ranging from 1 to 3838.

(arp|nd): The service type, ARP or ND.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Displays all VEG services, or services of the specified type on the NVI interface.

Example:

```
Switch(config-veg1)#show virtual-equipment-group 1 service
sync service name arp-Nvi-interface10
   local entry num : 0 .
  remote ip 2.2.2.2 not connected
   peer service waiting for remote peer service ready .
sync service name nd-Nvi-interface10
   local entry num : 0 .
  remote ip 2.2.2.2 not connected
   peer service waiting for remote peer service ready .
```

12.4.34 show vxlan mac-address-table

Command: show vxlan mac-address-table [nvi <nvi-id>|]

Function: Displays the MAC address table entries in network virtual instances.

Parameters: <nvi-id>: The NVI ID, ranging from 1 to 3838.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Displays the MAC address table entries in NVIs. By default, all NVIs are displayed; an NVI ID can be specified.

Example:

```
Switch# show vxlan mac-address-table
Read mac address table....
Nvi-id  Mac Address          Type    Creator   Ports
----   --------------------- ------- ---------- -------------------------
4     00-00-00-02-44-23   DYNAMIC Hardware   Ethernet1/0/1
4     00-00-00-00-00-22   DYNAMIC Hardware   Nve1
4     00-00-00-00-00-33   STATIC  User       Nve2
```

12.4.35 show vxlan mac-address-table count

Output	Description
Nvi-id	NVI ID
Mac Address	MAC address
Type	MAC address type
Creator	Hardware: Learned by hardware User: Configured manually
Ports	Port name

Command: `show vxlan mac-address-table count [ nvi <nvi-id>|]`

Function: Displays the number of MAC address table entries in network virtual instances.

Parameters: <nvi-id>: The NVI ID, ranging from 1 to 3838.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Displays the number of MAC address table entries in NVIs. By default, all NVIs are displayed; an NVI ID can be specified.

Example:

```
Switch# show vxlan mac-address-table count
nvi-id             Mac count
------------------ --------------------------
10                 16
30                 16
```

Output	Description
Nvi-id	NVI ID
Mac count	Number of MAC address table entries

12.4.36 source

Command: `[no] source WORD|<ip-address>`

Function: Configures the source address of a VXLAN tunnel.

Parameters: WORD|<ip-address>: The source IP address of the VTEP (VXLAN tunnel endpoint).

Command Mode: NVE Interface Mode.

Default: None.

Usage Guidelines: Manually specify the tunnel source IP address (local VTEP); use it with the **destination** command to establish a VXLAN tunnel. The address of a VLAN interface or loopback interface can be specified; the loopback interface address is recommended.

Example: Set the source IP address of NVE tunnel 1 to 1.1.1.1.

```
Switch(config)# interface nve 1
Switch(config-if-nve1)# source 1.1.1.1
```

12.4.37 source ip

Command: `source ip <ip-address>`

Function: Specifies the IP address of the local device for VEG communication.

Parameters: <ip-address>: The IP address for VEG communication (IPv4 only).

Command Mode: VEG Mode.

Default: None.

Usage Guidelines: Configures the communication IP address of the local device in the VEG.

Example:

```
Switch(config)#virtual-equipment-group 1
Switch(config-veg1)#source ip 1.1.1.1
```

12.4.38 virtual-equipment-group ID

Command: [no] virtual-equipment-group <ID>

Function: Configures a virtual equipment group (VEG).

Parameters: <ID>: The VEG ID; the only valid value is 1.

Command Mode: Global Mode.

Default: None.

Usage Guidelines: Multiple devices can be associated with the VEG by specifying its source IP and remote IP addresses.

Example:

```
Switch(config)#virtual-equipment-group 1
Switch(config-veg1)#
```

12.4.39 vxlan remote arp-learning disable

Command: [no] vxlan remote arp-learning disable

Function: Disables automatic remote ARP learning.

Parameters: None.

Command Mode: Global Mode.

Default: Automatic remote ARP learning is enabled.

Usage Guidelines: Configures whether automatic remote ARP learning is enabled.

Example:

```
Switch(config)# vxlan remote arp-learning disable
```

12.4.40 vxlan remote mac-address-learning disable

Command: [no] vxlan remote mac-address-learning disable

Function: Disables automatic remote MAC address learning.

Parameters: None.

Command Mode: Global Mode.

Default: Automatic remote MAC address learning is enabled.

Usage Guidelines: Configures whether automatic remote MAC address learning is enabled.

Example:

```
Switch(config)# vxlan remote mac-address-learning disable
```

12.4.41 vxlan remote nd-learning disable

Command: [no] vxlan remote arp-learning disable

Function: Disables automatic remote ND learning.

Parameters: None.

Command Mode: Global Mode.

Default: Automatic remote ND learning is enabled.

Usage Guidelines: Configures whether automatic remote ND learning is enabled.

Example:

```
Switch(config)# vxlan remote nd-learning disable
```

12.4.42 vxlan udp destination-port-number

Command: [no] vxlan udp destination-port-number <1-65535>

Function: Configures the destination UDP port number in the VXLAN packet header.

Parameters: <1-65535>: The port number, ranging from 1 to 65535.

Command Mode: Global Mode.

Default: 4789.

Usage Guidelines: Configures the destination UDP port number in the VXLAN packet header.

Example: Set the destination UDP port number in the VXLAN packet header to 5000.

```
Switch(config)# vxlan udp destination-port-number 5000
```

12.4.43 vxlan-id

Command: vxlan-id <vxlan-id>

Function: Configures the VXLAN network identifier (VNI) and associates it with the network virtual instance.

Parameters: <vxlan-id>: The VXLAN network identifier, ranging from 1 to 16777215.

Command Mode: NVI Mode.

Default: No VXLAN ID is configured.

Usage Guidelines: In a VXLAN (Virtual eXtensible Local Area Network) network, the NVI broadcast domain is a virtual broadcast domain that must be bound to the NVI with the **vxlan-id** command. VXLAN IDs and NVIs map one to one: a VXLAN ID can be bound to only one NVI, and an NVI can be bound to only one VXLAN ID. After this command is configured, the VXLAN ID cannot be modified.

Example: Set the VXLAN ID of NVI 10 to 5000.

```
Switch(config)# nvi 10
Switch(config-nvi)# vxlan-id 5000
```

12.4.44 xconnect nvi

Command: [no] xconnect nvi <nvi-id> {mode {ethernet| vlan svid <vid>}| }

Function: Configures the VXLAN access mapping of the access port.

Parameters: <nvi-id>: The NVI ID, ranging from 1 to 2048.

{ethernet | vlan}: The VXLAN access mapping mode, Ethernet or VLAN.

<vid>: The outer VLAN ID of the packets, ranging from 1 to 4094.

Command Mode: Port Mode.

Default: None.

Usage Guidelines: This command binds the port to an NVI in Ethernet or VLAN mode. If the mode and its parameters are not specified, Ethernet mode is used. In Ethernet mode, a port can be associated with only one NVI.

Example: Associate Ethernet 1/0/1 with NVI 10 in VLAN mode with VLAN ID 10.

```
Switch(config)# interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# xconnect nvi 10 mode vlan svid 10
```

12.5 EVPN Commands

12.5.1 address-family l2vpn evpn

Command: `address-family l2vpn evpn`

Function: Enters EVPN Address Family Mode.

Parameters: None.

Command Mode: BGP Mode.

Default: None.

Usage Guidelines: Enters EVPN Address Family Mode.

Example: Enter EVPN Address Family Mode.

```
Switch(config-router)#address-family l2vpn evpn
Switch(config-router-af)#
```

12.5.2 distributed-gateway enable

Command: `[no] distributed-gateway enable`

Function: Configures the gateway interface as a distributed gateway interface.

Parameters: None.

Command Mode: NVI Interface Mode.

Default: The interface is a centralized gateway interface.

Usage Guidelines: This command configures the gateway interface as a distributed gateway interface. The VRF bound to the NVI interface must already have an L3VNI configured.

Example: Configure NVI interface 10 as a distributed gateway interface.

```
Switch(config)#interface nvi-interface 10
Switch(config-if-nvi-interface10)#distributed-gateway enable
```

12.5.3 dup-addr-detection

Command: `[no] dup-addr-detection [max-moves <max-moves>] [detect-time <time>]`

Function: Configures the duplicate MAC address detection threshold.

Parameters: <max-moves>: The maximum number of MAC address moves within the detection time, ranging from 2 to 1000.

<time>: The detection time, ranging from 2 to 1800 seconds.

Command Mode: EVI Mode.

Default: max-moves is 5 and **detect-time** is 180 seconds.

Usage Guidelines: When the device detects that a MAC address has moved, it starts the duplicate address detection timer. If the MAC address moves **max-moves** times before the timer expires, the device considers it a duplicate MAC address and raises an alarm.

Example: Raise an alarm if a MAC address moves 10 times within 300 seconds.

```
Switch(config-nvi-evpn)#dup-addr-detection max-moves 10 detect-time 300
```

12.5.4 enable/disable

Command: `enable`

disable

Function: Enables or disables the EVPN instance in the NVI.

Parameters: None.

Command Mode: EVI Mode.

Default: Disabled.

Usage Guidelines: Enabling the EVPN instance in the NVI generates the related Type 2 and Type 3 routes. The RD must be configured before the EVPN instance is enabled. Disabling the EVPN instance deletes the related Type 2 and Type 3 routes.

Example: Enable the EVPN instance in the NVI.

```
Switch(config-nvi-evpn)#enable
```

12.5.5 esi

Command: [no] esi <id>

Function: Configures the ESI of the interface.

Parameters: <id>: The ESI of the interface, in the format 00xx.xxxx.xxxx.xxxx.xxxx.

Command Mode: Port Mode.

Default: None.

Usage Guidelines: This command configures the ESI of the interface. In a single-homing environment, the ESI is always 0 and no configuration is required. In a multihoming environment, the interfaces of all PEs connected to the same CE must be configured with the same ESI.

Example: Set the ESI of interface Ethernet 1/0/1 to 0012.1212.1212.1212.1212.

```
Switch#(config-if-ethernet1/0/1)#esi 0012.1212.1212.1212.1212
```

12.5.6 evpn

Command: [no] evpn

Function: Creates an EVPN instance associated with the NVI.

Parameters: None.

Command Mode: NVI Mode.

Default: No EVPN instance is associated with the NVI.

Usage Guidelines: This command creates an EVPN instance associated with the NVI and enters EVI Mode. The VXLAN ID of the NVI and **evpn nve source-address** must be configured first. Deleting the EVPN instance also deletes its associated entries, including the local MAC-VRF and the EVPN routes advertised by the device.

Example: Create an EVPN instance associated with NVI 10.

```
Switch(config)# nvi 10
Switch(config-nvi)#evpn
```

12.5.7 evpn nve source-address

Command: [no] evpn nve source-address <ip-address>

Function: Configures the NVE source IP address of EVPN instances.

Parameters: <ip-address>: The NVE source IP address.

Command Mode: Global Mode.

Default: None.

Usage Guidelines: This address is used as the next-hop address of advertised EVPN routes and as the Originating Router's IP in the NLRI, and is used to establish VXLAN tunnels. It must be a local Layer 3 interface address; a loopback interface address is recommended. Only one NVE source address can be configured in the system, and it cannot be modified after configuration; to change it,

delete and reconfigure it. When this configuration is deleted, the system prompts to delete all EVPN configuration.

Example: Set the NVE source address of EVPN instances to 2.2.2.2.

```
Switch(config)#evpn nve source-address 2.2.2.2
```

12.5.8 evpn nvi-vlan-mapping-monitor disable

Command: `[no] evpn nvi-vlan-mapping-monitor disable`

Function: Disables mapping of ingress VLANs to the Ethernet tag ID (eti-id), which implements the VLAN-based EVPN service model.

Parameters: None.

Command Mode: Global Mode.

Default: Enabled.

Usage Guidelines: After this command is configured, the eti-id field of all locally generated or learned EVPN routes is 0. When the function is enabled (the default), the VLAN configuration of the access port is identified and mapped to the eti-id field of EVPN routes.

Example:

```
Switch(config)#evpn nvi-vlan-mapping-monitor disable
```

12.5.9 evpn timer df-delay

Command: `[no] evpn timer df-delay <delay-value>`

Function: Configures the designated forwarder (DF) election delay.

Parameters: <delay-value>: The delay, ranging from 1 to 120 seconds.

Command Mode: Global Mode.

Default: 3 seconds.

Usage Guidelines: In a multihoming access network, a PE starts the DF election delay timer after sending a Type 4 route and performs DF election when the timer expires. This command configures the delay, that is, the timeout of the timer. The **no** form of this command restores the default.

Example: Set the DF election delay to 5 seconds.

```
Switch(config)#evpn timer df-delay 5
```

12.5.10 evpn-exit

Command: `evpn-exit`

Function: Exits EVI Mode.

Parameters: None.

Command Mode: EVI Mode.

Default: None.

Usage Guidelines: Exits EVI Mode.

Example:

```
Switch(config-nvi-evpn)#evpn-exit
Switch(config-nvi)#
```

12.5.11 exit-address-family

Command: `exit-address-family`

Function: Exits BGP EVPN Address Family Mode.

Parameters: None.

Command Mode: BGP EVPN Address Family Mode.

Default: None.

Usage Guidelines: Exits BGP EVPN Address Family Mode and returns to BGP Mode.

Example: Exit BGP EVPN Address Family Mode.

```
Switch(config-router-af)#exit-address-family
Switch(config-router)#
```

12.5.12 ip vrf forwarding

Command: `[no] ip vrf forwarding <vrf-name>`

Function: Associates the NVI Layer 3 gateway interface with an L3VPN instance.

Parameters: <vrf-name>: The name of the L3VPN instance.

Command Mode: NVI Interface Mode.

Default: None.

Usage Guidelines: This command associates the NVI interface with an L3VPN instance. The **no** form of this command removes the association and deletes the configured IP address and related routes.

Example: Associate NVI virtual interface 10 with VRF a1.

```
Switch(config)#interface nvi-interface 10
Switch(config-if-nvi-interface10)#ip vrf forwarding a1
```

12.5.13 l3-vni

Command: `[no] l3-vni <vxlan-id>`

Function: Configures the VNI of an L3VPN instance.

Parameters: <vxlan-id>: The VXLAN network identifier, ranging from 1 to 16777215.

Command Mode: VRF Mode.

Default: None.

Usage Guidelines: This command configures the VNI of an L3VPN instance to establish a VXLAN Layer 3 tunnel; it is needed only on distributed gateways. After configuration, EVPN Type 2 and Type 5 routes are used to advertise VPN routes between PEs. Only one VNI can be configured per L3VPN instance, and the same L3VPN instance on different PEs must use the same VNI. Deleting the VNI also deletes the VXLAN tunnels associated with it and the related routes.

Example: Associate the L3VPN instance with VXLAN ID 100.

```
Switch(config-vrf)#l3-vni 100
```

12.5.14 rd

Command: `[no] rd <ASN:nn_or_IP-address:nn>`

Function: Configures the route distinguisher (RD) of the EVPN instance.

Parameters: <ASN:nn_or_IP-address:nn>: The RD value, either an AS number plus a unique identifier within the AS, or a router ID plus a unique identifier within the device.

Command Mode: EVI Mode.

Default: None.

Usage Guidelines: The RD is used only to distinguish EVPN routes. Only one RD can be configured for each EVPN instance. After the EVPN instance is enabled, the RD cannot be deleted or modified. The RD must be unique among all EVIs.

Example: Set the RD of the EVPN instance to 20:20.

```
Switch(config)# nvi 10
Switch(config-nvi)#evpn
Switch(config-nvi-evpn)#rd 20:20
```

12.5.15 route-target

Command: [no] route-target {import | export | both} <rt-value>

Function: Configures the route targets of the EVPN instance.

Parameters: {import | export | both}: Configures the import route target, the export route target, or both.

<rt-value>: The route target value.

Command Mode: EVI Mode.

Default: None.

Usage Guidelines: Route targets filter EVPN routes. If the route targets of an EVPN route in a received BGP message intersect the import route targets of an EVI, the route is imported to the MAC-VRF of that EVI. When the device advertises an EVPN route of an EVI, the route carries the export route targets of the EVI. Multiple import and export route targets can be configured. After the EVPN instance is enabled, the route targets cannot be modified or deleted.

Example: Set both the import and export route targets of the EVPN instance to 1:1.

```
Switch(config)# nvi 10
Switch(config-nvi)#evpn
Switch(config-nvi-evpn)#route-target both 1:1
```

12.5.16 neighbor activate

Command: [no] neighbor {<ip-address>|<TAG>} activate

Function: Advertises EVPN capability to a peer.

Parameters: <ip-address>: The IPv4 address of the BGP peer.

<TAG>: The name of the peer group.

Command Mode: BGP EVPN Address Family Mode.

Default: None.

Usage Guidelines: Advertises EVPN capability to a peer. If the peer also supports EVPN, EVPN routes are then sent to it.

Example: Advertise EVPN capability to neighbor 1.1.1.1.

```
Switch(config-router-af)# neighbor 1.1.1.1 activate
```

12.5.17 neighbor route-reflector-client

Command: [no] neighbor {<ip-address>|<TAG>} route-reflector-client

Function: Configures a route reflector client.

Parameters: <ip-address>: The IPv4 address of the BGP peer.

<TAG>: The name of the peer group.

Command Mode: BGP EVPN Address Family Mode.

Default: None.

Usage Guidelines: Configures a route reflector client.

Example: Configure neighbor 3.3.3.3 as a route reflector client.

```
Switch(config-router-af)# neighbor 3.3.3.3 route-reflector-client
```

12.5.18 show evpn es

Command: `show evpn es all|<esi> [detail]`

Function: Displays information about Ethernet segments (ESs).

Parameters: <esi>: The ESI of the ES, in the format 00xx.xxxx.xxxx.xxxx.xxxx.

detail: Displays detailed information.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Displays information about the specified ES; **all** displays information about all ESs.

Example: Display detailed information about all ESs.

```
Switch#show evpn es all detail
Ethernet Segment 0001.0000.0011.0000.0001 (LOCAL)
 State: DF Done
 NVE list:
  1.1.1.1              Flags: 0x0
  2.2.2.2              Flags: 0x0
 Route Distinguisher: 1.1.1.1:2908
 ES Import Route-Target:
 Link Name: Ethernet1/0/11
 Link State: Up
 DF infomation:
  1.1.1.1              EVI(10) : DF
Ethernet Segment 0011.2222.3333.4444.4444 (REMOTE)
 State: Remote
 NVE list:
  2.2.2.2              Flags: 0x0
```

Output	Description
Ethernet Segment	Ethernet Segment Ethernet segment (LOCAL or REMOTE)
State	Designated forwarder election status
NVE list	NVE interface list
Route Distinguisher	Route distinguisher of the EVPN instance
ES Import Route-Target	ES import route target
Link Name	Port name
Link State	Port link status
DF infomation	Designated forwarder information

12.5.19 show evpn mac-ip

Command: `show evpn mac-ip all|nvi <nvi-id>`

Function: Displays the MAC and IP information learned by EVPN.

Parameters: <nvi-id>: The NVI ID, ranging from 1 to 2048.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Displays the MAC and IP information learned by EVPN.

Example:

```
Switch#show evpn mac-ip all
 VXLAN_ID  MAC      ETH_TAG_ID   SEQ_NUM  STICKY  ESI
  IP ADDRESS                          DST NVE          FLAGS
```

```
 20        00-10-94-00-fa-d2  20          0        FALSE
0000.0000.0000.0000.0000
  N/A                                     3.3.3.3          R
 20        00-10-94-00-fa-d3  20          0        FALSE
0000.0000.0000.0000.0000
  N/A                                     3.3.3.3          R
 20        00-10-94-00-fa-d4  20          0        FALSE
0000.0000.0000.0000.0000
  N/A                                     3.3.3.3          R
 20        00-10-94-00-fa-d5  20          0        FALSE
0000.0000.0000.0000.0000
```

Output	Description
VXLAN_ID	VXLAN ID
MAC	MAC address learned by EVPN
ETH_TAG_ID	Ethernet tag ID of the forwarding instance associated with the MAC/IP entry learned by EVPN
SEQ_NUM	Sequence number that records the number of MAC moves
STICKY	Whether the entry is a protected (sticky) MAC entry
ESI	ESI carried by the MAC/IP entry learned by EVPN
IP ADDRESS	IP address of the MAC/IP entry learned by EVPN
DST NVE	Next-hop NVE address
FLAGS	L: Local entry; R: Remote entry S: Synchronized local entry A: Synchronized remote alias path

12.5.20 show evpn mac-mobility

Command: `show evpn mac-mobility`

Function: Displays MAC move information.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Displays MAC move information, including the moved MAC addresses, the number of moves, and the current status (Detecting or Suppression).

Example:

```
Switch# show evpn mac-mobility
EVPN Instance (NVI 10)
00-00-00-00-00-01 2 Detecting
00-00-00-00-00-02 6 Suppression
```

12.5.21 show evpn nvi

Command: `show evpn nvi all|<nvi-id>`

Function: Displays global information about EVPN instances.

Parameters: <nvi-id>: The NVI ID, ranging from 1 to 3838.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Displays information about the EVPN instance associated with the specified NVI.

Example: Display information about the EVPN instance associated with NVI 10.

```
Switch#show evpn nvi 10
EVPN Instance (NVI 10)
 Encapsolution VXLAN
 VNI: 10
 Status: ACTIVE
 Route Distinguisher: 2:2
 Import Route Target
  RT: 1:1
  RT: 3:3
 Export Route Target
  RT: 2:2
 NVE Source Address: 2.2.2.2 (GLOBAL_USED)
 Duplication MAC-Address Detect
  Detect time: 300        Max moves: 10
```

Output	Description
VNI	VXLAN ID
Status	Status of the EVPN instance (ACTIVE or CONFIG)
Route Distinguisher	Route distinguisher of the EVPN instance
Import Route Target	Import route target list
Export Route Target	Export route target list
NVE Source Address	NVE source address of the EVPN instance
Duplication MAC-Address Detect	Duplicate MAC address detection threshold

12.5.22 show ip bgp evpn

Command: `show ip bgp evpn {all|type-1|type-2|type-3|type-4|type-5}`

Function: Displays information about EVPN routes.

Parameters: {all|type-1|type-2|type-3|type-4|type-5}: The route type; **all** displays EVPN routes of all types.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: Displays information about EVPN routes.

Example: Display EVPN routes of all types.

```
Switch#show ip bgp evpn all
BGP local router ID is 33.33.33.33
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
network format description
RT-1:[RT][ESI][ETID]
RT-2:[RT][ETID][MAC][IPv4/v6]
RT-3:[RT][ETID][IPv4/v6]
RT-4:[RT][ESI][IPv4/v6]
RT-5:[RT][ETID][Prefix len][Prefix]
Route Distinguisher 1:3837
   Network          Next Hop         Metric     LocPrf     Weight Path
*>i[1][00ff.ffff.ffff.ffff.ffff][0]
                    11.1.1.1                    100        0      ?
*>i[3][3837][11.1.1.1]
```

```
                    11.1.1.1                    100        0      ?
Route Distinguisher 11111:3837
   Network          Next Hop         Metric     LocPrf     Weight Path
*>i[5][0][16][101.1.0.0]
                    11.1.1.1                    100        0      ?
*>i[5][0][64][1001::]
                    11.1.1.1                    100        0      ?
Route Distinguisher 11.1.1.1:13427
   Network          Next Hop         Metric     LocPrf     Weight Path
*>i[1][00ff.ffff.ffff.ffff.ffff][4294967295]
                    11.1.1.1                    100        0      ?
*>i[2][300][2203-0000-000d][]
                    11.1.1.1                    100        0      ?
*>i[2][300][2203-0000-000d][30.30.1.112]
11.1.1.1                    100        0      ?
*>i[4][00ff.ffff.ffff.ffff.ffff][11.1.1.1]
                    11.1.1.1                    100        0      ?
```

Chapter 13 Commands for IPv6

13.1 DHCPv6

13.1.1 clear ipv6 dhcp binding

Command: `clear ipv6 dhcp binding [<ipv6-address>] [pd <ipv6-prefix | prefix-length>]`

Function: Clears a specified DHCPv6 address binding record, or all IPv6 address binding records.

Parameters: <ipv6-address> is the IPv6 address of the binding record to clear. **<ipv6-prefix | prefix-length>** is the IPv6 prefix of the binding record to clear. If no record is specified, all IPv6 address binding records are cleared.

Command Mode: Admin Mode.

Usage Guidelines: DHCPv6 address binding information can be displayed with **show ipv6 dhcp binding**. If a DHCPv6 client no longer uses an allocated IPv6 address but the address lifetime has not expired, the DHCPv6 server does not remove the binding. In this case, use this command to remove the binding manually. If no parameter is specified, all address bindings are removed, and all addresses and prefixes in the DHCPv6 address pool can be assigned again.

Example: Delete all IPv6 address and prefix binding records.

```
Switch#clear ipv6 dhcp binding
```

Related Commands: show ipv6 dhcp binding

13.1.2 clear ipv6 dhcp conflict

Command: `clear ipv6 dhcp conflict [<address>]`

Function: Clears the conflict records of addresses from the address conflict log.

Parameters: <address> is the address whose conflict record is cleared. If no address is specified, all conflict records are cleared.

Command Mode: Admin Mode.

Usage Guidelines: Use **show ipv6 dhcp conflict** to check which IPv6 addresses have conflicts. This command clears the conflict record of an address, or of all addresses in the log if none is specified. After the conflict records are cleared, the DHCPv6 server can use these addresses again.

Example: The administrator finds in the conflict log that address 2001::1 is not in use and clears its conflict record.

```
Switch#clear ipv6 dhcp conflict 2001::1
```

13.1.3 clear ipv6 dhcp statistics

Command: `clear ipv6 dhcp statistics`

Function: Clears the DHCPv6 packet statistics counters.

Parameters: None.

Command Mode: Admin Mode.

Usage Guidelines: Use **show ipv6 dhcp statistics** to check the DHCPv6 packet counters; all statistics are cumulative. Clear the counters with this command to make debugging easier.

Example: Clear the DHCPv6 packet counters.

```
Switch#clear ipv6 dhcp statistics
```

Related Commands: show ipv6 dhcp statistics

13.1.4 debug ipv6 dhcp client packet

Command: debug ipv6 dhcp client {event | packet}
no debug ipv6 dhcp client {event | packet}

Function: Enables debugging of DHCPv6 prefix delegation client events or protocol packets. The **no** form of this command disables it.

Default: Disabled.

Command Mode: Admin Mode.

Example:

```
Switch# debug ipv6 dhcp client packet
```

13.1.5 debug ipv6 dhcp detail

Command: debug ipv6 dhcp detail
no debug ipv6 dhcp detail

Function: Enables display of debugging information for all packets received or sent by DHCPv6. The **no** form of this command disables it.

Default: Disabled.

Command Mode: Admin Mode.

Example:

```
Switch# debug ipv6 dhcp detail
```

13.1.6 debug ipv6 dhcp relay packet

Command: debug ipv6 dhcp relay packet
no debug ipv6 dhcp relay packet

Function: Enables debugging of DHCPv6 relay protocol packets. The **no** form of this command disables it.

Default: Disabled.

Command Mode: Admin Mode.

Example:

```
Switch# debug ipv6 dhcp relay packet
```

13.1.7 debug ipv6 dhcp server

Command: debug ipv6 dhcp server { event | packet }
no debug ipv6 dhcp server { event | packet }

Function: Enables DHCPv6 server debugging. The **no** form of this command disables it.

Parameters: event enables debugging of DHCPv6 server events, such as address allocation. **packet** enables debugging of DHCPv6 server protocol packets.

Default: Disabled.

Command Mode: Admin Mode.

Example:

```
Switch#debug ipv6 dhcp server packet
```

13.1.8 dns-server

Command: `dns-server <ipv6-address>`
`no dns-server <ipv6-address>`

Function: Configures the IPv6 address of the DNS server for DHCPv6 clients. The **no** form of this command removes the DNS server.

Parameters: <ipv6-address> is the IPv6 address of the DNS server.

Default: No DNS server is configured in the address pool.

Command Mode: DHCPv6 Address Pool Mode.

Usage Guidelines: Up to three DNS servers can be configured for each address pool. The DNS server addresses must be valid IPv6 addresses.

Example: Set the DNS server address for DHCPv6 clients to 2001:da8::1.

```
Switch(dhcp-1-config)#dns-server 2001:da8::1
```

13.1.9 domain-name

Command: `domain-name <domain-name>`
`no domain-name <domain-name>`

Function: Configures the domain name for DHCPv6 clients. The **no** form of this command deletes the domain name.

Parameters: <domain-name> is the domain name, less than 32 characters.

Command Mode: DHCPv6 Address Pool Mode.

Default: No domain name is configured in the address pool.

Usage Guidelines: Up to three domain names can be configured for each address pool.

Example: Set the domain name for DHCPv6 clients to www.google.com.

```
Switch(dhcp-1-config)#domain-name www.google.com
```

13.1.10 excluded-address

Command: `excluded-address <ipv6-address> <ipv6-address>`
`no excluded-address <ipv6-address> <ipv6-address>`

Function: Excludes the specified IPv6 addresses from the address pool so that they are not allocated to any host. The **no** form of this command removes the configuration.

Parameters: <ipv6-address> is the IPv6 address to exclude from allocation in the address pool.

Default: None.

Command Mode: DHCPv6 Address Pool Mode.

Usage Guidelines: Use this command to reserve the specified addresses from DHCPv6 address allocation.

Example: Exclude 2001:da8:123::1 and 2001:da8:123::2 from DHCPv6 address allocation.

```
Switch(dhcpv6-1-config)#excluded-address 2001:da8:123::1 2001:da8:123::2
```

13.1.11 ipv6 address

Command: `ipv6 address <prefix-name> <ipv6-prefix/prefix-length>`
`no ipv6 address <prefix-name> <ipv6-prefix/prefix-length>`

Function: Configures the specified interface to use a delegated prefix for address allocation. The **no** form of this command disables it.

Parameters: <prefix-name> is a string of up to 32 characters that names an address prefix defined in the prefix pool, obtained through prefix delegation or configured manually. **<ipv6-prefix/prefix-length>** is the rest of the IPv6 address after the prefix, with its length.

Command Mode: Interface Mode.

Default: No global address is configured on the interface.

Usage Guidelines: The IPv6 address of an interface consists of two parts: **<prefix-name>** and **<ipv6-prefix>/<prefix-length>**. If router advertisement is enabled, the first 64 bits of the address are advertised. When this configuration is removed, the address generated from **<prefix-name>** and **<ipv6-prefix/prefix-length>** is removed and advertisement of the prefix stops. Only one **<ipv6-prefix/prefix-length>** can be configured for each prefix name.

Example: If prefix name my-prefix designates 2001:da8:221::/48, the following command adds address 2001:da8:221:2008::2008 to interface VLAN 1.

```
Switch(Config-if-Vlan1)# ipv6 address my-prefix 0:0:0:2008::2008/64
```

13.1.12 ipv6 dhcp client pd

Command: ipv6 dhcp client pd <prefix-name> [rapid-commit]
no ipv6 dhcp client pd

Function: Configures the DHCPv6 prefix delegation client on the specified interface. The **no** form of this command disables the client and removes the allocated prefix.

Parameters: <prefix-name> is a string of up to 32 characters that names the address prefix. If **rapid-commit** is specified and the prefix delegation server has rapid commit enabled, the server replies to the client directly with a REPLY message, and prefix delegation completes in a single message exchange.

Command Mode: Interface Mode.

Default: Disabled.

Usage Guidelines: This command configures the prefix delegation client on the specified interface. An interface with the client enabled sends SOLICIT packets to obtain an address prefix from the server. If the prefix is obtained, it can be used from the global address pool by the **ipv6 address** command to generate a valid IPv6 address. This command is mutually exclusive with **ipv6 dhcp server** and **ipv6 dhcp relay destination**. If the client is disabled on an interface, the prefix obtained through this interface is removed from the global address pool, the interface address generated from it is removed, and router advertisement of the prefix stops. If the same prefix has been configured with **ipv6 general-prefix**, the prefix learned through prefix delegation is rejected.

Example:

```
Switch(Config-if-Vlan1)#ipv6 dhcp client pd ClientA rapid-commit
```

13.1.13 ipv6 dhcp client pd hint

Command: ipv6 dhcp client pd hint <prefix|prefix-length>
no ipv6 dhcp client pd hint <prefix|prefix-length>

Function: Specifies the prefix and prefix length requested by the client. The **no** form of this command deletes them from the interface.

Parameters: <prefix|prefix-length>: The prefix and prefix length requested by the client.

Command Mode: Interface Mode.

Default: Not configured.

Usage Guidelines: This command specifies a preferred prefix and length on the interface for the client. If the prefix delegation client is enabled on the interface and the hint function is enabled on the

server, the server gives priority to the requested prefix and length when allocating. Only one hint prefix is allowed in the system.

Example:

```
Switch(vlan-1-config)#ipv6 dhcp client pd hint 2001::/48
```

13.1.14 ipv6 dhcp pool

Command: ipv6 dhcp pool <poolname>
no ipv6 dhcp pool <poolname>

Function: Configures a DHCPv6 address pool and enters DHCPv6 Address Pool Mode, in which the address prefix to allocate, DNS server addresses, domain names, and other information for DHCPv6 clients can be configured. The **no** form of this command removes the address pool.

Parameters: <poolname> is the DHCPv6 address pool name, up to 32 characters.

Default: No DHCPv6 address pool is configured.

Command Mode: Global Mode.

Usage Guidelines: Run this command in Global Mode; if it succeeds, the device enters DHCPv6 Address Pool Mode. When an address pool is removed, its interface bindings and the related address bindings are also removed.

Example: Define an address pool named 1.

```
Switch(config)#ipv6 dhcp pool 1
```

13.1.15 ipv6 dhcp relay destination

Command: ipv6 dhcp relay destination {[<ipv6-address>] [interface
{ <interface-name> | vlan <1-4096> }] }
no ipv6 dhcp relay destination { [<ipv6-address>] [interface
{ <interface-name> | vlan <1-4096> }] }

Function: Configures the destination to which the DHCPv6 relay forwards client requests; the destination must be another DHCPv6 relay or a DHCPv6 server. The **no** form of this command removes the configuration.

Parameters: <ipv6-address> is the destination address to which the DHCPv6 relay forwards requests. **<interface-name>** or **vlan** is the interface name or VLAN ID used to forward DHCPv6 requests; **<interface-name>** must be a Layer 3 VLAN interface name, and the VLAN ID ranges from 1 to 4096. If **<ipv6-address>** is a global unicast address, do not configure the interface parameter. If **<ipv6-address>** is a link-local address, the interface parameter is required. If only the interface parameter is configured, the destination is the All_DHCP_Servers multicast address (FF05::1:3).

Command Mode: Interface Mode.

Default: No DHCPv6 relay destination address is configured.

Usage Guidelines: This command configures the DHCPv6 relay on the specified interface. The address must be that of another DHCPv6 relay or a DHCPv6 server. Up to three relay addresses can be configured per interface. The DHCPv6 relay stops working only after all relay destination addresses are removed. This command is mutually exclusive with **ipv6 dhcp server** and **ipv6 dhcp client pd**.

Example:

```
Switch(Config-if-Vlan1)#ipv6 dhcp relay destination 2001:da8::1
```

13.1.16 ipv6 dhcp server

Command: ipv6 dhcp server <poolname> [preference <value>] [rapid-commit] [allow-hint]
no ipv6 dhcp server <poolname>

Function: Configures the address pool that the DHCPv6 server allocates through the specified interface. The **no** form of this command removes the configuration.

Parameters: <poolname> is a string of less than 32 characters that names the address pool associated with the interface. With **rapid-commit**, the DHCPv6 server sends a REPLY packet to the client immediately after receiving a SOLICIT packet. With **preference**, **<value>** is the priority of the DHCPv6 server, ranging from 0 to 255 (default 0); a larger value means a higher priority. With **allow-hint**, the parameter values requested by the client are taken into account.

Command Mode: Interface Mode.

Default: No DHCPv6 address pool is configured on the interface.

Usage Guidelines: This command configures the DHCPv6 address pool used by the DHCPv6 server on the specified interface, with optional parameters. A VLAN can be bound to multiple DHCPv6 address pools and allocate addresses for DHCPv6 requests received directly or through a relay.

Example:

```
Switch(Config-if-Vlan1)#ipv6 dhcp server PoolA preference 80 rapid-commit
allow-hint
```

13.1.17 ipv6 general-prefix

Command: ipv6 general-prefix <prefix-name> <ipv6-prefix/prefix-length>
no ipv6 general-prefix <prefix-name>

Function: Defines an IPv6 general prefix. The **no** form of this command deletes it.

Parameters: <prefix-name> is a string of less than 32 characters used as the general prefix name. **<ipv6-prefix/prefix-length>** is the prefix defined as the IPv6 general prefix.

Command Mode: Global Mode.

Default: No IPv6 general prefix is configured.

Usage Guidelines: When an IPv6 general prefix is configured, interfaces can use it to generate IPv6 addresses. A general prefix is commonly used for an enterprise IPv6 prefix; when entering an IPv6 address, users only append the address suffix to the general prefix name. The configured prefix is kept in the general prefix pool. Up to eight general prefixes can be configured at the same time. Removing a general prefix name fails if any interface uses the prefix. Only one prefix can be defined for each prefix name. A general prefix cannot use the same prefix as one learned through prefix delegation.

Example: Define 2001:da8:221::/48 as general prefix my-prefix.

```
Switch(config)# ipv6 general-prefix my-prefix 2001:da8:221::/48
```

13.1.18 ipv6 local pool

Command: ipv6 local pool <poolname> <prefix/prefix-length> <assigned-length>
no ipv6 local pool <poolname>

Function: Configures the address pool for prefix delegation. The **no** form of this command removes the configuration.

Parameters: <poolname> is the name of the IPv6 prefix delegation pool, less than 32 characters. **<prefix/prefix-length>** is the prefix and prefix length of the pool. **<assigned-length>** is the length of the prefix that a client can obtain from the pool; it must be no less than **<prefix-length>**.

Command Mode: Global Mode.

Default: No IPv6 prefix delegation pool is configured.

Usage Guidelines: Use this command with the **prefix-delegation pool** command to allocate prefixes to clients. If the IPv6 prefix delegation pool is removed, the associated **prefix-delegation pool** command no longer takes effect.

13.1.19 lifetime

Command: `lifetime {<valid-time> | infinity} {<preferred-time> | infinity}`
`no lifetime`

Function: Configures the lifetimes of the addresses or prefixes allocated by DHCPv6. The **no** form of this command restores the defaults.

Parameters: <valid-time> and **<preferred-time>** are the valid lifetime and preferred lifetime of the IPv6 addresses allocated from the local address pool, ranging from 1 to 31536000 seconds. **<preferred-time>** must not exceed **<valid-time>**. **infinity** specifies the maximum lifetime.

Command Mode: DHCPv6 Address Pool Mode.

Default: The valid lifetime is 2592000 seconds (30 days), and the preferred lifetime is 604800 seconds (7 days).

Example: Set the valid lifetime to 1000 seconds and the preferred lifetime to 600 seconds.

```
Switch(dhcpv6-1-1config)#lifetime 1000 600
```

13.1.20 network-address

Command: `network-address <ipv6-pool-start-address> {<ipv6-pool-end-address> | <prefix-length>} [eui-64]`
`no network-address`

Function: Configures the DHCPv6 address pool range. The **no** form of this command removes it.

Parameters: <ipv6-pool-start-address> is the start of the address pool. **<ipv6-pool-end-address>** is the end of the address pool. **<prefix-length>** is the prefix length, ranging from 3 to 128 (default 64); if specified, it determines the size of the pool. **<ipv6-pool-end-address>** and **<prefix-length>** are alternative ways to set the pool size. If **<prefix-length>** is 64 and **eui-64** is configured, the DHCPv6 server allocates addresses according to EUI-64; otherwise, it allocates addresses sequentially.

Default: No address pool range is configured.

Command Mode: DHCPv6 Address Pool Mode.

Usage Guidelines: This command configures the address range that the DHCPv6 server allocates from the pool. Only one address range can be configured for each address pool. If the DHCPv6 server is enabled and the IPv6 prefix length is configured, the prefix length of the pool must be no less than the prefix length of the IPv6 address of the corresponding Layer 3 interface on the switch. If **<ipv6-pool-end-address>** is greater than **<ipv6-pool-start-address>**, this command returns immediately.

Example: Set the address range of the pool to 2001:da8:123::100-2001:da8:123::200.

```
Switch(dhcpv6-1-config)#network-address 2001:da8:123::100 2001:da8:123::200
```

Related Commands: excluded-address

13.1.21 prefix-delegation

Command: prefix-delegation <ipv6-prefix/prefix-length> <client-DUID> [iaid <iaid>] [lifetime {<valid-time> | infinity} {<preferred-time> | infinity}]
no prefix-delegation <ipv6-prefix/prefix-length> <client-DUID> [iaid <iaid>]

Function: Configures a dedicated prefix delegation for the specified client. The **no** form of this command removes it.

Parameters: <ipv6-prefix/prefix-length> is the prefix and length allocated to the client. **<client-DUID>** is the DUID of the client; DUID-LLT and DUID-LL types are supported, and a DUID-LLT DUID must be 14 characters. **<iaid>** is the value carried in the IA_PD field of client requests. **<valid-time>** and **<preferred-time>** are the valid and preferred lifetimes of the allocated prefix in seconds, ranging from 1 to 31536000; **<preferred-time>** must not exceed **<valid-time>**. If not configured, the valid lifetime is 2592000 seconds and the preferred lifetime is 604800 seconds. **infinity** specifies an infinite lifetime.

Command Mode: DHCPv6 Address Pool Mode.

Default: None.

Usage Guidelines: This command binds the specified IPv6 prefix to the specified client. If no IAID is configured, any IA of the client can obtain the prefix. Up to eight static prefix bindings can be configured for each address pool. For prefix delegation, static bindings have higher priority than the prefix pool.

Example: Allocate 2001:da8::/48 to the client with DUID 00010006000000005000BBFAA2408 and IAID 12.

```
Switch(dhcp-1-config)#prefix-delegation 2001:da8::/48
00010006000000005000BBFAA2408 iaid 12
```

13.1.22 prefix-delegation pool

Command: prefix-delegation pool <poolname> [lifetime {<valid-time> | infinity} {<preferred-time> | infinity}]
no prefix-delegation pool <poolname>

Function: Configures the prefix delegation pool used by the DHCPv6 address pool. The **no** form of this command deletes the configuration.

Parameters: <poolname> is the name of the prefix pool, less than 32 characters. **<valid-time>** and **<preferred-time>** are the valid and preferred lifetimes of the allocated prefix in seconds, ranging from 1 to 31536000; **<preferred-time>** must not exceed **<valid-time>**. If not configured, the valid lifetime is 2592000 seconds and the preferred lifetime is 604800 seconds. **infinity** specifies an infinite lifetime.

Command Mode: DHCPv6 Address Pool Mode.

Default: Not configured.

Usage Guidelines: This command configures the prefix pool used for allocation; prefixes in that pool are then allocated to clients. Use it with the **ipv6 local pool** command. Only one prefix delegation pool can be bound to an address pool. If the prefix pool configuration is removed while the address pool has no other prefix pool and no static prefix delegation binding, the prefix delegation service of the server becomes unavailable.

Example:

```
Switch(dhcpv6-1-config)#prefix-delegation pool abc
```

13.1.23 service dhcpv6

Command: `service dhcpv6`
`no service dhcpv6`

Function: Enables the DHCPv6 service. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: DHCPv6 services include the DHCPv6 server, DHCPv6 relay, and DHCPv6 prefix delegation functions, all configured on ports. The DHCPv6 client address assignment, DHCPv6 relay, and DHCPv6 prefix delegation functions configured on ports take effect only when this service is enabled.

Example: Enable the DHCPv6 service.

```
Switch(config)#service dhcpv6
```

13.1.24 show ipv6 dhcp

Command: `show ipv6 dhcp`

Function: Displays whether the DHCPv6 service is enabled and the DUID of the DHCPv6 service.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays whether the DHCPv6 service is enabled and its DUID. The server identifier option uses only the DUID-LLT DUID.

Example:

```
Switch#show ipv6 dhcp
DHCPv6 is enabled
LLT DUID is <00:01:00:01:43:b7:1b:81:00:03:0f:01:5f:9d>
LL DUID is <00:03:00:01:00:03:0f:01:5f:9d>
```

13.1.25 show ipv6 dhcp binding

Command: `show ipv6 dhcp binding [<ipv6-address>| pd <ipv6-prefix|prefix-length>|count]`

Function: Displays all DHCPv6 address and prefix binding information.

Parameters: <ipv6-address> is the specified IPv6 address. **count** displays the number of DHCPv6 address bindings.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays all DHCPv6 address and prefix binding information, including type, DUID, IAID, prefix, and valid lifetime.

Example:

```
Switch#show ipv6 dhcp binding
Client: iatype IANA, iaid 0x0e001d92
DUID: 00:01:00:01:0f:55:82:4f:00:19:e0:3f:d1:83
IANA leased address: 2001:da8::10
Preferred lifetime 604800 seconds, valid lifetime 2592000 seconds
Lease obtained at %Jan 01 01:34:44 1970
Lease expires at %Jan 31 01:34:44 1970 (2592000 seconds left)
The number of DHCPv6 bindings is 1
```

13.1.26 show ipv6 dhcp conflict

Command: `show ipv6 dhcp conflict`

Function: Displays the log of addresses with conflict records.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch# show ipv6 dhcp conflict
```

13.1.27 show ipv6 dhcp interface

Command: `show ipv6 dhcp interface [<interface-name>]`

Function: Displays DHCPv6 interface information.

Parameters: <interface-name> is the interface name and number. If it is not specified, information about all DHCPv6 interfaces is displayed.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays DHCPv6 interface information, including the interface mode (prefix delegation client, DHCPv6 server, or DHCPv6 relay) and the related configuration in each mode.

Example:

```
Switch#show ipv6 dhcp interface vlan10
Vlan10 is in server mode
Using pool: poolv6
Preference value: 20
Rapid-Commit is disabled
```

13.1.28 show ipv6 dhcp pool

Command: `show ipv6 dhcp pool [<poolname>]`

Function: Displays DHCPv6 address pool information.

Parameters: <poolname> is the name of a configured DHCPv6 address pool, less than 32 characters. If it is not specified, information about all DHCPv6 address pools is displayed.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the configuration and dynamic allocation information of DHCPv6 address pools, including the pool name, pool prefix, excluded addresses, DNS server configuration, and related prefix information. For a pool used for address assignment, the number of address bindings is displayed; for a pool used for prefix delegation, the number of delegated prefixes is displayed.

Example:

```
Switch#show ipv6 dhcp pool poolv6
```

13.1.29 show ipv6 dhcp statistics

Command: `show ipv6 dhcp statistics`

Function: Displays statistics of DHCPv6 packets of all types handled by the DHCPv6 server.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch#show ipv6 dhcp server statistics
Address pools                    1
Active bindings                   0
Expiried bindings                 0
Malformed message              0
Message                  Received
```

```
DHCP6SOLICIT                0
DHCP6ADVERTISE              0
DHCP6REQUEST                0
DHCP6REPLY                  0
DHCP6RENEW                  0
DHCP6REBIND                 0
DHCP6RELEASE                0
DHCP6DECLINE                0
DHCP6CONFIRM                0
DHCP6RECONFIGURE            0
DHCP6INFORMREQ              0
DHCP6RELAYFORW              0
DHCP6RELAYREPLY             0
Message                     Send
DHCP6SOLICIT                0
DHCP6ADVERTISE              0
DHCP6REQUEST                0
DHCP6REPLY                  0
DHCP6RENEW                  0
DHCP6REBIND                 0
DHCP6RELEASE                0
DHCP6DECLINE                0
DHCP6CONFIRM                0
DHCP6RECONFIGURE            0
DHCP6INFORMREQ              0
DHCP6RELAYFORW              0
DHCP6RELAYREPLY             0
```

Output	Description
Address pools	Number of configured DHCPv6 address pools
Active bindings	Number of dynamically assigned addresses
Expiried bindings	Number of expired bindings
Malformed message	Number of malformed messages
Message Received	Statistics of received DHCPv6 packets
DHCP6SOLICIT	The number of DHCPv6 SOLICIT packets.
DHCP6ADVERTISE	The number of DHCPv6 ADVERTISE packets.
DHCPv6REQUEST	The number of DHCPv6 REQUEST packets.
DHCP6REPLY	The number of DHCPv6 REPLY packets.
DHCP6RENEW	The number of DHCPv6 RENEW packets.
DHCP6REBIND	The number of DHCPv6 REBIND packets.
DHCP6RELEASE	The number of DHCPv6 RELEASE packets.
DHCP6DECLINE	The number of DHCPv6 DECLINE packets.
DHCP6CONFIRM	The number of DHCPv6 CONFIRM packets.
DHCP6RECONFIGURE	The number of DHCPv6 RECONFIGURE packets.
DHCP6INFORMREQ	The number of DHCPv6 INFORMREQ packets.
DHCP6RELAYFORW	The number of DHCPv6 RELAYFORW packets.
DHCP6RELAYREPLY	The number of DHCPv6 RELAYREPLY packets.
Message Send	Statistics of sent DHCPv6 packets
DHCP6SOLICIT	The number of DHCPv6 SOLICIT packets.
DHCP6ADVERTISE	The number of DHCPv6 ADVERTISE packets.
DHCPv6REQUEST	The number of DHCPv6 REQUEST packets.
DHCP6REPLY	The number of DHCPv6 REPLY packets.
DHCP6RENEW	The number of DHCPv6 RENEW packets.
DHCP6REBIND	The number of DHCPv6 REBIND packets.
DHCP6RELEASE	The number of DHCPv6 RELEASE packets.
DHCP6DECLINE	The number of DHCPv6 DECLINE packets.
DHCP6CONFIRM	The number of DHCPv6 CONFIRM packets.

DHCP6RECONFIGURE	The number of DHCPv6 RECONFIGURE packets.
DHCP6INFORMREQ	The number of DHCPv6 INFORMREQ packets.
DHCP6RELAYFORW	The number of DHCPv6 RELAYFORW packets.

13.1.30 show ipv6 general-prefix

Command: `show ipv6 general-prefix`

Function: Displays IPv6 general prefix pool information.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays IPv6 general prefix pool information, including the number of prefixes in the pool, the name of each prefix, the interface from which each prefix was obtained, and the prefix value.

Example:

```
Switch#show ipv6 general-prefix
```

13.1.31 show ipv6 local pool

Command: `show ipv6 local pool`

Function: Displays DHCPv6 prefix pool statistics.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays DHCPv6 prefix pool statistics, including the prefix pool name, prefix and prefix length, assigned prefix length, number of assigned prefixes, and the related DHCPv6 address pool information.

Example:

```
Switch#show ipv6 local pool
Pool       Prefix            Free        In use
a          2010::1/48        65536      0
```

13.2 DHCPv6 option37, 38

13.2.1 Commands for DHCPv6 option37, 38

13.2.1.1 address range

Command: `address range <start-ip> <end-ip>`
`no address range <start-ip> <end-ip>`

Function: Configures the address range of a DHCPv6 class in a DHCPv6 address pool. The **no** form of this command removes the address range. The prefix/prefix-length format is not supported.

Parameters: <start-ip>: The start address of the range.

<end-ip>: The end address of the range.

Default: None.

Command Mode: DHCPv6 Address Pool Class Mode.

Usage Guidelines: Make sure that the address range assigned to the class does not exceed the address range of the address pool. Each class is assigned one address range; the ranges of different classes in the same address pool can overlap. If no address range is assigned to a DHCPv6 class, the class uses the whole subnet of the address pool by default.

Example: Associate DHCPv6 class CLASS1 with DHCPv6 pool 1 and assign the address range 2001:da8:100:1::2 to 2001:da8:100:1::30 to CLASS1.

```
Switch(Config)#ipv6 dhcp pool 1
```

```
Switch(dhcp-1-config)#class CLASS1
Switch(dhcp-1-class-CLASS1-config)#address range 2001:da8:100:1::2
2001:da8:100:1::30
```

13.2.1.2 class

Command: `class <class-name>`
`no class <class-name>`

Function: Associates a class with the address pool and enters the class mode of the address pool. The **no** form of this command removes the association.

Parameters: <class-name>: The name of the DHCPv6 class.

Default: None.

Command Mode: DHCPv6 Address Pool Mode.

Usage Guidelines: Define the class first with the global **ipv6 dhcp class** command. If the specified class does not exist, no class is created.

Example: Associate DHCPv6 class CLASS1 with DHCPv6 pool 1.

```
Switch(Config)#ipv6 dhcp pool 1
Switch(dhcp-1-config)#class CLASS1
```

13.2.1.3 ipv6 dhcp class

Command: `ipv6 dhcp class <class-name>`
`no ipv6 dhcp class <class-name>`

Function: Defines a DHCPv6 class and enters DHCPv6 Class Mode. The **no** form of this command removes the class.

Parameters: <class-name>: The name of the DHCPv6 class, less than 32 characters.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: In a DHCPv6 class, configure a set of option 37 entries, option 38 entries, or both. This command can be used only when the server supports DHCPv6 classes.

Example: Define DHCPv6 class CLASS1.

```
Switch(Config)# ipv6 dhcp class CLASS1
```

13.2.1.4 ipv6 dhcp relay remote-id

Command: `ipv6 dhcp relay remote-id <remote-id>`
`no ipv6 dhcp relay remote-id`

Function: Configures the content of option 37 added to received DHCPv6 request packets. **<remote-id>** is the user-defined remote-id of option 37, a string of less than 128 characters. The **no** form of this command restores the remote-id of option 37 to the enterprise number and the VLAN MAC address.

Parameters: <remote-id>: The user-defined content of option 37.

Default: The VLAN MAC address is used as the remote ID, for example "00-01-ac-12-23" with hyphens.

Command Mode: Interface Mode.

Usage Guidelines: Because the option 37 information added by the switch may be used by third-party DHCPv6 servers, specify the remote-id content according to the server when the default remote-id of the switch does not meet the server's requirements. By default, the enterprise number and the VLAN MAC address are used as the remote ID.

Example: Set the remote-id of DHCPv6 option 37 to abc.

```
Switch(Config-if-vlan1)# ipv6 dhcp relay remote-id abc
```

13.2.1.5 ipv6 dhcp relay remote-id option

Command: ipv6 dhcp relay remote-id option
no ipv6 dhcp relay remote-id option

Function: Enables the switch relay to support option 37. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Only after this command is configured can the DHCPv6 relay agent add option 37 to DHCPv6 request packets before sending them to the server or the next relay agent. Make sure the DHCPv6 service is enabled before running this command.

Example: Enable the switch relay to support option 37.

```
Switch(Config)#service dhcpv6
Switch(Config)#ipv6 dhcp relay remote-id option
```

13.2.1.6 ipv6 dhcp relay subscriber-id

Command: ipv6 dhcp relay subscriber-id <subscriber-id>
no ipv6 dhcp relay subscriber-id

Function: Configures the content of option 38 added to received DHCPv6 request packets. **<subscriber-id>** is the user-defined subscriber-id of option 38, a string of less than 128 characters. The **no** form of this command restores the subscriber-id of option 38 to the VLAN name and port name, such as "Vlan2+Ethernet1/0/2".

Parameters: <subscriber-id>: The user-defined content of option 38.

Default: The subscriber ID of option 38 is the VLAN name and port name.

Command Mode: Interface Mode.

Usage Guidelines: Because the option 38 information added by the switch may be used by third-party DHCPv6 servers, specify the subscriber-id content according to the server when the default subscriber-id of the switch does not meet the server's requirements. By default, the VLAN name and physical port name are used as the subscriber ID.

Example: Set the subscriber-id of DHCPv6 option 38 to abc.

```
Switch(Config-if-vlan1)# ipv6 dhcp relay subscriber-id abc
```

13.2.1.7 ipv6 dhcp relay subscriber-id option

Command: ipv6 dhcp relay subscriber-id option
no ipv6 dhcp relay subscriber-id option

Function: Enables the switch relay to support option 38. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Only after this command is configured can the DHCPv6 relay agent add option 38 to DHCPv6 request packets before sending them to the server or the next relay agent. Make sure the DHCPv6 service is enabled before running this command.

Example: Enable the switch relay to support option 38.

```
Switch(Config)#service dhcpv6
Switch(Config)#ipv6 dhcp relay subscriber-id option
```

13.2.1.8 ipv6 dhcp relay subscriber-id select delimiter

Command: `ipv6 dhcp relay subscriber-id select (sp | sv | pv | spv) delimiter WORD (delimiter WORD |)`
`no ipv6 dhcp relay subscriber-id select delimiter`

Function: Configures the user options used to generate the subscriber ID. The **no** form of this command restores the default, the VLAN name and port name.

Parameters: (sp | sv | pv | spv): The combination of slot, port, and VLAN: **sp** is slot and port, **sv** is slot and VLAN, **pv** is port and VLAN, and **spv** is slot, port, and VLAN.

WORD: The delimiter between slot, port, and VLAN: #, ., ,, ;, :, /, or space. There are two **delimiter WORD** parameters: the first is the delimiter between slot and port, and the second is the delimiter between port and VLAN.

Default: Not configured.

Command Mode: Global Mode.

Usage Guidelines: This command has no effect on ports with a user-defined subscriber ID. If the subscriber ID of a port is redefined after this command is used, the user-defined subscriber ID takes precedence.

Example:

```
Switch(config)# ipv6 dhcp relay subscriber-id select sp delimiter #
```

13.2.1.9 ipv6 dhcp server remote-id option

Command: `ipv6 dhcp server remote-id option`
`no ipv6 dhcp server remote-id option`

Function: Enables the DHCPv6 server to recognize option 37. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Configure this command if the DHCPv6 server is to recognize and process option 37; otherwise, the option is ignored.

Example: Enable the DHCPv6 server to support option 37.

```
Switch(Config)# ipv6 dhcp server remote-id option
```

13.2.1.10 ipv6 dhcp server select relay-forw

Command: `ipv6 dhcp server select relay-forw`
`no ipv6 dhcp server select relay-forw`

Function: When multiple option 37 or option 38 options exist, configures the DHCPv6 server to select option 37 and option 38 from the innermost relay-forw layer. The **no** form of this command restores the default, which selects option 37 and option 38 of the original packet.

Parameters: None.

Default: Option 37 and option 38 of the original packet are selected.

Command Mode: Interface Mode.

Usage Guidelines: Make sure the server is enabled to support option 37 and option 38 before using this command.

Example: Configure the VLAN 1 interface of the DHCPv6 server to select option 37 and option 38 from the innermost relay-forw layer.

```
Switch(Config-if-vlan1)# ipv6 dhcp server select relay-forw
```

13.2.1.11 ipv6 dhcp server subscriber-id option

Command: `ipv6 dhcp server subscriber-id option`
`no ipv6 dhcp server subscriber-id option`

Function: Enables the DHCPv6 server to recognize option 38. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Configure this command if the DHCPv6 server is to recognize and process option 38; otherwise, the option is ignored.

Example: Enable the DHCPv6 server to support option 38.

```
Switch(Config)# ipv6 dhcp server subscriber-id option
```

13.2.1.12 ipv6 dhcp snooping information option subscriber-id format

Command: `ipv6 dhcp snooping information option subscriber-id format {hex | acsii }`

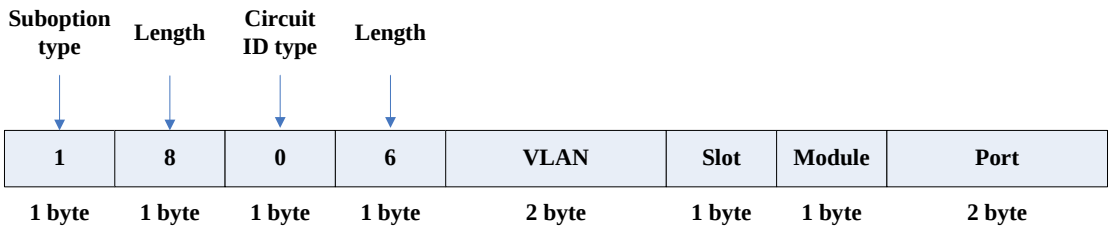
Function: Configures the default subscriber ID format of DHCPv6 snooping option 38 on the switch.

Parameters: hex: The subscriber ID is the VLAN and port information in hexadecimal. **acsii**: The subscriber ID is the VLAN and port information in ASCII.

Default: ASCII.

Command Mode: Global Mode.

Usage Guidelines: The ASCII VLAN and port information has the form Vlan1+Ethernet1/0/11. The hexadecimal VLAN and port information is defined as follows:



The VLAN field contains the switch VLAN ID. For a chassis switch, Slot is the slot number; for a box switch, it is 1. Module is 0 by default. Port is the port number, starting from 1.

Example: Set the subscriber ID format of DHCPv6 snooping option 38 to hexadecimal.

```
Switch(config)#ipv6 dhcp snooping information option subscriber-id format hex
```

13.2.1.13 ipv6 dhcp snooping remote-id

Command: `ipv6 dhcp snooping remote-id <remote-id>`
`no ipv6 dhcp snooping remote-id`

Function: Configures the content of option 37 added to received DHCPv6 request packets. **<remote-id>** is the user-defined remote ID of option 37, a string of less than 128 characters. The **no** form of this command restores the remote ID of option 37 to the enterprise number and the VLAN MAC address.

Parameters: <remote-id>: The user-defined content of option 37.

Default: The VLAN MAC address is used as the remote ID, for example "00-01-ac-12-23" with hyphens.

Command Mode: Port Mode.

Usage Guidelines: Because the option 37 information added by the switch may be used by third-party DHCPv6 servers, specify the remote ID content according to the server when the default remote ID of the switch does not meet the server's requirements. By default, the enterprise number and the VLAN MAC address are used as the remote ID.

Example: Set the remote ID of DHCPv6 option 37 to abc.

```
Switch(Config-if-Ethernet1/0/1)# ipv6 dhcp snooping remote-id abc
```

13.2.1.14 ipv6 dhcp snooping remote-id option

Command: `ipv6 dhcp snooping remote-id option`
`no ipv6 dhcp snooping remote-id option`

Function: Enables DHCPv6 snooping to support option 37. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Only after this command is configured can DHCPv6 snooping add option 37 to DHCPv6 packets before sending them to the server or relay agent. Make sure DHCPv6 snooping is enabled before running this command.

Example: Enable option 37 for DHCPv6 snooping.

```
Switch(Config)#ipv6 dhcp snooping enable
Switch(Config)#ipv6 dhcp snooping remote-id option
```

13.2.1.15 ipv6 dhcp snooping remote-id policy

Command: `ipv6 dhcp snooping remote-id policy {drop | keep | replace}`
`no ipv6 dhcp snooping remote-id policy`

Function: Configures how the system forwards received DHCPv6 packets that contain option 37. In **drop** mode, the system discards the packets. In **keep** mode, the system keeps option 37 unchanged and forwards the packets to the server. In **replace** mode, the system replaces option 37 of the packets with its own before forwarding them to the server. The **no** form of this command sets the policy to **replace**.

Parameters: drop, **keep**, and **replace**, as described above.

Default: replace; option 37 of the packets is replaced with the system's own.

Command Mode: Global Mode.

Usage Guidelines: DHCPv6 client packets may already contain option 37, so DHCPv6 snooping needs a processing policy for them. If the policy is **replace**, option 37 must be enabled first.

Example: Set the DHCPv6 snooping forwarding policy for packets with option 37 to keep.

```
Switch(Config)# ipv6 dhcp snooping remote-id policy keep
```

13.2.1.16 ipv6 dhcp snooping subscriber-id

Command: `ipv6 dhcp snooping subscriber-id <subscriber-id>`
`no ipv6 dhcp snooping subscriber-id`

Function: Configures the content of option 38 added to received DHCPv6 request packets. **<subscriber-id>** is the user-defined subscriber ID of option 38, a string of less than 128 characters. The **no** form of this command restores the subscriber ID of option 38 to the VLAN name and port name, such as "Vlan2+Ethernet1/0/2".

Parameters: <subscriber-id>: The user-defined content of option 38.

Default: The subscriber ID of option 38 is the VLAN name and port name.

Command Mode: Port Mode.

Usage Guidelines: Because the option 38 information added by the switch may be used by third-party DHCPv6 servers, specify the subscriber ID content according to the server when the default subscriber ID of the switch does not meet the server's requirements. By default, the VLAN name and physical port name are used as the subscriber ID.

Example: Set the subscriber ID of DHCPv6 option 38 to abc.

```
Switch(Config-if-Ethernet1/0/1)#ipv6 dhcp snooping subscriber-id abc
```

13.2.1.17 ipv6 dhcp snooping subscriber-id option

Command: ipv6 dhcp snooping subscriber-id option
no ipv6 dhcp snooping subscriber-id option

Function: Enables DHCPv6 snooping to support option 38. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Only after this command is configured can DHCPv6 snooping add option 38 to DHCPv6 packets before sending them to the server or relay agent. Make sure DHCPv6 snooping is enabled before running this command.

Example: Enable option 38 for DHCPv6 snooping.

```
Switch(Config)#ipv6 dhcp snooping enable
Switch(Config)#ipv6 dhcp snooping subscriber-id option
```

13.2.1.18 ipv6 dhcp snooping subscriber-id policy

Command: ipv6 dhcp snooping subscriber-id policy {drop | keep | replace}
no ipv6 dhcp snooping subscriber-id policy

Function: Configures how the system forwards received DHCPv6 packets that contain option 38. In **drop** mode, the system discards the packets. In **keep** mode, the system keeps option 38 unchanged and forwards the packets to the server. In **replace** mode, the system replaces option 38 of the packets with its own before forwarding them to the server. The **no** form of this command sets the policy to **replace**.

Parameters: drop, **keep**, and **replace**, as described above.

Default: replace; option 38 of the packets is replaced with the system's own.

Command Mode: Global Mode.

Usage Guidelines: DHCPv6 client packets may already contain option 38, so DHCPv6 snooping needs a processing policy for them. If the policy is **replace**, option 38 must be enabled first.

Example: Set the DHCPv6 snooping forwarding policy for packets with option 38 to keep.

```
Switch(Config)# ipv6 dhcp snooping subscriber-id policy keep
```

13.2.1.19 ipv6 dhcp snooping subscriber-id select delimiter

Command: ipv6 dhcp snooping subscriber-id select (sp | sv | pv | spv)
delimiter WORD (delimiter WORD |)
no ipv6 dhcp snooping subscriber-id select delimiter

Function: Configures the user options used to generate the subscriber ID. The **no** form of this command restores the default, the VLAN name and port name.

Parameters: (sp | sv | pv | spv): The combination of slot, port, and VLAN: **sp** is slot and port, **sv** is slot and VLAN, **pv** is port and VLAN, and **spv** is slot, port, and VLAN.

WORD: The delimiter between slot, port, and VLAN: #, ., ,, ;, :, /, or space. There are two **delimiter WORD** parameters: the first is the delimiter between slot and port, and the second is the delimiter between port and VLAN.

Default: Not configured.

Command Mode: Global Mode.

Usage Guidelines: This command has no effect on ports with a user-defined subscriber ID. If the subscriber ID of a port is redefined after this command is configured, the user-defined subscriber ID takes precedence.

Example:

```
Swithc(config)# ipv6 dhcp snooping subscriber-id select sv delimiter #
```

13.2.1.20 ipv6 dhcp use class

Command: ipv6 dhcp use class
no ipv6 dhcp use class

Function: Enables the DHCPv6 server to use DHCPv6 classes during address assignment. The **no** form of this command disables it without removing the configured DHCPv6 class information.

Parameters: None.

Default: Enabled.

Command Mode: Global Mode.

Usage Guidelines: The **no** form of this command does not remove the configured DHCPv6 class information. Make sure the DHCPv6 service is enabled before using this command.

Example: Enable the DHCPv6 server to use DHCPv6 classes during address assignment.

```
Switch(Config)# ipv6 dhcp use class
```

13.2.1.21 remote-id subscriber-id

Command: {remote-id [*] <remote-id> [*] | subscriber-id [*] <subscriber-id> [*]}
no {remote-id [*] <remote-id> [*] | subscriber-id [*] <subscriber-id> [*]}

Function: Configures the option 37 and option 38 values that match the class, in DHCPv6 Class Mode.

Parameters: <remote-id>: A string of 1 to 128 bytes used to match the remote ID in option 37.

<subscriber-id>: A string of 1 to 128 bytes used to match the subscriber ID in option 38.

[*]: Matches zero or more characters.

Default: None.

Command Mode: DHCPv6 Class Mode.

Usage Guidelines: This command configures a match pattern for an existing DHCPv6 class; multiple patterns can be configured for a class. If no pattern is configured in the class, any remote ID or subscriber ID matches the class, but the remote ID or subscriber ID must be present in the DHCPv6 packet.

Example: Configure remote IDs and subscriber IDs that belong to DHCPv6 class CLASS1.

```
Switch(Config)# ipv6 dhcp class CLASS1
Switch(Dhcpv6-class)#remote-id abc* subscriber-id bcd*
Switch(Dhcpv6-class)#remote-id edf*
Switch(Dhcpv6-class)#subscriber *mmn
```

13.2.2 Commands for Monitoring and Debugging

13.2.2.1 debug ipv6 dhcp detail

Command: `debug ipv6 dhcp detail`

Function: Displays detailed debugging of the packets sent and received by DHCPv6, including option 37 and option 38 when present. This command applies to both the server and the relay.

Parameters: None.

Command Mode: Admin Mode.

Usage Guidelines: Enables or disables the display of detailed debugging of packets sent and received by DHCPv6.

Example:

```
Switch# debug ipv6 dhcp detail
%Jan 01 01:38:45 2006 DHCPv6 DETAILS: contents of SOLICIT packet
%Jan 01 01:38:45 2006     transaction-ID: 0x00b2d47c
%Jan 01 01:38:45 2006   elapsed time option(8), option-len 2
%Jan 01 01:38:45 2006     elapsed time: 0
%Jan 01 01:38:45 2006   client ID option(1), option-len 14
%Jan 01 01:38:45 2006     DUID: 00:01:00:01:0f:55:82:4f:00:19:e0:3f:d1:83
%Jan 01 01:38:45 2006   identity association option(3), option-len 12
%Jan 01 01:38:45 2006     IANA: 0x0e001d92, T1 0, T2 0
%Jan 01 01:38:45 2006   vendor class option(16), option-len 14
%Jan 01 01:38:45 2006     enterprise number : 311
%Jan 01 01:38:45 2006   option request option(6), option-len 6
%Jan 01 01:38:45 2006     requested-option: domain search list
%Jan 01 01:38:45 2006     requested-option: DNS server list
%Jan 01 01:38:45 2006     requested-option: vendor specific info
%Jan 01 01:38:45 2006   remote-id option(37), option-len 14
%Jan 01 01:38:45 2006     remote-id : 0x0a0b0c
%Jan 01 01:38:45 2006   subscriber-id option(38), option-len 16
%Jan 01 01:38:45 2006     subscriber-id : 0x0a0b0c0d
```

13.2.2.2 debug ipv6 dhcp relay packet

Command: `debug ip dhcp relay packet`

Function: Displays information about relay packet processing.

Parameters: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays how the relay agent processes relay packets, including the actions taken on option 37 and option 38.

Example:

```
Switch# debug ip dhcpv6 relay packet
%May 19 16:45:34 2010 DHCPv6 RELAY PACKET: received msg0 from
<fe80::211:22ff:fe33:4455> on <Vlan8>
%May 19 16:45:34 2010 DHCPv6 RELAY PACKET: add subscriber-id option
“Vlan8+Ethernet1/0/12”
```

13.2.2.3 debug ipv6 dhcp snooping packet

Command: `debug ipv6 dhcp snooping packet`

Function: Debugs DHCPv6 snooping packets. Information is also displayed when option 37 or option 38 is added or deleted.

Parameters: None.

Command Mode: Admin Mode.

Usage Guidelines: Enables or disables the display of DHCPv6 packets processed by DHCPv6 snooping, including the received packet type, source and destination MAC addresses, client DUID, IA address, preferred lifetime, valid lifetime, and packet discards.

Example:

```
switch#debug ipv6 dhcp snooping packet
dhcpv6 snooping packet debug is on
switch#%Jan 05 00:26:40 2006 DHCP6SNP EVENT: Parse packet SOLICIT from
fe80::200:ff:fe00:1
    src MAC 00-00-00-00-00-01 interface Ethernet1/0/23 vlan 24
%Jan 05 00:26:40 2006 DHCP6SNP PACKET: Receive DHCPv6 packet SOLICIT from
fe80::200:ff:fe00:1
         src MAC 00-00-00-00-00-01, dst MAC 33-33-00-01-00-02,
         interface Ethernet1/0/23 vlan 24,
         transaction-ID 6137412, smac host flag 0, dmac host flag 0
%Jan 05 00:26:40 2006 DHCP6SNP PACKET: Forward packet SOLICIT (protocol 0x37)
%Jan 05 00:26:40 2006 DHCP6SNP PACKET: to vlan 24 except port Ethernet1/0/23
(designPort flag 0)
%Jan 05 00:26:40 2006 DHCP6SNP PACKET: and return packet to network stack
switch#
```

13.2.2.4 show ipv6 dhcp relay option

Command: `show ipv6 dhcp relay option`

Function: Displays the relay agent configuration, including whether option 37 and option 38 are enabled.

Parameters: None.

Command Mode: Admin Mode.

Usage Guidelines: Use this command to check the option 37 and option 38 configuration of the relay agent.

Example:

```
Switch#show ipv6 dhcp relay option
remote-id option enable
subscriber-id option enable
Interface Vlan 1: remote-id option configure “abc”
```

13.2.2.5 show ipv6 dhcp snooping option

Command: `show ipv6 dhcp snooping option`

Function: Displays the snooping configuration, including whether option 37 and option 38 are enabled.

Parameters: None.

Command Mode: Admin Mode.

Usage Guidelines: Use this command to check the option 37 and option 38 configuration of DHCPv6 snooping.

Example:

```
Switch#show ipv6 dhcp snooping option
remote-id option enable
subscriber-id option enable
The slot port vlan select option is : port and vlan
The delimiter is : #
```

13.3 Prevent ND Spoofing

13.3.1 ipv6 nd-security updateprotect

Command: `ipv6 nd-security updateprotect`
`no ipv6 nd-security updateprotect`

Function: Disables automatic ND entry updates for IPv6. The **no** form of this command restores automatic updates.

Parameters: None.

Default: ND entries are updated normally.

Command Mode: Global Mode and Interface Mode.

Usage Guidelines: When automatic ND updates are disabled, ND packets that conflict with an existing ND entry (for example, the same IP address with a different MAC address or port) are dropped; other packets are accepted to refresh the aging timer or create new entries. Existing ND entries remain unchanged, and new entries can still be learned.

Example:

```
Switch(Config-if-Vlan1)#ipv6 nd -security updateprotect
Switch(config)#ipv6 nd -security updateprotect
```

13.3.2 ipv6 nd-security learnprotect

Command: `ipv6 nd-security learnprotect`
`no ipv6 nd-security learnprotect`

Function: Disables ND learning for IPv6. The **no** form of this command re-enables ND learning.

Parameters: None.

Default: ND learning is enabled.

Command Mode: Global Mode and Interface Mode.

Usage Guidelines: This command prevents automatic learning and updating of ND entries. Unlike **ipv6 nd-security updateprotect**, after this command is configured, entries still time out even if the switch keeps sending request and reply messages.

Example:

```
Switch(Config-if-Vlan1)#ipv6 nd -security learnprotect
Switch(config)#ipv6 nd -security learnprotect
```

13.3.3 ipv6 nd-security convert

Command: `ipv6 nd-security convert`

Function: Converts all dynamic ND entries to static entries.

Parameters: None.

Command Mode: Global Mode and Interface Mode.

Usage Guidelines: This command converts dynamic ND entries to static entries; combined with disabling automatic learning, it can prevent ND spoofing. The command takes effect once when it is run and is not retained.

Example:

```
Switch(Config-if-Vlan1)#ipv6 nd -security convert
Switch(config)#ipv6 nd -security convert
```

13.4 RIPng

13.4.1 clear ipv6 route

Command: `clear ipv6 rip route {<ipv6-address >| kernel |static | connected |rip |ospf |isis | bgp |all }`

Function: Clears specific routes from the RIPng routing table.

Parameters: <ipv6-address> is the destination address, in hexadecimal notation with prefix length; routes that exactly match it are cleared from the RIPng routing table.

kernel: Deletes kernel routes from the RIPng routing table.

static: Deletes static routes from the RIPng routing table.

connected: Deletes connected routes from the RIPng routing table.

rip: Deletes only RIPng routes from the RIPng routing table.

ospf: Deletes only IPv6 OSPF routes from the RIPng routing table.

bgp: Deletes only IPv6 BGP routes from the RIPng routing table.

isis: Deletes only IPv6 IS-IS routes from the RIPng routing table.

all: Deletes all routes from the RIPng routing table.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Use this command with **all** to delete all routes in the RIPng routing table.

Example: Clear route 2001:1:1::/64, and then the OSPF routes, from the RIPng routing table.

```
Switch#clear ipv6 rip route 2001:1:1::/64
Switch#clear ipv6 rip route ospf
```

13.4.2 default-information originate

Command: `default-information originate`
`no default-information originate`

Function: Allows the default route ::/0 to be redistributed into RIPng. The **no default-information originate** command disables this function.

Parameters: None.

Default: Disabled.

Command Mode: Router Mode.

Example: Advertise the default route in RIPng.

```
Switch#config terminal
Switch(config)#router ipv6 rip
Switch(config-router)#default-information originate
```

13.4.3 default-metric

Command: `default-metric <value>`
`no default-metric`

Function: Sets the default metric of redistributed routes. The **no default-metric** command restores the default.

Parameters: <value> is the route metric, ranging from 1 to 16.

Default: 1.

Command Mode: Router Mode.

Usage Guidelines: The **default-metric** command sets the default metric of routes from other routing protocols when they are redistributed into RIPng. When the **redistribute** command imports routes from other protocols without a specific metric, the metric set by **default-metric** is used.

Example: Set the default metric of routes redistributed into RIPng from other routing protocols to 3.

```
Switch(config-router)#default-metric 3
```

Related Commands: redistribute

13.4.4 distance

Command: distance <number> [<ipv6-address>] [<access-list-name | access-list-number>]
no distance [<ipv6-address>]

Function: Sets the administrative distance. The **no distance** command restores the default of 120.

Parameters: <number> is the distance, ranging from 1 to 255. **<ipv6-address>** is the link-local address or its prefix. **<access-list-name|access-list-number>** is the name or number of the access list to apply.

Default: The administrative distance of RIPng is 120.

Command Mode: Router Mode and Address Family Mode.

Usage Guidelines: When routes from two different routing protocols lead to the same destination, the administrative distance is used to select the route. The smaller the administrative distance of a protocol, the more reliable the routes learned from it.

Example:

```
Switch#config terminal
Switch(config)#router rip
Switch(config-router)#distance 8 fe80:1111::4200:21ff:fe00:11 mylist
```

13.4.5 distribute-list

Command: distribute-list {access-list-name> |prefix<prefix-list-name>} {in|out} [<ifname>|vlan <vlan-id>]
no distribute-list {access-list-name> |prefix<prefix-list-name>} {in|out} [<ifname>|vlan <vlan-id>]

Function: Uses an access list or prefix list to filter the route updates sent and received. The **no distribute-list** command removes the filter.

Parameters: <access-list-name> is the name or number of the access list to apply. **<prefix-list-name>** is the name of the prefix list to apply. **<ifname>** is the name of the interface to which route filtering applies.

Default: Disabled.

Command Mode: Router Mode.

Usage Guidelines: If no interface is specified, the filter applies to all interfaces.

Example: Filter incoming RIPng updates on VLAN 1 with prefix list myfilter.

```
Switch#config terminal
Switch(config)#router ipv6 rip
Switch(config-router)#distribute-list prefix myfilter in Vlan1
```

13.4.6 debug ipv6 rip

Command: debug ipv6 rip [events| nsm| packet [recv|send][detail]| all]
no debug ipv6 rip [events| nsm| packet [recv|send][detail]| all]

Function: Enables RIPng debugging and displays the debugging messages. The **no debug ipv6 rip** command disables the corresponding debugging.

Parameters: events: Displays RIPng event debugging messages.

nsm: Displays messages exchanged between RIPng and NSM.

packet: Displays RIPng packet debugging messages.

recv: Displays received packets.

send: Displays sent packets.

detail: Displays the details of packets received or sent.

Default: Disabled.

Command Mode: Admin Mode.

Example: Enable RIPng packet debugging.

```
Switch#debug ipv6 rip packet
Switch#1970/01/01 21:15:08 IMI: SEND[Ethernet1/0/4]: Send to [ff02::9]:521
1970/01/01 21:15:08 IMI: SEND[Ethernet1/0/2]: Send to [ff02::9]:521
1970/01/01 21:15:09 IMI: RECV[Ethernet1/0/4]: Receive from
[fe80::20b:46ff:fe57:8e60]:521
1970/01/01 21:15:09 IMI: RECV[Ethernet1/0/4]: 3000:1:1::/64 is filtered by
access-list dclist
1970/01/01 21:15:09 IMI: RECV[Ethernet1/0/4]: 3ffe:1:1::/64 is filtered by
access-list dclist
1970/01/01 21:15:15 IMI: RECV[Ethernet1/0/2]: Receive from
[fe80::203:fff:fe01:257c]:521
```

13.4.7 debug ipv6 rip redistribute message send

Command: debug ipv6 rip redistribute message send
no debug ipv6 rip redistribute message send

Function: Enables debugging of the redistribution messages sent to RIPng from OSPFv3 or other external processes. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example:

```
Switch# debug ipv6 rip redistribute message send
Switch# no debug ipv6 rip redistribute message send
```

13.4.8 debug ipv6 rip redistribute route receive

Command: debug ipv6 rip redistribute route receive
no debug ipv6 rip redistribute route receive

Function: Enables debugging of the redistributed routing information that RIPng receives from NSM. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example:

```
Switch#debug ipv6 rip redistribute route receive
Switch# no debug ipv6 rip redistribute route receive
```

13.4.9 ipv6 rip aggregate-address

Command: ipv6 rip aggregate-address X:X::X:X/M
no ipv6 rip aggregate-address X:X::X:X/M

Function: Configures an IPv6 aggregate route. The **no** form of this command deletes it.

Parameters: X:X::X:X/M: The IPv6 address and prefix length.

Command Mode: Router Mode or Interface Mode.

Default: No aggregate route is configured.

Usage Guidelines: To configure an aggregate route in Router Mode, RIPng must be enabled. In Interface Mode, RIPng need not be enabled; the aggregate route takes effect after RIPng is enabled on the interface.

Example: Configure aggregate route 2001:3f:ed8::99/64 globally.

```
Switch(config)#router rip
Switch(config-router) #ipv6 rip agg 2001:3f:ed8::99/64
```

13.4.10 ipv6 rip split-horizon

Command: ipv6 rip split-horizon [poisoned]
no ipv6 rip split-horizon

Function: Enables split horizon. The **no ipv6 rip split-horizon** command disables split horizon.

Parameters: poisoned: Enables split horizon with poison reverse.

Default: Split horizon with poison reverse.

Command Mode: Interface Mode.

Usage Guidelines: Split horizon prevents routing loops by preventing the Layer 3 switch from advertising a route on the interface from which it was learned. The command can be configured on an IPv6 tunnel interface; configure the tunnel carefully.

Example: Enable split horizon with poison reverse on VLAN 1.

```
Switch#config terminal
Switch(config)#interface Vlan1
Switch(config-if-Vlan1)#ipv6 rip split-horizon poisoned
```

13.4.11 ipv6 router rip

Command: ipv6 router rip
no ipv6 router rip

Function: Enables RIPng on the interface. The **no ipv6 router rip** command disables RIPng on the interface.

Default: Not configured.

Command Mode: Interface Mode.

Usage Guidelines: The command can be configured on an IPv6 tunnel interface; configure the tunnel carefully.

Example: Enable RIPng on VLAN 1.

```
Switch#config terminal
Switch(config)#interface Vlan1
```

```
Switch(Config-if-Vlan1)#ipv6 router rip
```

13.4.12 neighbor

Command: neighbor <ipv6-address> {<ifname> vlan <vlan-id>}
no neighbor <ipv6-address> {<ifname> vlan <vlan-id>}

Function: Specifies a destination address to which routing updates are always sent. The **no neighbor** command removes the specified address.

Parameters: <ipv6-address> is the IPv6 link-local address of the neighbor, in colon-hexadecimal notation without prefix length. **<ifname>** is the interface name.

Default: No fixed destination address is configured.

Command Mode: Router Mode.

Usage Guidelines: Used with the **passive-interface** command, this command sends routing updates only to the specified neighbor.

Example: Specify neighbor FE80:506::2 on VLAN 1.

```
Switch#config terminal
Switch(config)#router ipv6 rip
Switch(config-router)#neighbor FE80:506::2 Vlan1
```

Related Commands: passive-interface

13.4.13 offset-list

Command: offset-list <access-list-number|access-list-name> {in|out}
<number >[<ifname>|vlan <vlan-id>]
no offset-list <access-list-number|access-list-name> {in|
out }<number >[<ifname>|vlan <vlan-id>]

Function: Adds an offset to the metric of routes learned by RIPng. The **no offset-list** command disables this function.

Parameters: <access-list-number|access-list-name> is the number or name of the access list to apply. **<number>** is the offset to add, ranging from 0 to 16. **<ifname>** is the name of the interface.

Default: The offset is the interface metric defined by the system.

Command Mode: Router Mode.

Example: Add an offset of 5 to incoming routes matching access list 1 on VLAN 1.

```
Switch#config terminal
Switch(config)#router ipv6 rip
Switch(config-router)#offset-list 1 in 5 Vlan1
```

Related Commands: access-list

13.4.14 passive-interface

Command: passive-interface<ifname>|vlan <vlan-id>
no passive-interface<ifname>|vlan <vlan-id>

Function: Blocks RIPng broadcasts on the specified interface; RIPng packets are sent only to Layer 3 switches configured as neighbors.

Parameters: <ifname> is the interface name.

Default: Not configured.

Command Mode: Router Mode.

Example: Configure VLAN 1 as a passive interface.

```
Switch#config terminal
```

```
Switch(config)#router ipv6 rip
Switch(config-router)#passive-interface Vlan1
```

Related Commands: show ipv6 rip

13.4.15 redistribute

Command: redistribute {kernel |connected| static| ospf| isis| bgp} [metric<value>] [route-map<word>]
no redistribute {kernel |connected| static| ospf| isis| bgp} [metric<value>] [route-map<word>]

Function: Redistributes routes learned from other routing protocols into RIPng.

Parameters: kernel: Redistributes kernel routes.

connected: Redistributes connected routes.

static: Redistributes static routes.

ospf: Redistributes IPv6 OSPF routes.

isis: Redistributes IPv6 IS-IS routes.

bgp: Redistributes IPv6 BGP routes.

<value>: The metric assigned to redistributed routes, ranging from 0 to 16.

<word>: The route map applied to redistributed routes.

Command Mode: Router Mode.

Example: Redistribute kernel routes into RIPng using route map ip.

```
Switch#config terminal
Switch(config)#router ipv6 rip
Switch(config-router)#redistribute kernel route-map ip
```

13.4.16 redistribute ospf

Command: redistribute ospf [<process-tag>] [metric<value>] [route-map<word>]
no redistribute ospf [<process-tag>]

Function: Redistributes routes from an OSPFv3 process into the RIPng process. The **no** form of this command removes the redistributed OSPFv3 routes.

Parameters: <process-tag> is the tag of the OSPFv3 process, up to 15 characters. If it is not specified, the default process is used.

metric <value>: The metric of redistributed routes, ranging from 0 to 16.

route-map <word>: The route map applied to redistributed routes.

Default: Not redistributed.

Command Mode: Router Mode.

Usage Guidelines: None.

Example: Redistribute routes from OSPFv3 process abc into RIPng.

```
Switch(config)#router ipv6 rip
Switch (config-router)#redistribute ospf abc
```

13.4.17 route

Command: route <ipv6-address>
no route <ipv6-address>

Function: Configures a static RIPng route. The **no route** command deletes the route.

Parameters: <ipv6-address>: The destination IPv6 prefix and prefix length, in colon-hexadecimal notation.

Usage Guidelines: This command adds a static RIPng route and is mainly used for debugging. Routes configured with this command do not appear in the kernel routing table but in the RIPng route database, and can be viewed with **show ipv6 rip**.

Command Mode: Router Mode.

Example: Configure static RIPng route 3ffe:1234:5678::1/64.

```
Switch#config terminal
Switch(config)#router ipv6 rip
Switch(config-router)#route 3ffe:1234:5678::1/64
```

13.4.18 router ipv6 rip

Command: `router ipv6 rip`
`no router ipv6 rip`

Function: Enables the RIPng routing process and enters RIPng Router Mode. The **no router ipv6 rip** command disables RIPng.

Default: RIPng is not running.

Command Mode: Global Mode.

Usage Guidelines: Enable RIPng with this command before performing other global RIPng configuration.

Example: Enter RIPng Router Mode.

```
Switch(config)#router ipv6 rip
```

13.4.19 show debugging ipv6 rip

Command: `show debugging ipv6 rip`

Function: Displays the RIPng debugging status, including NSM debugging, RIPng event debugging, and RIPng packet debugging.

Command Mode: Admin Mode.

Example:

```
Switch#show debugging ipv6 rip
RIPng debugging status:
  RIPng event debugging is on
  RIPng packet detail debugging is on
RIPng NSM debugging is on
```

13.4.20 show ipv6 rip interface

Command: `show ipv6 rip interface`

Function: Displays RIPng interface information, including whether the interface and line protocol are up.

Command Mode: Admin Mode.

Example: Display RIPng interface information.

```
Switch(config)#show ipv6 rip interface
Loopback is up, line protocol is up
  RIPng is not enabled on this interface
Vlan1 is up, line protocol is up
  Routing Protocol: RIPng
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
```

```
    IPv6 interface address:
      3000:1:1::1/64
      fe80::203:fff:fe0c:cda/64
```

Output	Description
Vlan1 is up, line protocol is up	The interface is up.
Routing Protocol: RIP	The routing protocol running on the interface is RIPng.
Passive interface: Disabled	Passive interface is disabled.
Split horizon: Enabled with Poisoned Reversed	Split horizon with poison reverse is enabled on the interface.
IP interface address: 3000:1:1::1/64 fe80::203:fff:fe01:429e/64	IPv6 addresses of the interface

13.4.21 show ipv6 rip redistribute

Command: `show ipv6 rip redistribute`

Function: Displays the configuration of routes redistributed into RIPng from other protocols.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: None.

Example:

```
Switch#show ipv6 rip redistribute
```

13.4.22 show ipv6 protocols rip

Command: `show ipv6 protocols rip`

Function: Displays RIPng process parameters and statistics.

Command Mode: Admin Mode.

Example: Display RIPng process parameters.

```
Switch(config)#show ipv6 protocols rip
Routing Protocol is "RIPng"
  Sending updates every 30 seconds with +/-50%, next due in 1 second
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
    Ethernet1/0/4 filtered by dclist
  Default redistribute metric is 1
  Redistributing: static
  Interface
    Vlan10
    Vlan2
  Routing for Networks:
```

Output	Description
Sending updates every 30 seconds with +/-50%, next due in 1 seconds	Updates are sent every 30 seconds.
Timeout after 180 seconds, garbage collect after 120 seconds	The route timeout is 180 seconds, and the garbage collection time is 120 seconds.
Outgoing update filter list for all interface is not set	No outgoing update filter list is set for any interface.
Incoming update filter list for all interface is not set	No incoming update filter list is set for any interface.

Default redistribution metric is 1	The default redistribution metric is 1.
Redistributing: static	Static routes are redistributed into RIPng.
Interface Vlan10 Vlan2	RIPng runs on interfaces VLAN 10 and VLAN 2.

13.4.23 show ipv6 rip

Command: `show ipv6 rip`

Function: Displays RIPng routes.

Command Mode: Admin Mode.

Example: Display RIPng routes.

```
Switch#show ipv6 rip
Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS,
       B - BGP, a - aggregate, s - suppressed
   Network                     Next Hop                  If     Met Tag  Time
R  2000:1:1::/64               ::                          Vlan2   1   0
R  2001:1:1::/64               fe80::203:fff:fe01:257c       Vlan2   2   0
02:40
R  3000:1:1::/64               ::                           Vlan10   1   0
R  3010:1:1::/64               ::                           --      1   0
```

In the output, R indicates a RIP route. For example, the RIP route to destination network 2001:1:1::/64 has next hop fe80::203:fff:fe01:257c, was learned on VLAN 2 with a metric of 2, and times out in 2 minutes 40 seconds.

Equivalent Command: **show ipv6 rip database**

13.4.24 show ipv6 rip database

Command: `show ipv6 rip database`

Function: Displays RIPng database information.

Command Mode: Admin Mode.

Example: Display the RIPng database.

```
Switch#show ipv6 rip database
```

Equivalent Command: **show ipv6 rip**

13.4.25 show ipv6 rip aggregate

Command: `show ipv6 rip aggregate`

Function: Displays IPv6 aggregate route information.

Parameters: None.

Command Mode: Admin Mode and Configuration Mode.

Default: None.

Usage Guidelines: Displays the interface on which each aggregate route is configured, the metric, count, suppression count, and so on. If an aggregate route is configured globally, the interface is shown as "----". Metric is the route metric, Count is the number of routes aggregated, and Suppress is the number of times aggregation occurred.

Example: Display IPv6 aggregate route information.

```
Switch(config-router)#show ipv rip agg
 Aggregate information of ripng
```

```
      Network                 Aggregated Ifname     Metric Count Suppress
      2001::/16                Vlan1                  1      2     0
      2001:1::/32               ----                    1      2     0
      2001:1:2::/60             Vlan1                  1      1     1
                                ----                   1      1     1
```

Output	Description
Network	Route prefix and prefix length
Aggregated Ifname	Interface on which the aggregate route is configured. For a globally configured aggregate route, "---" is displayed.
Metric	Metric of the aggregate route
Count	Number of routes aggregated
Suppress	Number of times the route was aggregated

13.4.26 timers basic

Command: `timers basic <update> <invalid> <garbage>`
`no timers basic`

Function: Adjusts the RIPng update, timeout, and garbage collection timers. The **no timers basic** command restores the defaults.

Parameters: <update> is the interval for sending update packets, in seconds, ranging from 5 to 2147483647. **<invalid>** is the time after which a route is declared invalid, in seconds, ranging from 5 to 2147483647. **<garbage>** is the time an invalid route remains in the routing table before deletion, in seconds, ranging from 5 to 2147483647.

Default: <update> is 30 seconds, **<invalid>** is 180 seconds, and **<garbage>** is 120 seconds.

Command Mode: Router Mode.

Usage Guidelines: By default, the system sends RIPng updates every 30 seconds; a route is considered invalid after 180 seconds and remains for another 120 seconds before it is deleted from the routing table.

Example: Set the RIPng update time to 20 seconds, the timeout to 80 seconds, and the garbage collection time to 60 seconds.

```
Switch(Config-Router)#timers basic 20 80 60
```

13.5 OSPFv3

13.5.1 area authentication-mode

Command: `area (A.B.C.D|<0-4294967295>) authentication-mode (hmac-sha-256) key-id <0-65535>  (0 LINE|7 WORD)`
`no area (A.B.C.D|<0-4294967295>) authentication-mode`

Function: Configures an OSPFv3 area to use RFC 7166 authentication. The **no** form of this command restores the default.

Parameters: (A.B.C.D|<0-4294967295>) is the area ID, either a number from 0 to 4294967295 or an IP address.

hmac-sha-256: The authentication algorithm; only HMAC-SHA-256 is supported.

key-id <0-65535>: The key ID.

(0 LINE|7 WORD): The authentication key. With **0**, the key that follows is in plaintext; with **7**, it is the ciphertext string encrypted from the plaintext key. The key length ranges from 1 to 128.

Default: No authentication.

Command Mode: OSPFv3 Router Mode.

Usage Guidelines: This command configures an OSPFv3 area to use RFC 7166 authentication. Authentication can also be configured in Interface Mode; interface authentication takes precedence over area authentication. After authentication is configured on an interface, the area authentication does not affect that interface. Only one such configuration is allowed per area.

Example:

```
Switch(config-router)# area 0 authentication-mode hmac-sha-256 key-id 1 0
qwerty
```

13.5.2 area default cost

Command: `area <id> default-cost <cost>`
`no area <id> default-cost`

Function: Configures the cost of the default summary route sent into a stub or NSSA area. The **no** form of this command restores the default.

Parameters: <id> is the area ID, either a number from 0 to 4294967295 or an IP address. **<cost>** ranges from 0 to 16777214.

Default: 1.

Command Mode: OSPFv3 Router Mode.

Usage Guidelines: This command applies only to ABRs connected to a stub area.

Example: Set the default cost of area 1 to 10.

```
Switch(config-router)#area 1 default-cost 10
```

13.5.3 area range

Command: `area <id> range <ipv6address> [advertise| not-advertise|]`
`no area <id> range <ipv6address>`

Function: Summarizes OSPF routes at the area border. The **no area <id> range** command cancels this function.

Parameters: <id> is the area ID, either a number from 0 to 4294967295 or an IP address.

<ipv6address> = **<X:X::X:X/M>**: The IPv6 network prefix and prefix length of the area.

advertise: Advertises the summary route.

not-advertise: Does not advertise the summary route.

If neither is specified, the summary route is advertised.

Default: Not configured.

Command Mode: OSPFv3 Router Mode.

Usage Guidelines: Use this command to summarize routes within an area. If the network IDs in the area are not contiguous, configure this command on the ABR to advertise a summary route that covers all networks in the specified range.

Example:

```
Switch # config terminal
Switch (config)# router ipv6 ospf
Switch (config-router)# area 1 range 2000::/3
```

13.5.4 area stub

Command: `area <id> stub [no-summary]`
`no area <id> stub [no-summary]`

Function: Configures an area as a stub area. The **no area <id> stub** command cancels this function.

Parameters: <id> is the area ID, either a number from 0 to 4294967295 or an IPv4 address.

no-summary: The ABR stops sending summary LSAs into the stub area.

Default: Not configured.

Command Mode: OSPFv3 Router Mode.

Usage Guidelines: Configure **area stub** on all routers in the stub area. Two commands apply to routers in a stub area: **stub** and **default-cost**. All routers connected to the stub area must be configured with **area stub**; for ABRs connected to the stub area, the cost of the default route is set with **area default-cost**.

Example:

```
Switch # config terminal
Switch (config)# router ipv6 ospf
Switch (config-router)# area 1 stub
```

Related Commands: area default-cost

13.5.5 area virtual-link

Command: area <id> virtual-link A.B.C.D [instance-id <instance-id> | INTERVAL <value>]
no area <id> virtual-link A.B.C.D [instance-id <instance-id> | INTERVAL]

Function: Configures a virtual link between two backbone area segments separated by a non-backbone area. The **no** form of this command removes the virtual link.

Parameters: <id> is the area ID, either a number from 0 to 4294967295 or an IP address.

<instance-id> is the interface instance ID, ranging from 0 to 255. The default is 0.

INTERVAL = [**dead-interval** | **hello-interval** | **retransmit-interval** | **transmit-delay**]

<value>: The delay or interval in seconds, ranging from 1 to 65535.

dead-interval: The time after which a neighbor is considered down if no packets are received from it. The default is 40 seconds.

hello-interval: The interval at which the router sends Hello packets. The default is 10 seconds.

retransmit-interval: The interval before the router retransmits a packet. The default is 5 seconds.

transmit-delay: The delay before the router sends a packet. The default is 1 second.

Default: None.

Command Mode: OSPFv3 Router Mode.

Usage Guidelines: In OSPF, all non-backbone areas must connect to the backbone area. If the connection to the backbone area is lost, a virtual link can restore it. A virtual link can be configured between any two backbone routers that share a common non-backbone area. The protocol treats routers connected by a virtual link as a point-to-point network.

Example:

```
Switch#config terminal
Switch(config) #router ipv6 ospf
Switch(config-router) #area 1 virtual-link 10.10.11.50 hello 5 dead 20
Switch(config-router) #area 1 virtual-link 10.10.11.50 instance-id 1
```

13.5.6 abr-type

Command: abr-type {cisco|ibm| standard}
no abr-type [cisco|ibm| standard]

Function: Configures the OSPF ABR type. The **no abr-type** command restores the default.

Parameters: cisco: Cisco ABR implementation. **ibm**: IBM ABR implementation. **shortcut**: Shortcut ABR. **standard**: Standard (RFC 2328) ABR implementation.

Default: cisco.

Command Mode: OSPFv3 Router Mode.

Usage Guidelines: This command specifies the ABR implementation type. It improves interoperability among different OSPF implementations and is especially useful in multihomed environments.

Example: Set the ABR type to standard.

```
Switch#config terminal
Switch(config)#router ipv6 ospf
Switch(config-router)#abr-type standard
```

13.5.7 default-metric

Command: `default-metric <value>`
`no default-metric`

Function: Sets the default metric of the OSPF routing protocol. The **no default-metric** command restores the default.

Parameters: <value>: The metric, ranging from 1 to 16777214.

Default: Built-in; metrics are translated automatically.

Command Mode: OSPFv3 Router Mode.

Usage Guidelines: When metrics are incompatible, route redistribution still proceeds. If a metric cannot be translated, the default metric is used so that redistribution can continue. With this command, all redistributed routes use the same metric. Use this command together with **redistribute**.

Example:

```
Switch#config terminal
Switch(config)#router ipv6 ospf
Switch(config-router)#default-metric 100
```

13.5.8 debug ipv6 ospf events

Command: `[no] debug ipv6 ospf events [abr|asbr|os|router|vlink]`

Function: Enables debugging of OSPF events. The **no debug ipv6 ospf events** command disables it.

Default: Disabled.

Command Mode: Admin Mode.

Example:

```
Switch#debug ipv6 ospf events
1970/01/01 01:10:35 IMI: ROUTER[Process:(null)]: GC timer expire
```

13.5.9 debug ipv6 ospf ifsm

Command: `[no] debug ipv6 ospf ifsm [status|events|timers]`

Function: Enables debugging of OSPF interface states. The **no debug ipv6 ospf ifsm** command disables it.

Default: Disabled.

Command Mode: Admin Mode.

Example:

```
Switch#debug ipv6 ospf ifsm
1970/01/01 01:11:44 IMI: IFSM[Vlan1]: Hello timer expire
1970/01/01 01:11:44 IMI: IFSM[Vlan2]: Hello timer expire
```

13.5.10 debug ipv6 ospf lsa

Command: [no]debug ipv6 ospf lsa [generate|flooding|install|maxage| refresh]

Function: Enables debugging of link state advertisements. The **no debug ipv6 ospf lsa** command disables it.

Default: Disabled.

Command Mode: Admin Mode.

13.5.11 debug ipv6 ospf nfsm

Command: [no] debug ipv6 ospf nfsm [status|events|timers]

Function: Enables debugging of the OSPF neighbor state machine. The **no debug ipv6 ospf nfsm** command disables it.

Default: Disabled.

Command Mode: Admin Mode.

Example:

```
Switch#debug ipv6 ospf nfsm
1970/01/01 01:14:07 IMI: NFSM[192.168.2.3-000007d4]: LS update timer expire
1970/01/01 01:14:07 IMI: NFSM[192.168.2.1-000007d3]: LS update timer expire
1970/01/01 01:14:08 IMI: NFSM[192.168.2.1-000007d3]: Full (HelloReceived)
1970/01/01 01:14:08 IMI: NFSM[192.168.2.1-000007d3]: nfsm_ignore called
1970/01/01 01:14:08 IMI: NFSM[192.168.2.1-000007d3]: Full (2-WayReceived)
```

13.5.12 debug ipv6 ospf nsm

Command: [no] debug ipv6 ospf nsm [interface|redistribute]

Function: Enables debugging of OSPF NSM. The **no debug ipv6 ospf nsm** command disables it.

Default: Disabled.

Command Mode: Admin Mode.

13.5.13 debug ipv6 ospf packet

Command: [no] debug ipv6 ospf packet [dd | detail | hello | ls-ack | ls-request | ls-update | recv | send]

Function: Enables debugging of OSPF packets. The **no debug ipv6 ospf packet** command disables it.

Default: Disabled.

Command Mode: Admin Mode.

13.5.14 debug ipv6 ospf redistribute message send

Command: debug ipv6 ospf redistribute message send
no debug ipv6 ospf redistribute message send

Function: Enables or disables debugging of messages sent by an IPv6 OSPF process for redistribution into other IPv6 OSPF processes.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example:

```
Switch#debug ipv6 ospf redistribute message send
```

13.5.15 debug ipv6 ospf redistribute route receive

Command: debug ipv6 ospf redistribute route receive
no debug ipv6 ospf redistribute route receive

Function: Enables or disables debugging of routing messages that the IPv6 OSPF process receives from NSM.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example:

```
Switch# debug ipv6 ospf redistribute route receive
```

13.5.16 debug ipv6 ospf route

Command: [no] debug ipv6 ospf route [ase|ia|install|spf]

Function: Enables debugging of OSPF routes. The **no debug ipv6 ospf route** command disables it.

Default: Disabled.

Command Mode: Admin Mode.

13.5.17 ipv6 ospf authentication-mode

Command: ipv6 ospf authentication-mode (null|(hmac-sha-256) key-id <0-65535> (0 WORD |7 WORD) (instance-id <0-255> |))
no ipv6 ospf authentication-mode

Function: Configures RFC 7166 authentication for OSPFv3 packets on the specified interface. The **no** form of this command restores the default.

Parameters: null: The interface does not use authentication.

hmac-sha-256: The authentication algorithm; only HMAC-SHA-256 is supported.

key-id <0-65535>: The key ID.

(0 WORD |7 WORD): The authentication key. With **0**, the key that follows is in plaintext; with **7**, it is the ciphertext string encrypted from the plaintext key. The key length ranges from 1 to 128.

instance-id: The instance ID, ranging from 0 to 255. The default is 0.

Default: The area authentication is used.

Command Mode: Interface Mode.

Usage Guidelines: This command configures RFC 7166 authentication for OSPFv3 packets on the specified interface. By default, the interface uses the authentication of its area. If the area has authentication configured but the interface does not require authentication, configure **null**. If the area has no authentication, an interface configured with **null** also uses no authentication.

Example:

```
Switch#config terminal
Switch(config)#interface vlan 10
Switch(Config-if-Vlan10)#ipv6 ospf authentication-mode hmac-sha-256 key-id
100 0 asdfg
```

13.5.18 ipv6 ospf cost

Command: ipv6 ospf cost <cost> [instance-id <id>]
no ipv6 ospf <cost> [instance-id <id>]

Function: Specifies the OSPF cost of the interface. The **no ipv6 ospf cost** command restores the default.

Parameters: <id> is the interface instance ID, ranging from 0 to 255. The default is 0.

<cost> is the OSPF cost, ranging from 1 to 65535.

Default: 10.

Command Mode: Interface Mode.

Usage Guidelines: The command can be configured on an IPv6 tunnel interface; configure the tunnel carefully.

Example:

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 ospf cost 3
```

13.5.19 ipv6 ospf dead-interval

Command: ipv6 ospf dead-interval <time > [instance-id <id>]
no ipv6 ospf dead-interval [instance-id <id>]

Function: Specifies the dead interval for neighboring Layer 3 switches. The **no ipv6 ospf dead-interval** command restores the default.

Parameters: <id> is the interface instance ID, ranging from 0 to 255. The default is 0.

<time> is the dead interval in seconds, ranging from 1 to 65535.

Default: 40 seconds (normally four times the hello interval).

Command Mode: Interface Mode.

Usage Guidelines: If no Hello packet is received within the **dead-interval**, the neighboring Layer 3 switch is considered unreachable. Use this command to adjust the dead interval according to the actual link conditions. The configured **dead-interval** is carried in Hello packets. For OSPF to operate normally, the dead interval must be the same on adjacent Layer 3 switches and should be at least four times the **hello-interval**. The command can be configured on an IPv6 tunnel interface; configure the tunnel carefully.

Example:

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 ospf dead-interval 80
```

13.5.20 ipv6 ospf display route single-line

Command: [no] ipv6 ospf display route single-line

Function: Changes the output format of the **show ipv6 ospf route** command. The **no ipv6 ospf display route single-line** command restores the default format.

Default: Not configured.

Command Mode: Global Mode.

Usage Guidelines: By default, **show ipv6 ospf route** displays a route over several lines. With this command, each route is displayed on a single line.

Example:

```
Switch#config terminal
Switch(config)#ipv6 ospf display route single-line
```

13.5.21 ipv6 ospf hello-interval

Command: ipv6 ospf hello-interval <time> [instance-id <id>]
no ipv6 ospf hello-interval [instance-id <id>]

Function: Specifies the hello interval of the interface. The **no ipv6 ospf hello-interval** command restores the default.

Parameters: <id> is the interface instance ID, ranging from 0 to 255. The default is 0.

<time> is the hello interval in seconds, ranging from 1 to 65535.

Default: 10 seconds.

Command Mode: Interface Mode.

Usage Guidelines: Hello packets are the most common packets; they are sent periodically to adjacent Layer 3 switches to discover and maintain adjacencies and to elect the DR and BDR. The configured **hello-interval** is carried in Hello packets. A smaller hello interval detects topology changes sooner but increases overhead. For OSPF to operate normally, the **hello-interval** must be the same on adjacent Layer 3 switches. The command can be configured on an IPv6 tunnel interface; configure the tunnel carefully.

Example:

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 ospf hello-interval 20
```

Related Commands: ipv6 ospf dead-interval

13.5.22 ipv6 ospf priority

Command: ipv6 ospf priority <priority> [instance-id <id>]
no ipv6 ospf priority[instance-id <id>]

Function: Configures the priority of the interface in the designated router (DR) election. The **no ipv6 ospf priority** command restores the default.

Parameters: <id> is the interface instance ID, ranging from 0 to 255. The default is 0.

<priority> is the priority, ranging from 0 to 255.

Default: 1.

Command Mode: Interface Mode.

Usage Guidelines: When two Layer 3 switches on the same segment both want to become the DR, the priority determines which one is elected. Normally the switch with the higher priority is elected; if the priorities are equal, the switch with the larger router ID is elected. A switch with priority 0 is never elected DR or BDR. The command can be configured on an IPv6 tunnel interface; configure the tunnel carefully.

Example: Configure the DR election priority. Set the priority of interface VLAN 1 to 0 so that it is not eligible for election.

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 ospf priority 0
```

13.5.23 ipv6 ospf retransmit-interval

Command: ipv6 ospf retransmit-interval <time> [instance-id <id>]
no ipv6 ospf retransmit-interval [instance-id <id>]

Function: Specifies the LSA retransmission interval between the interface and adjacent Layer 3 switches. The **no ipv6 ospf retransmit-interval** command restores the default.

Parameters: <id> is the interface instance ID, ranging from 0 to 255. The default is 0.

<time> is the LSA retransmission interval in seconds, ranging from 1 to 65535.

Default: 5 seconds.

Command Mode: Interface Mode.

Usage Guidelines: When a Layer 3 switch sends an LSA to a neighbor, it keeps the LSA until it receives an acknowledgment. If no acknowledgment is received within the interval, the LSA is retransmitted. The retransmission interval must be greater than the round-trip time between the two switches. The command can be configured on an IPv6 tunnel interface; configure the tunnel carefully.

Example: Set the LSA retransmission interval of interface VLAN 1 to 10 seconds.

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 ospf retransmit-interval 10
```

13.5.24 ipv6 ospf transmit-delay

Command: ipv6 ospf transmit-delay <time> [instance-id <id>]
no ipv6 ospf transmit-delay [instance-id <id>]

Function: Configures the LSA transmission delay of the interface. The **no ipv6 ospf transmit-delay** command restores the default.

Parameters: <id> is the interface instance ID, ranging from 0 to 255. The default is 0.

<time> is the LSA transmission delay in seconds, ranging from 1 to 65535.

Default: 1 second.

Command Mode: Interface Mode.

Usage Guidelines: LSAs age inside Layer 3 switches but not during transmission, so the transmission delay is added to the LSA age before the LSA is sent. The command can be configured on an IPv6 tunnel interface; configure the tunnel carefully.

Example: Set the LSA transmission delay of interface VLAN 1 to 3 seconds.

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 ospf transmit-delay 3
```

13.5.25 ipv6 router ospf

Command: [no] ipv6 router ospf {area <area-id> [instance-id <instance-id>]| tag <tag>[instance-id <instance-id>]}| tag <tag> area <area-id> [instance-id <instance-id>]}

Function: Enables OSPFv3 on the interface. The **no ipv6 router ospf** command cancels the configuration.

Parameters: <area-id> is the area ID, either a number from 0 to 4294967295 or an IPv4 address.

<instance-id> is the interface instance ID, ranging from 0 to 255. The default is 0.

<tag> is the OSPFv3 process tag.

Default: Not configured.

Command Mode: Interface Mode.

Usage Guidelines: To enable OSPFv3 on the interface, the area ID must be configured; the instance ID and process tag are optional. An OSPFv3 process allows one routing instance per instance ID. Several OSPF processes can run on one interface if their instance IDs differ; different OSPF processes must not use the same instance ID. The command can be configured on an IPv6 tunnel interface; configure the tunnel carefully.

Example:

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 router ospf area 1 tag IPI instance-id 1
```

13.5.26 max-concurrent-dd

Command: `max-concurrent-dd <value>`
`no max-concurrent-dd`

Function: Configures the maximum number of DD packets processed concurrently in OSPF. The **no max-concurrent-dd** command restores the default.

Parameters: <value> is the maximum number of DD packets processed concurrently, ranging from 1 to 65535.

Default: No limit.

Command Mode: OSPFv3 Router Mode.

Usage Guidelines: Specifies the maximum number of DD packets processed concurrently in OSPF.

Example: Set the maximum number of concurrent DD packets to 20.

```
Switch#config terminal
Switch(config)#router ipv6 ospf
Switch(config-router)#max-concurrent-dd 20
```

13.5.27 passive-interface

Command: `[no] passive-interface {<ifname>|vlan <vlan-id>}`

Function: Stops sending Hello packets on the specified interface. The **no passive-interface** command cancels this function.

Parameters: <ifname> is the interface name.

Default: Not configured.

Command Mode: OSPFv3 Router Mode.

Example: Configure VLAN 1 as a passive interface.

```
Switch#config terminal
Switch(config)#router ipv6 ospf
Switch(config-router)#passive-interface vlan1
```

13.5.28 redistribute

Command: `[no] redistribute {kernel |connected| static| rip| isis| bgp}`
`[metric<value>] [metric-type {1|2}][route-map<word>]`

Function: Redistributes routes learned from other routing protocols into OSPFv3.

Parameters: kernel: Redistributes kernel routes.

connected: Redistributes connected routes.

static: Redistributes static routes.

rip: Redistributes RIP routes.

isis: Redistributes IS-IS routes.

bgp: Redistributes BGP routes.

metric <value>: The metric of redistributed routes, ranging from 0 to 16777214.

metric-type {1|2}: The external metric type of redistributed routes, 1 or 2. The default is 2.

route-map <word>: The route map applied to redistributed routes.

Command Mode: OSPFv3 Router Mode.

Usage Guidelines: Redistributes routes from other routing protocols into the OSPFv3 area as AS-external LSAs.

Example: Redistribute BGP routes with metric 12 and metric type 1.

```
Switch#config terminal
Switch(config)#router ipv6 ospf
Switch(config-router)#redistribute bgp metric 12 metric-type 1
```

13.5.29 redistribute ospf

Command: `redistribute ospf [<process-tag>] [metric<value>] [metric-type {1|2}] [route-map<word>]`
`no redistribute ospf [<process-tag>] [metric<value>] [metric-type {1|2}][route-map<word>]`

Function: Redistributes routes from another OSPFv3 process (process-tag) into this process. The **no** form of this command cancels the redistribution; if the optional metric, metric-type, or route-map parameters are specified, only those settings are restored to the defaults.

Parameters: <process-tag>: The tag of the IPv6 OSPF process. The default is NULL.

metric <value>: The metric of redistributed routes, ranging from 0 to 16777214.

metric-type {1|2}: The metric type of redistributed routes, 1 or 2. The default is 2.

route-map <word>: The route map applied to redistributed routes.

Default: No OSPFv3 routes are redistributed.

Command Mode: OSPFv3 Router Mode.

Usage Guidelines: If no process tag is specified, routes of the default OSPFv3 process (process tag NULL) are redistributed. If the **no** form includes the optional metric, metric-type, or route-map parameters, those settings are restored to the defaults; without optional parameters, redistribution from that process is removed.

Example:

```
Switch(config)#router ipv6 ospf
Switch(config-router)#redistribute ospf
```

13.5.30 router-id

Command: `router-id <router-id>`
`no router-id`

Function: Configures the router ID of the OSPFv3 process. The **no router-id** command restores the ID to 0.0.0.0.

Parameters: <router-id> is the router ID, in IPv4 address format.

Default: 0.0.0.0.

Usage Guidelines: If the router ID is 0.0.0.0, the OSPFv3 process cannot start normally. A router ID must be configured for OSPFv3.

Command Mode: OSPFv3 Router Mode.

Example: Set the router ID to 192.168.2.1.

```
Switch#config terminal
Switch(config)#router ipv6 ospf
Switch(config-router)#router-id 192.168.2.1
```

13.5.31 router ipv6 ospf

Command: [no] router ipv6 ospf [<tag>]

Function: Initializes the OSPFv3 routing process and enters OSPFv3 Router Mode. The **no router ipv6 ospf** command stops the process.

Parameters: <tag> is the OSPFv3 process tag, a string of letters and digits.

Command Mode: Global Mode.

Usage Guidelines: For the OSPFv3 routing process to work, this command must be configured and OSPFv3 must be enabled on at least one interface. When the tag configured with **ipv6 router ospf area** in Interface Mode matches the tag of the OSPF process, the OSPFv3 process is enabled on that interface.

Example: Start OSPFv3 process IPI.

```
Switch#config terminal
Switch(config)#router ipv6 ospf IPI
```

13.5.32 show ipv6 ospf

Command: show ipv6 ospf [<tag>]

Function: Displays OSPF global and area information.

Parameters: <tag> is the process tag, a character string.

Default: None.

Command Mode: All Modes.

Example:

```
Switch#show ipv6 ospf
Routing Process "OSPFv3 (*null*)" with ID 192.168.2.2
 SPF schedule delay 5 secs, Hold time between SPFs 10 secs
 Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x0000
 Number of AS-Scoped Unknownnnnn LSA 0
 Number of LSA originated 6
 Number of LSA received 14
 Number of areas in this router is 1
    Area BACKBONE(0)
        Number of interfaces in this area is 2
        SPF algorithm executed 6 times
        Number of LSA 8.  Checksum Sum 0x43D52
        Number of Unknownnnnn LSA 0
```

13.5.33 show ipv6 ospf database

Command: show ipv6 ospf [<tag>] database
[router [adv-router <advertiser_router>]
|network [adv-router <advertiser_router>]
| intra-prefix [adv-router <advertiser_router>]
| link [adv-router <advertiser_router>]
| external [adv-router <advertiser_router>]
| inter-prefix [adv-router <advertiser_router>]
| inter-router [adv-router <advertiser_router>]]

Function: Displays the OSPF link state database.

Parameters: <tag> is the process tag, a character string.

<advertiser_router> is the ID of the advertising router, in IPv4 address format.

Default: None.

Command Mode: All Modes.

Usage Guidelines: Use this command to view the OSPF link state database.

Example:

The **show ipv6 ospf database** command displays the LSAs of the OSPF routing protocol.

Sample output:

```
            OSPFv3 Router with ID (192.168.2.2) (Process *null*)
                Link-LSA (Interface Vlan1)
Link State ID   ADV Router      Age  Seq#       CkSum  Prefix
0.0.7.211       192.168.2.2     1409 0x80000001 0x6dda      1
0.0.7.212       192.168.2.3     1357 0x80000001 0x248e      1
                Link-LSA (Interface Vlan2)
Link State ID   ADV Router      Age  Seq#       CkSum  Prefix
0.0.7.211       192.168.2.1     1450 0x80000001 0xa565      1
0.0.7.212       192.168.2.2     1399 0x80000001 0x4305      1
                Router-LSA (Area 0.0.0.0)
Link State ID   ADV Router      Age  Seq#       CkSum    Link
0.0.0.0         192.168.2.1     1390 0x80000006 0x9fe2      1
0.0.0.0         192.168.2.2     1354 0x80000007 0x4af5      2
0.0.0.0         192.168.2.3     1308 0x80000004 0xbbc4      1
                Network-LSA (Area 0.0.0.0)
       Link State ID   ADV Router      Age  Seq#       CkSum
0.0.7.211       192.168.2.1     1390 0x80000001 0x897e
0.0.7.211       192.168.2.2     1354 0x80000001 0x9b69
                Intra-Area-Prefix-LSA (Area 0.0.0.0)
Link State ID   ADV Router      Age  Seq#       CkSum  Prefix  Reference
0.0.0.1         192.168.2.1     1389 0x80000005 0x7e2e      1  Router-LSA
0.0.0.2         192.168.2.1     1389 0x80000001 0x22cb      1  Network-LSA
0.0.0.1         192.168.2.3     1306 0x80000002 0xd0d7      1  Router-LSA
```

Output	Description
Link-LSA (Interface Vlan1)	Link LSAs of interface VLAN 1
Router-LSA (Area 0.0.0.0)	Router LSAs in area 0
Network-LSA (Area 0.0.0.0)	Network LSAs in area 0
Intra-Area-Prefix-LSA (Area 0.0.0.0)	Intra-area prefix LSAs in area 0

13.5.34 show ipv6 ospf interface

Command: show ipv6 ospf interface <ifname>|vlan <vlan-id>

Function: Displays OSPF interface information.

Parameters: <ifname> is the interface name.

Default: None.

Command Mode: All Modes.

Example:

```
Switch#show ipv6 ospf interface
Loopback is up, line protocol is up
  OSPFv3 not enabled on this interface
Vlan1 is up, line protocol is up
  Interface ID 2003
  IPv6 Prefixes
    fe80::203:fff:fe01:257c/64 (Link-Local Address)
    2001:1:1::1/64
  OSPFv3 Process (*null*), Area 0.0.0.0, Instance ID 0
    Router ID 192.168.2.2, Network Type BROADCAST, Cost: 10
    Transmit Delay is 1 sec, State DR, Priority 1
    Designated Router (ID) 192.168.2.2
```

```
      Interface Address fe80::203:fff:fe01:257c
    Backup Designated Router (ID) 192.168.2.3
      Interface Address fe80::203:fff:fe01:d28
    Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:10
    Neighbor Count is 1, Adjacent neighbor count is 1
Vlan2 is up, line protocol is up
  Interface ID 2004
  IPv6 Prefixes
    fe80::203:fff:fe01:257c/64 (Link-Local Address)
    2000:1:1::1/64
  OSPFv3 Process (*null*), Area 0.0.0.0, Instance ID 0
    Router ID 192.168.2.2, Network Type BROADCAST, Cost: 10
    Transmit Delay is 1 sec, State Backup, Priority 1
    Designated Router (ID) 192.168.2.1
      Interface Address fe80::203:fff:fe01:429e
    Backup Designated Router (ID) 192.168.2.2
      Interface Address fe80::203:fff:fe01:257c
    Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:10
    Neighbor Count is 1, Adjacent neighbor count is 1
```

Output	Description
Vlan1 is up, line protocol is up	The interface is up both logically and physically.
IPv6 Prefixes fe80::203:fff:fe01:257c/64 (Link-Local Address) 2001:1:1::1/64	IPv6 addresses and prefix lengths of the interface
OSPFv3 Process (*null*)	OSPFv3 process to which the interface belongs
Area 0.0.0.1	Area to which the interface belongs
Instance ID 0	The instance ID is 0.
Router ID 192.168.2.2, Network Type BROADCAST, Cost: 10	Router ID, network type, and cost
Transmit Delay is 1 sec, State DR, Priority 1	LSA transmission delay, interface state, and DR election priority of the interface
Designated Router (ID) 192.168.2.2 Interface Address fe80::203:fff:fe01:257c	Designated router
Backup Designated Router (ID) 192.168.2.3 Interface Address fe80::203:fff:fe01:d28	Backup designated router
Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due in 00:00:10	OSPF timers: Hello, wait, dead, and retransmission intervals
Neighbor Count is 1, Adjacent neighbor count is 1	Number of neighbors, and number of neighbors with which adjacencies are established

13.5.35 show ipv6 ospf neighbor

Command: show ipv6 ospf [<tag>] neighbor [<neighbor_id> | <ifname> detail | detail]

Function: Displays OSPF neighbor information.

Parameters: <tag> is the process tag, a character string.

<neighbor_id> is the neighbor ID, in IPv4 address format.

detail: Displays neighbor details.

<ifname> is the interface name.

Default: None.

Command Mode: All Modes.

Usage Guidelines: Use this command to check the OSPF neighbor state.

Example:

```
Switch#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
192.168.2.3       1   Full/Backup     00:00:29    Vlan1      0
192.168.2.1       1   Full/DR         00:00:38    Vlan2      0          Vlan1
```

Output	Description
Neighbor ID	Neighbor ID
Instance ID	Instance ID
Address	IP address of the neighboring Layer 3 switch
Interface	Interface on which the neighbor is located
State	Neighbor state
Pri	Priority

13.5.36 show ipv6 ospf route

Command: `show ipv6 ospf [<tag>] route`

Function: Displays the OSPF routing table.

Parameters: <tag> is the process tag, a character string.

Default: None.

Command Mode: All Modes.

Example:

```
Switch#show ipv6 ospf route
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2
   Destination                                  Metric
     Next-hop
O  2000:1:1::/64                                   10
     directly connected, Vlan2
O  2001:1:1::/64                                   10
     directly connected, Vlan1
O  3000:1:1::/64                                   20
     via fe80::203:fff:fe01:429e, Vlan2
O  3003:1:1::/64                                   20
     via fe80::203:fff:fe01:d28, Vlan1
```

13.5.37 show ipv6 ospf redistribute

Command: `show ip ospf v6 [<process-tag>] redistribute`

Function: Displays the routes redistributed into OSPF from external processes.

Parameters: <process-tag> is the IPv6 OSPF process tag. If it is not specified, routes redistributed from external processes into all IPv6 OSPF processes are displayed.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: None.

Example:

```
Switch#show ipv6 ospf redistribute
ospf process abc redistribute information :
ospf process def
```

```
bgp
ospf process def redistribute information:
ospf process abc
Switch#show ipv6 ospf abc redistribute
ospf process abc redistribute information:
ospf process def
bgp
```

13.5.38 show ipv6 ospf topology

Command: show ipv6 ospf [<tag>] topology [area <area-id>]

Function: Displays OSPF topology information.

Parameters: <tag> is the process tag, a character string.

<area-id> is the area ID, either a number from 0 to 4294967295 or an IPv4 address.

Default: None.

Command Mode: All Modes.

Example:

```
Switch#show ipv6 ospf topology
OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits  Metric     Next-Hop            Interface
192.168.2.1            10         192.168.2.1         Vlan2
192.168.2.2            --
192.168.2.3            10         192.168.2.3         Vlan1
```

13.5.39 show ipv6 ospf virtual-links

Command: show ipv6 ospf [<tag>] virtual-links

Function: Displays OSPF virtual link information.

Parameters: <tag> is the process tag, a character string.

Default: None.

Command Mode: All Modes.

Example:

```
Switch#show ipv6 ospf virtual-links
Virtual Link VLINK1 to router 5.6.7.8 is up
Transit area 0.0.0.1 via interface Vlan1, instance ID 0
Local address 3ffe:1234:1::1/128
Remote address 3ffe:5678:3::1/128
Transmit Delay is 1 sec, State Point-To-Point,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:01
Adjacency state Up
```

13.5.40 show ipv6 route process-detail

Command: show ipv6 route [database] process-detail

Function: Displays the IPv6 routing table with the process ID or tag of each route.

Parameters: database displays all routes; without it, only active routes are displayed.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: None.

Example:

```
Switch#show ipv6 route database process-detail
```

```
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - IS-IS, B - BGP
       > - selected route, * - FIB route, p - stale info
Timers: Uptime
C*> ::1/128 via ::, Loopback, 00:29:53
O   2001::/64 [110/10] via ::, Vlan1, 00:01:07 ,process aaa
C*> 2001::/64 via ::, Vlan1, 00:02:54
O*> 2006::/64 [110/10] via ::, Vlan1, 00:01:07, process aaa
O*> 2008::/64 [110/20] via fe80::203:fff:fe01:2542, Vlan1, 00:00:54, process
bbb
```

13.5.41 timers spf

Command: `timers spf <spf-delay> <spf-holdtime>`
`no timers spf`

Function: Adjusts the route calculation (SPF) timers. The **no timers spf** command restores the defaults.

Parameters: <spf-delay>: The SPF delay. The default is 5 seconds.

<spf-holdtime>: The SPF hold time. The default is 10 seconds.

Command Mode: OSPFv3 Router Mode.

Usage Guidelines: This command configures the delay between receiving a topology change and starting the SPF calculation, and the hold time between two consecutive SPF calculations.

Example: Set the SPF delay to 5 seconds and the hold time to 10 seconds.

```
Switch#config terminal
Switch(config)#router ipv6 ospf
Switch(config-router)#timers spf 5 10
```

13.6 MBGP4+

13.6.1 debug ipv6 bgp redistribute message send

Command: `debug ipv6 bgp redistribute message send`
`no debug ipv6 bgp redistribute message send`

Function: Enables debugging of the messages sent to MBGP4+ for redistribution of routes from external processes such as OSPFv3. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example:

```
Switch# debug ipv6 bgp redistribute message send
```

13.6.2 debug ipv6 bgp redistribute route receive

Command: `debug ipv6 bgp redistribute route receive`
`no debug ipv6 bgp redistribute route receive`

Function: Enables debugging of the messages that MBGP4+ receives from NSM. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: None.

Example:

```
Switch# debug ipv6 bgp redistribute route receive
Switch# no debug ipv6 bgp redistribute route receive
```

13.6.3 redistribute ospf (MBGP4+)

Command: `redistribute ospf [<process-tag>] [route-map<word>]`
`no redistribute ospf [<process-tag>]`

Function: Redistributes routes from OSPFv3 into MBGP4+. The **no** form of this command removes the configuration.

Parameters: <process-tag> is the OSPFv3 process tag, less than 15 characters. If it is not specified, the default process is used.

route-map <word>: The route map applied to redistributed routes.

Default: Not redistributed.

Command Mode: BGP IPv6 Address Family Mode.

Usage Guidelines: None.

Example: Redistribute routes from OSPFv3 process abc into MBGP4+ (AS 1).

```
Switch (config)#router bgp 1
Switch (config-router)#address-family ipv6 unicast
Switch (config-router-af)#redistribute ospf abc
```

13.6.4 show ipv6 bgp redistribute

Command: `show ipv6 bgp redistribute`

Function: Displays the configuration of routes redistributed into MBGP4+ from other protocols.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: None.

Example:

```
Switch#show ipv6 bgp redistribute
```

13.7 Black Hole Routing

13.7.1 ipv6 route null0

Command: `ipv6 route <ipv6-prefix|prefix-length> null0 [<precedence>]`
`no ipv6 route <ipv6-prefix|prefix-length> null0`

Function: Configures a route that sends traffic destined to the specified network to the null0 interface.

Parameters: <ipv6-prefix> is the destination IPv6 network of the static route. **<prefix-length>** is the prefix length. **null0** is the outgoing interface of the black hole route. **<precedence>** is the route weight, ranging from 1 to 255. The default is 1.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: An IPv6 black hole route is configured like a normal static route, but with null0 as the outgoing interface.

Example: Configure a black hole route to 2001:2:3:4::/64.

```
Switch(config)#ipv6 route 2001:2:3:4::/64 null0
```

13.8 IPv6 Multicast Protocol

13.8.1 Multicast

13.8.1.1 show ipv6 mroute

Command: show ipv6 mroute [<GroupAddr> [<SourceAddr>]]

Function: Displays the IPv6 software multicast routing table.

Parameters: <GroupAddr>: Displays the multicast entries for this group address.

<SourceAddr>: Displays the multicast entries for this source address.

Default: None.

Command Mode: Admin Mode and Global Mode.

Usage Guidelines: None.

Example: Display all entries in the IPv6 multicast routing table.

```
Switch(config)# show ipv6 mroute
Name: Loopback, Index: 2002, State:49
Name: Vlan1, Index: 2006, State:1043
Name: Vlan11, Index: 2007, State:1043
Name: Vlan12, Index: 2008, State:1043
Name: Tunnel1, Index: 2009, State:d1
Name: Tunnel2, Index: 0, State:0
Name: pim6reg, Index: 2010, State:c1
Name: pimreg, Index: 2011, State:c1
The total matched ip6mr active mfc entries is 1, unresolved ip6mr entries is
1
Group            Origin                    Iif          Wrong     Oif:TTL
ff2f::1         2014:1:2:3::2               Tunnel1         0        2008:1
ff3f::1         2012:1:2:3::2                 NULL         4          0:0
```

Output	Description
Name	Interface name
Index	Interface index
State	Interface state
The total matched ipmr active mfc entries	Total number of matched active multicast forwarding cache (MFC) entries
unresolved ipmr entries	Number of unresolved multicast routing entries
Group	Destination (group) address of the entry
Origin	Source address of the entry
Iif	Incoming interface of the entry
Wrong	Packets received on the wrong interface

13.8.2 PIM-DM6

Note: Some PIM-DM6 show and debug commands are the same as those of PIM-SM6; see the PIM-SM6 commands.

13.8.2.1 debug ipv6 pim timer sat

Command: **`debug ipv6 pim timer sat`**
`no debug ipv6 pim timer sat`

Function: Enables detailed debugging of the PIM-DM source active timer (SAT). The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: When enabled, detailed source active timer (SAT) information is displayed.

Example:

```
Switch # debug ipv6 pim timer sat
```

Note: Other PIM-DM debugging commands are shared with PIM-SM.

13.8.2.2 debug ipv6 pim timer srt

Command: **`debug ipv6 pim timer srt`**
`no debug ipv6 pim timer srt`

Function: Enables detailed debugging of the PIM-DM state refresh timer (SRT). The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: When enabled, detailed state refresh timer (SRT) information is displayed.

Example:

```
Switch # debug ipv6 pim timer srt
```

Note: Other PIM-DM debugging commands are shared with PIM-SM.

13.8.2.3 ipv6 mroute

Command: **`ipv6 mroute <X:X::X:X> <X:X::X:X> <ifname> <.ifname>`**
`no ipv6 mroute <X:X::X:X> <X:X::X:X> [<ifname> <.ifname>]`

Function: Configures a static multicast entry. The **no** form of this command deletes static multicast entries or specific egress interfaces.

Parameters: **<X:X::X:X> <X:X::X:X>** are the multicast source address and group address.

<ifname> <.ifname>: The first interface is the ingress interface; the following interfaces are egress interfaces.

Command Mode: Global Mode.

Default: None.

Usage Guidelines: **<ifname>** must be a valid VLAN interface. Multicast traffic is forwarded only if PIM is configured on the egress interface and the interface is up; if the interface is not up, PIM is not configured, or RPF is not valid, the traffic is not forwarded. With the **no** form, if all egress interfaces or no interfaces are specified, the multicast routing entry is removed; otherwise, only the specified egress interfaces are removed from the entry.

Example:

```
Switch(config)#ipv6 mroute 2001::1 ff1e::1 v10 v20 v30
```

13.8.2.4 ipv6 pim bsr-border

Command: `ipv6 pim bsr-border`
`no ipv6 pim bsr-border`

Function: Configures or removes a PIM6 BSR border interface.

Parameters: None.

Default: The interface is not a BSR border.

Command Mode: Interface Mode.

Usage Guidelines: This command configures the interface as a BSR border. BSR messages are then neither received nor sent on the interface, and all networks connected to the interface are treated as directly connected.

Example:

```
Switch(Config-if-Vlan1)#ipv6 pim bsr-border
```

13.8.2.5 ipv6 pim dense-mode

Command: `ipv6 pim dense-mode`
`no ipv6 pim dense-mode`

Function: Enables PIM-DM on the interface. The **no ipv6 pim dense-mode** command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Interface Mode.

Usage Guidelines: This command takes effect only after IPv6 multicast routing is enabled in Global Mode. Multicast protocol interoperation is not supported; dense mode and sparse mode cannot be enabled on the same switch at the same time. The command can be configured on an IPv6 tunnel interface; configure the tunnel carefully.

Example: Enable PIM-DM on interface VLAN 1.

```
Switch (config)#ipv6 pim multicast-routing
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 pim dense-mode
```

13.8.2.6 ipv6 pim dr-priority

Command: `ipv6 pim dr-priority <priority>`
`no ipv6 pim dr-priority`

Function: Configures the DR priority of the interface. Border nodes on the same segment elect the DR of the segment through Hello messages. The **no ipv6 pim dr-priority** command restores the default.

Parameters: <priority>: The priority, ranging from 0 to 4294967294.

Default: 1.

Command Mode: Interface Mode.

Usage Guidelines: A larger value means a higher priority. The command can be configured on an IPv6 tunnel interface; configure the tunnel carefully.

Example: Set the DR priority of interface VLAN 1 to 100.

```
Switch (config)# interface vlan 1
Switch(Config-if-Vlan1)ipv6 pim dr-priority 100
```

13.8.2.7 ipv6 pim exclude-genid

Command: ipv6 pim exclude-genid
no ipv6 pim exclude-genid

Function: Excludes the GenID option from Hello messages sent by PIM-SM. The **no ipv6 pim exclude-genid** command restores the default.

Parameters: None.

Default: Hello messages include the GenID option.

Command Mode: Interface Mode.

Usage Guidelines: This command is used for interoperability with older Cisco IOS versions. The command can be configured on an IPv6 tunnel interface; configure the tunnel carefully.

Example: Exclude the GenID option from Hello messages sent by the switch.

```
Switch(Config-if-Vlan1)#ipv6 pim exclude-genid
```

13.8.2.8 ipv6 pim hello-holdtime

Command: ipv6 pim hello-holdtime <value>
no ipv6 pim hello-holdtime

Function: Configures or removes the Holdtime value in Hello messages, which is the neighbor timeout. If no Hello message is received from a neighbor within this time, the neighbor is deleted.

Parameters: <value> is the holdtime.

Default: 3.5 times the hello interval. With the default hello interval of 30 seconds, the default holdtime is 105 seconds.

Command Mode: Interface Mode.

Usage Guidelines: If not configured, the holdtime is 3.5 times the current hello interval. A configured holdtime less than the current hello interval is rejected. Each time the hello interval is updated, the holdtime is updated as follows: if the holdtime is not configured, or is less than the current hello interval, it is set to 3.5 times the hello interval; otherwise, the configured value is kept. The command can be configured on an IPv6 tunnel interface; configure the tunnel carefully.

Example: Set the hello holdtime of interface VLAN 1 to 10.

```
Switch (config)# interface vlan1
Switch (Config -if-Vlan1)#ipv6 pim hello-holdtime 10
```

13.8.2.9 ipv6 pim hello-interval

Command: ipv6 pim hello-interval < interval>
no ipv6 pim hello-interval

Function: Configures the PIM-DM Hello message interval of the interface. The **no ipv6 pim hello-interval** command restores the default.

Parameters: <interval> is the interval for sending PIM-DM Hello messages, ranging from 1 to 18724 seconds.

Default: 30 seconds.

Command Mode: Interface Mode.

Usage Guidelines: Hello messages allow PIM-DM switches to discover each other and maintain neighbor relationships. A PIM-DM switch announces its presence by periodically sending Hello messages to its neighbors. If no Hello message is received from a neighbor within the specified time, the neighbor is considered lost. The configured interval must not exceed the neighbor timeout. The command can be configured on an IPv6 tunnel interface; configure the tunnel carefully.

Example: Set the PIM-DM hello interval of interface VLAN 1.

```
Switch (config)#interface vlan1
```

```
Switch(Config-if-Vlan1)#ipv6 pim hello-interval 20
```

13.8.2.10 ipv6 pim multicast-routing

Command: `ipv6 pim multicast-routing`
`no ipv6 pim multicast-routing`

Function: Enables PIM globally. The **no ipv6 pim multicast-routing** command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: IPv6 PIM can be enabled on interfaces only after this command is run.

Example: Enable PIM globally.

```
Switch (config)#ipv6 pim multicast-routing
```

13.8.2.11 ipv6 pim neighbor-filter

Command: `ipv6 pim neighbor-filter <acess-list-name>`
`no ipv6 pim neighbor-filter <acess-list-name>`

Function: Configures a neighbor access list. If an existing neighbor is filtered by the list, the neighbor relationship is torn down immediately; if no neighbor relationship exists, none is established.

Parameters: <access-list-name> is the name of the access list to apply.

Default: No neighbor filter is configured.

Command Mode: Interface Mode.

Usage Guidelines: Use this command to filter PIM messages from peers that should not become neighbors. The command can be configured on an IPv6 tunnel interface; configure the tunnel carefully.

Example: Configure a PIM neighbor access list on interface VLAN 1.

```
Switch (Config-if-Vlan1)#ipv6 pim neighbor-filter myfilter
Switch(config)#ipv6 access-list standard myfilter
Switch(config_IPv6_Std-Nacl-myfilter)#deny fe80:20e:cff:fe01:facc
Switch(config)#ipv6 access-list standard myfilter
Switch(config_IPv6_Std-Nacl-myfilter)#permit any
```

13.8.2.12 ipv6 pim scope-border

Command: `ipv6 pim scope-border [<500-599>|<acl_name>]`
`no ipv6 pim scope-border`

Function: Configures or removes a PIM6 administrative scope border.

Parameters: <500-599> is the ACL number for the administrative scope border.

<acl_name> is the ACL name for the administrative scope border.

Default: Not configured. If no ACL is specified, the default administrative scope border is used.

Command Mode: Interface Mode.

Usage Guidelines: This command configures the administrative scope border and its ACL for IPv6 PIM. Multicast traffic is not forwarded across the scope border.

Example:

```
Switch(Config-if-Vlan2)#ipv6 pim scope-border 503
```

13.8.2.13 ipv6 pim state-refresh origination-interval

Command: ipv6 pim state-refresh origination-interval <interval>
no ipv6 pim state-refresh origination-interval

Function: Configures the interval for sending state refresh messages on the interface. The **no ipv6 pim state-refresh origination-interval** command restores the default.

Parameters: <interval>: The interval, ranging from 4 to 100 seconds.

Default: 60 seconds.

Usage Guidelines: The first-hop router periodically sends state refresh messages to maintain the PIM-DM entries of all downstream routers. This command changes the interval; normally it does not need to be changed. The command can be configured on an IPv6 tunnel interface; configure the tunnel carefully.

Example: Set the state refresh interval of interface VLAN 1 to 90 seconds.

```
Switch (Config-if-Vlan1)#ipv6 pim state-refresh origination-interval  90
```

13.8.2.14 show ipv6 pim interface

Command: show ipv6 pim interface [detail]

Function: Displays PIM interface information.

Parameters: None.

Default: None.

Command Mode: All Modes.

Example:

```
Switch#show ipv6 pim interface
Interface VIFindex Ver/   Nbr    DR
                   Mode   Count  Prior
Vlan2     0        v2/S   0      1
    Address       : fe80::203:fff:fee3:1244
    Global Address: 2000:1:111::100
    DR            : this system
Vlan3     2        v2/S   0      1
    Address       : fe80::203:fff:fee3:1244
    Global Address: 2000:10:1:13::1
    DR            : this system
```

Output	Description
Address	Interface address
Interface	Interface name
VIF index	Interface index
Ver/Mode	PIM version and mode: usually v2; S for sparse mode, D for dense mode
Nbr Count	Number of neighbors on the interface
DR Prior	DR priority
DR	DR address of the interface

13.8.2.15 show ipv6 pim mroute dense-mode

Command: show ipv6 pim mroute dense-mode [group <X:X::X:X>] [source <X:X::X:X>]

Function: Displays PIM-DM forwarding entries.

Parameters: group <X:X::X:X>: Displays the forwarding entries for this group address.

source <X:X::X:X>: Displays the forwarding entries for this source address.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays the PIM-DM multicast forwarding entries, that is, the entries in the system FIB used to forward multicast packets.

Example: Display all PIM-DM forwarding entries.

```
Switch(config)#show ipv6 pim mroute dense-mode
IP Multicast Routing Table
(*,G) Entries: 1
(S,G) Entries: 1
(*, ff1e::15)
 Local     ..l.............................
(2000:10:1:12::11, ff1e::15)
RPF nbr: ::
RPF idx: Vlan12
Upstream State: FORWARDING
Origin State: ORIGINATOR
 Local     ..............................
 Pruned    ..............................
 Asserted  ..............................
 Outgoing  ..o............................
Switch#
```

Output	Description
(*, ff1e::15)	(*,G) forwarding entry
(2000:10:1:12::11, ff1e::15)	(S,G) forwarding entry
RPF nbr	RPF neighbor: the upstream neighbor toward the source in DM; 0.0.0.0 means the switch is the first hop.
RPF idx	Interface on which the RPF neighbor is located
Upstream State	Upstream state: FORWARDING (upstream is forwarding data), PRUNED (upstream has stopped forwarding data), or ACKPENDING (waiting for an upstream response; upstream is forwarding data)
Origin State	Origin state: ORIGINATOR (sends state refresh messages) or NON_ORIGINATOR (does not send state refresh messages)
Local	Local join interface: the interface has received an IGMP join
Pruned	PIM pruned interface: the interface has received Prune messages
Asserted	Assert state
Outgoing	Index of the interface on which multicast data is finally forwarded; here the index is 2. Use **show ipv6 pim interface** to view interface details.

13.8.2.16 show ipv6 pim neighbor

Command: `show ipv6 pim neighbor [detail|]`

Function: Displays PIM neighbor routers.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the multicast router neighbors maintained by PIM.

Example:

```
Switch(config)#show ipv6 pim neighbor
Neighbor                Interface          Uptime/Expires    Ver   DR
Address
Priority/Mode
Fe80::203:fff:fee3:1244     Vlan1             00:00:10/00:01:35  v2     1 /DR
fe80::20e:cff:fe01:facc      Vlan1             00:00:13/00:01:32  v2     1 /
```

Output	Description
Neighbor Address	Neighbor address
Interface	Interface on which the neighbor is located
Uptime/Expires	Uptime and expiration time
Ver	PIM version, usually v2
DR Priority/Mode	DR priority in the neighbor's Hello messages, and whether the neighbor is the DR of the interface

13.8.2.17 show ipv6 pim nexthop

Command: `show ipv6 pim nexthop`

Function: Displays the next-hop routers cached by PIM from the unicast routing table.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the next-hop router information cached by PIM.

Example:

```
Switch#show ipv6 pim nexthop
Flags: N = New, R = RP, S = Source, U = Unreachable      ….
Destination          Type  Nexthop Nexthop   Nexthop  Nexthop Metric Pref
Refcnt  Num     Addr      Ifindex   Name
2000:1:111::11      ..S.     1                2004             0     0     2
2000:1:111::100    .RS.     1                2004             0     0     2
```

Output	Description
Destination	Destination of the next-hop entry
Type	N: newly created next hop; RP and source directions not yet determined. R: RP direction. S: source direction. U: unreachable.
Nexthop Num	Number of next hops
Nexthop Addr	Next-hop address
Nexthop Ifindex	Next-hop interface index
Nexthop Name	Next-hop interface name
Metric	Metric to the next hop
Pref	Route preference
Refcnt	Reference count

13.8.3 PIM-SM6

13.8.3.1 clear ipv6 pim bsr rp-set

Command: `clear ipv6 pim bsr rp-set *`

Function: Clears all RP information.

Parameters: None.

Command Mode: Admin Mode.

Usage Guidelines: Quickly clears all RP information.

Example: Clear all RP information.

```
Switch# clear ipv6 pim bsr rp-set *
```

Related Commands: show ipv6 pim bsr-router

13.8.3.2 debug ipv6 pim events

Command: debug ipv6 pim events
no debug ipv6 pim events

Function: Enables or disables PIM event debugging.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: When enabled, information about PIM operation events is displayed.

Example: Enable PIM event debugging.

```
Switch# debug ipv6 pim events
```

13.8.3.3 debug ipv6 pim mfc

Command: debug ipv6 pim mfc（in|out|）
no debug ipv6 pim mfc（in|out|）

Function: Enables or disables PIM MFC debugging.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: When enabled, information about the multicast forwarding cache entries generated and sent is displayed.

Example: Enable PIM MFC debugging.

```
Switch# debug ipv6 pim mfc in
```

13.8.3.4 debug ipv6 pim mib

Command: debug ipv6 pim mib
no ipv6 debug pim mib

Function: Enables or disables PIM MIB debugging.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Displays PIM MIB information. This function is currently not available and is reserved for future use.

Example: Enable PIM MIB debugging.

```
Switch# debug ipv6 pim mib
```

13.8.3.5 debug ipv6 pim nexthop

Command: debug ipv6 pim nexthop
no debug ipv6 pim nexthop

Function: Enables or disables PIM next-hop debugging.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Displays PIM next-hop change information.

Example: Enable PIM next-hop debugging.

```
Switch# debug ipv6 pim nexthop
```

13.8.3.6 debug ipv6 pim nsm

Command: **`debug ipv6 pim nsm`**
`no debug ipv6 pim nsm`

Function: Enables or disables debugging of communication between PIM and Network Services.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Displays the information exchanged between PIM and Network Services (NSM).

Example: Enable debugging of communication between PIM and Network Services.

```
Switch# debug ipv6 pim nsm
```

13.8.3.7 debug ipv6 pim packet

Command: **`debug ipv6 pim packet [in|out|]`**
`no debug ipv6 pim packet [in|out|]`

Function: Enables or disables PIM packet debugging.

Parameters: **in**: Displays only received PIM packets.

out: Displays only sent PIM packets.

If neither is specified, both are displayed.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Displays received and sent PIM packets.

Example: Enable debugging of received PIM packets.

```
Switch# debug ipv6 pim packet in
```

13.8.3.8 debug ipv6 pim state

Command: **`debug ipv6 pim state`**
`no debug ipv6 pim state`

Function: Enables or disables PIM state debugging.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Displays PIM state change information.

Example: Enable PIM state debugging.

```
Switch# debug ipv6 pim state
```

13.8.3.9 debug ipv6 pim timer

Command: debug ipv6 pim timer

```
debug ipv6 pim timer assert
debug ipv6 pim timer assert at
debug ipv6 pim timer bsr bst
debug ipv6 pim timer bsr crp
debug ipv6 pim timer bsr
debug ipv6 pim timer hello ht
debug ipv6 pim timer hello nlt
debug ipv6 pim timer hello tht
debug ipv6 pim timer hello
debug ipv6 pim timer joinprune et
debug ipv6 pim timer joinprune grt
debug ipv6 pim timer joinprune jt
debug ipv6 pim timer joinprune kat
debug ipv6 pim timer joinprune ot
debug ipv6 pim timer joinprune plt
debug ipv6 pim timer joinprune ppt
debug ipv6 pim timer joinprune pt
debug ipv6 pim timer joinprune
debug ipv6 pim timer register rst
debug ipv6 pim timer register
no debug ipv6 pim timer
no debug ipv6 pim timer assert
no debug ipv6 pim timer assert at
no debug ipv6 pim timer bsr bst
no debug ipv6 pim timer bsr crp
no debug ipv6 pim timer bsr
no debug ipv6 pim timer hello ht
no debug ipv6 pim timer hello nlt
no debug ipv6 pim timer hello tht
no debug ipv6 pim timer hello
no debug ipv6 pim timer joinprune et
no debug ipv6 pim timer joinprune grt
no debug ipv6 pim timer joinprune jt
no debug ipv6 pim timer joinprune kat
no debug ipv6 pim timer joinprune ot
no debug ipv6 pim timer joinprune plt
no debug ipv6 pim timer joinprune ppt
no debug ipv6 pim timer joinprune pt
no debug ipv6 pim timer joinprune
no debug ipv6 pim timer register rst
no debug ipv6 pim timer register
no debug ipv6 pim timer
```

Function: Enables or disables debugging of each PIM timer.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Enables debugging information for the specified timer.

Example: Enable debugging of the PIM assert timer.

```
Switch# debug ipv6 pim timer assert
```

13.8.3.10 ipv6 mroute

Command: `ipv6 mroute <X:X::X:X> <X:X::X:X> <ifname> <.ifname>`
`no ipv6 mroute <X:X::X:X> <X:X::X:X> [<ifname> <.ifname>]`

Function: Configures a static multicast entry. The **no** form of this command deletes static multicast entries or specific egress interfaces.

Parameters: <X:X::X:X> <X:X::X:X> are the multicast source address and group address.

<ifname> <.ifname>: The first interface is the ingress interface; the following interfaces are egress interfaces.

Command Mode: Global Mode.

Default: None.

Usage Guidelines: <ifname> must be a valid VLAN interface. Multicast traffic is forwarded only if PIM is configured on the egress interface and the interface is up; if the interface is not up, PIM is not configured, or RPF is not valid, the traffic is not forwarded. With the **no** form, if all egress interfaces or no interfaces are specified, the multicast routing entry is removed; otherwise, only the specified egress interfaces are removed from the entry.

Example:

```
Switch(config)#ipv6 mroute 2001::1 ff1e::1 v10 v20 v30
```

13.8.3.11 ipv6 multicast unresolved-cache aging-time

Command: `ipv6 multicast unresolved-cache aging-time <value>`
`no ipv6 multicast unresolved-cache aging-time`

Function: Configures the cache time of unresolved kernel multicast routes. The **no** form of this command restores the default.

Parameters: <value> is the cache time, ranging from 1 to 20 seconds.

Default: 20 seconds.

Command Mode: Global Mode.

Usage Guidelines: Configures the cache time of multicast route entries in the kernel.

Example:

```
Switch(config)# ipv6 multicast unresolved-cache aging-time 18
```

13.8.3.12 ipv6 pim accept-register

Command: `ipv6 pim accept-register list <acess-list-name>`
`no ipv6 pim accept-register`

Function: Filters PIM Register messages for the specified multicast sources and groups.

Parameters: <access-list-name> is the name of the access list to apply.

Default: Register messages from any source to any group are permitted.

Command Mode: Global Mode.

Usage Guidelines: This command configures the access list that filters PIM REGISTER packets. The addresses in the access list specify the filtered multicast sources and groups. For source-group pairs that match DENY, PIM immediately sends REGISTER-STOP and does not create group records when it receives REGISTER packets. Unlike other access lists, the default action of this access list is PERMIT.

Example: Filter Register messages with access list myfilter.

```
Switch(config)#ipv6 pim accept-register list myfilter
Switch(config)#ipv6 access-list standard myfilter
Switch(config_IPv6_Std-Nacl-myfilter)#permit ff1e::10/128
```

13.8.3.13 ipv6 pim bsr-border

Command: ipv6 pim bsr-border
no ipv6 pim bsr-border

Function: Configures or removes a PIM6 BSR border interface.

Parameters: None.

Default: The interface is not a BSR border.

Command Mode: Interface Mode.

Usage Guidelines: This command configures the interface as a BSR border. BSR messages are then neither received nor sent on the interface, and all networks connected to the interface are treated as directly connected.

Example:

```
Switch(Config-if-Vlan1)#ipv6 pim bsr-border
```

13.8.3.14 ipv6 pim bsr-candidate

Command: ipv6 pim bsr-candidate {vlan <vlan_id>|tunnel <tunnel-id>| <ifname>} [<hash-mask-length>] [<priority>]
no ipv6 pim bsr-candidate {vlan <vlan_id>| tunnel <tunnel-id>| <ifname>} [<hash-mask-length>] [<priority>]

Function: Configures the switch as a candidate BSR so that it competes with other candidate BSRs for the BSR role. The **no ipv6 pim bsr-candidate** command removes the candidate BSR configuration.

Parameters: <vlan_id> is the VLAN ID, ranging from 1 to 4094.

<tunnel-id> is the tunnel ID, ranging from 1 to 50.

<ifname> is the interface name.

<hash-mask-length> is the hash mask length used for RP selection, ranging from 0 to 32.

<priority> is the candidate BSR priority, ranging from 0 to 255. The default is 0.

Default: The switch is not a candidate BSR.

Command Mode: Global Mode.

Usage Guidelines: The switch becomes a candidate BSR only after this command is configured.

Example: Configure interface VLAN 1 as the candidate BSR interface.

```
Switch (config)# ipv6 pim bsr-candidate vlan1 30 10
```

13.8.3.15 ipv6 pim cisco-register-checksum

Command: ipv6 pim cisco-register-checksum [group-list <access-list name>]
no ipv6 pim cisco-register-checksum [group-list <access-list name>]

Function: Configures the Register packet checksum for the groups specified by the access list to be calculated over the whole packet.

Default: The checksum is calculated over the Register packet header (8 bytes).

Parameters: <access-list name> is the standard access list to apply.

Command Mode: Global Mode.

Usage Guidelines: This command is used for interoperability with older Cisco IOS versions.

Example: Calculate the Register packet checksum over the whole packet for the groups specified by myfilter.

```
Switch(config)#ipv6 pim cisco-register-checksum group-list myfilter
Switch(config)#ipv6 access-list standard myfilter
Switch(config_IPv6_Std-Nacl-myfilter)#permit ff1e::10/128
```

13.8.3.16 ipv6 pim dr-priority

Command: ipv6 pim dr-priority <priority>
no ipv6 pim dr-priority

Function: Configures the DR priority of the interface. Neighboring nodes on the same segment elect the DR of the segment through Hello packets. The **no ipv6 pim dr-priority** command restores the default.

Parameters: <priority>: The priority, ranging from 0 to 4294967294.

Default: 1.

Command Mode: Interface Mode.

Usage Guidelines: A larger value means a higher priority. The command can be configured on an IPv6 tunnel interface; configure the tunnel carefully.

Example: Set the DR priority of interface VLAN 1 to 100.

```
Switch (config)# interface vlan 1
Switch(Config-if-Vlan1)ipv6 pim dr-priority 100
```

13.8.3.17 ipv6 pim exclude-genid

Command: ipv6 pim exclude-genid
no ipv6 pim exclude-genid

Function: Excludes the GenID option from Hello packets sent by PIM-SM. The **no ipv6 pim exclude-genid** command restores the default.

Parameters: None.

Default: Hello packets include the GenID option.

Command Mode: Interface Mode.

Usage Guidelines: This command is used for interoperability with older Cisco IOS versions. The command can be configured on an IPv6 tunnel interface; configure the tunnel carefully.

Example: Exclude the GenID option from Hello packets sent by the switch.

```
Switch(Config-if-Vlan1)#ipv6 pim exclude-genid
```

13.8.3.18 ipv6 pim hello-holdtime

Command: ipv6 pim hello-holdtime <value>
no ipv6 pim hello-holdtime

Function: Configures or removes the Holdtime option in Hello packets, which is the neighbor holdtime. If no Hello packet is received from a neighbor within the holdtime, the neighbor is deleted.

Parameters: <value> is the holdtime.

Default: 3.5 times the hello interval. With the default hello interval of 30 seconds, the default holdtime is 105 seconds.

Command Mode: Interface Mode.

Usage Guidelines: If not configured, the holdtime is 3.5 times the hello interval. A configured holdtime less than the current hello interval is rejected. Each time the hello interval is updated, the holdtime is updated as follows: if the holdtime is not configured, or is less than the current hello

interval, it is set to 3.5 times the hello interval; otherwise, the configured value is kept. The command can be configured on an IPv6 tunnel interface; configure the tunnel carefully.

Example: Set the hello holdtime of VLAN 1 to 10 seconds.

```
Switch (config)# interface vlan1
Switch (Config -if-Vlan1)#ipv6 pim hello-holdtime 10
```

13.8.3.19 ipv6 pim hello-interval

Command: ipv6 pim hello-interval <interval>
no ipv6 pim hello-interval

Function: Configures the PIM Hello interval of the interface. The **no ipv6 pim hello-interval** command restores the default.

Parameters: <interval> is the interval for sending PIM Hello packets, ranging from 1 to 18724 seconds.

Default: 30 seconds.

Command Mode: Interface Mode.

Usage Guidelines: Hello messages allow PIM switches to discover each other and establish neighbor relationships. A PIM switch announces its presence by periodically sending Hello messages to its neighbors. If no Hello message is received from a neighbor within the specified time, the neighbor is considered lost. This value cannot be greater than the neighbor timeout. The command can be configured on an IPv6 tunnel interface; configure the tunnel carefully.

Example: Set the PIM-SM hello interval of VLAN 1.

```
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 pim hello-interval 20
```

13.8.3.20 ipv6 pim ignore-rp-set-priority

Command: ipv6 pim ignore-rp-set-priority
no ipv6 pim ignore-rp-set-priority

Function: Configures the switch to use only the hash algorithm and ignore RP priority during RP selection. This command is used for interoperability with older Cisco IOS versions.

Default: None.

Parameters: None.

Command Mode: Global Mode.

Usage Guidelines: PIM normally selects the RP by RP priority. When this command is configured, RP priority is ignored. This command is not recommended unless older routers exist in the network.

Example: Ignore RP priority.

```
Switch(config)#ipv6 pim ignore-rp-set-priority
```

13.8.3.21 ipv6 pim jp-timer

Command: ipv6 pim jp-timer <value>
no ipv6 pim jp-timer

Function: Configures the Join/Prune (JP) timer. The **no ipv6 pim jp-timer** command restores the default.

Parameters: <value>: The timer value, ranging from 10 to 65535 seconds.

Default: 60 seconds.

Command Mode: Global Mode.

Usage Guidelines: Configures the interval for sending Join/Prune messages.

Example: Set the Join/Prune interval to 59 seconds.

```
Switch(config)#ipv6 pim jp-timer 59
```

13.8.3.22 ipv6 pim multicast-routing

Command: `ipv6 pim multicast-routing`
`no ipv6 pim multicast-routing`

Function: Enables PIM-SM globally. The **no ipv6 pim multicast-routing** command disables PIM-SM globally.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: IPv6 PIM can be enabled on interfaces only after this command is run.

Example: Enable PIM-SM globally.

```
Switch (config)#ipv6 pim multicast-routing
```

13.8.3.23 ipv6 pim neighbor-filter

Command: `ipv6 pim neighbor-filter <acess-list-name>`
`no ipv6 pim neighbor-filter <acess-list-name>`

Function: Configures a neighbor access list. If an existing neighbor is filtered by the list, the neighbor relationship is torn down immediately; if no neighbor relationship exists, none is established.

Parameters: <access-list-name> is the name of the access list to apply.

Default: No neighbor filter is configured.

Command Mode: Interface Mode.

Usage Guidelines: The default action of an ACL is DENY. In the following example, if **permit any** is not configured, **deny fe80:20e:cff:fe01:facc** has the same effect as **deny any**. The command can be configured on an IPv6 tunnel interface; configure the tunnel carefully.

Example: Configure a PIM neighbor access list on VLAN 1.

```
Switch (Config-if-Vlan1)#ipv6 pim neighbor-filter myfilter
Switch(config)#ipv6 access-list standard myfilter
Switch(config_IPv6_Std-Nacl-myfilter)#deny fe80:20e:cff:fe01:facc
Switch(config)#ipv6 access-list standard myfilter
Switch(config_IPv6_Std-Nacl-myfilter)#permit any
```

13.8.3.24 ipv6 pim register-rate-limit

Command: `ipv6 pim Register-rate-limit <limit>`
`no ipv6 pim Register-rate-limit`

Function: Configures the rate at which the DR sends Register packets, in packets per second. The **no ipv6 pim register-rate-limit** command restores the default. The configured rate applies to each (S,G) state, not to the whole system.

Parameters: <limit> ranges from 1 to 65535.

Default: No limit.

Command Mode: Global Mode.

Usage Guidelines: Configures the rate at which the DR sends Register packets.

Example: Set the rate at which the DR sends Register packets to 59 packets per second.

```
Switch(config)#ipv6 pim Register-rate-limit 59
```

13.8.3.25 ipv6 pim register-rp-reachability

Command: `ipv6 pim Register-rp-reachability`
`no ipv6 pim Register-rp-reachability`

Function: Configures the DR to check RP reachability during registration.

Parameters: None.

Default: Not checked.

Command Mode: Global Mode.

Usage Guidelines: Configures whether the DR checks RP reachability.

Example: Configure the router to check RP reachability before sending Register packets.

```
Switch(config)# ipv6 pim Register-rp-reachability
```

13.8.3.26 ipv6 pim register-source

Command: `ipv6 pim register-source {<source-address> |<ifname>|vlan <vlan-id>}`
`no ipv6 pim register-source`

Function: Configures the source address of Register packets sent by the DR, overriding the default source address, which is usually the RPF neighbor toward the source host.

Parameters: <ifname> is the name of the interface whose address is used as the Register packet source.

<source-address> is the interface address used as the Register packet source, in hexadecimal notation without prefix length.

<vlan-id> is the VLAN ID.

Default: Not configured.

Command Mode: Global Mode.

Usage Guidelines: The **no ipv6 pim register-source** command restores the default; no parameter is needed. The configured address must be reachable by Register-Stop messages sent by the RP. It is usually a loopback address, but other physical addresses can be used. The address must be advertised by the unicast routing protocols of the DR.

Example: Use the address of VLAN 1 as the source address of Register packets.

```
Switch(config)# ipv6 pim register-source Vlan1
```

13.8.3.27 ipv6 pim register-suppression

Command: `ipv6 pim register-suppression <value>`
`no ipv6 pim register-suppression`

Function: Configures the Register suppression timer, in seconds.

Parameters: <value> is the timer value, ranging from 10 to 65535 seconds.

Default: 60 seconds.

Command Mode: Global Mode.

Usage Guidelines: On the DR, this value is the Register suppression timer. On the RP, if **ipv6 pim rp-register-kat** is not used, this command changes the Keepalive period. The **no ipv6 pim register-suppression** command restores the default.

Example: Set the Register suppression timer to 30 seconds.

```
Switch(config)# ipv6 pim register-suppression 30
```

13.8.3.28 ipv6 pim rp-address

Command: `ipv6 pim rp-address <rp-address> [<group-range>]`
`no ipv6 pim rp-address <rp-address> [all|<group-range>]`

Function: Configures a static RP globally or for a multicast address range. The **no ipv6 pim rp-address** command removes the static RP.

Parameters: <rp-address> is the RP IPv6 address, in the format X:X::X:X.

<group-range> is the group range served by the RP, in the format X:X::X:X/M (IPv6 address and prefix length).

Default: No static RP is configured.

Command Mode: Global Mode.

Usage Guidelines: Configures a static RP globally or for a multicast address range.

Example: Configure 2000:112::8 as the RP for group range ff1e::/64.

```
Switch (config)# ipv6 pim rp-address 2000:112::8 ff1e::/64
```

13.8.3.29 ipv6 pim rp-candidate

Command: `ipv6 pim rp-candidate{vlan<vlan-id> |loopback<index> |<ifname>}`
`[<group range>] [<priority>]`
`no ipv6 pim rp-candiate`

Function: Configures the switch as a candidate RP so that it competes with other candidate RPs for the RP role. The **no ipv6 pim rp-candidate** command removes the candidate RP configuration.

Parameters: <vlan-id> is the VLAN ID.

<index> is the loopback interface index.

<ifname> is the interface name.

<group range> is the group range of the candidate RP, in the format X:X::X:X/M (IPv6 address and prefix length).

<priority> is the RP selection priority, ranging from 0 to 255. The default is 192; a lower value means a higher priority.

Default: The switch is not a candidate RP.

Command Mode: Global Mode.

Usage Guidelines: The switch becomes a candidate RP only after this command is configured.

Example: Configure VLAN 1 as the interface for sending candidate RP advertisements.

```
Switch (config)# ipv6 pim rp-candidate vlan1 100
```

13.8.3.30 ipv6 pim rp-register-kat

Command: `ipv6 pim rp-register-kat <vaule>`
`no ipv6 pim rp-register-kat`

Function: Configures the KAT (Keepalive Timer) of (S,G) entries on the RP, in seconds. The **no ipv6 pim rp-register-kat** command restores the default.

Parameters: <value> is the timer value, ranging from 1 to 65535 seconds.

Default: 185 seconds.

Command Mode: Global Mode.

Usage Guidelines: Configures the Keepalive timer of (S,G) entries created on the RP by Register messages.

Example: Set the RP register KAT to 30 seconds.

```
Switch(config)# ipv6 pim rp-register-kat 30
```

13.8.3.31 ipv6 pim scope-border

Command: ipv6 pim scope-border [<500-599>|<acl_name>]
no ipv6 pim scope-border

Function: Configures or removes a PIM6 administrative scope border.

Parameters: <500-599> is the ACL number for the administrative scope border.

<acl_name> is the ACL name for the administrative scope border.

Default: Not configured. If no ACL is specified, the default administrative scope border is used.

Command Mode: Interface Mode.

Usage Guidelines: This command configures the administrative scope border and its ACL for IPv6 PIM. Multicast traffic is not forwarded across the scope border.

Example:

```
Switch(Config-if-Vlan2)#ipv6 pim scope-border 503
```

13.8.3.32 ipv6 pim sparse-mode

Command: ipv6 pim sparse-mode [passive]
no ipv6 pim sparse-mode [passive]

Function: Enables PIM-SM on the interface. The **no ipv6 pim sparse-mode** command disables PIM-SM.

Parameters: passive: PIM-SM does not receive any packets on the interface; only MLD is enabled (MLD packets are received and sent).

Default: Disabled.

Command Mode: Interface Mode.

Usage Guidelines: Enables PIM-SM on the interface. The command can be configured on an IPv6 tunnel interface; configure the tunnel carefully.

Example: Enable PIM-SM on interface VLAN 1.

```
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 pim sparse-mode
```

13.8.3.33 show ipv6 pim bsr-router

Command: show ipv6 pim bsr-router

Function: Displays BSR information.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Global Mode.

Example:

```
Switch#show ipv6 pim bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 2000:1:111::100 (?)
  Uptime:      00:16:00, BSR Priority: 0, Hash mask length: 126
  Next bootstrap message in 00:00:10
  Role: Candidate BSR
  State: Elected BSR
Next Cand_RP_advertisement in 00:00:10
  RP: 2000:1:111::100(Vlan2)
```

Output	Description
BSR address	BSR address
Priority	BSR priority

Hash mask length	BSR hash mask length
State	Current state of the candidate BSR; Elected BSR means it has been elected as the BSR

13.8.3.34 show ipv6 pim interface

Command: `show ipv6 pim interface [detail]`

Function: Displays PIM interface information.

Parameters: None.

Default: None.

Command Mode: All Modes.

Example:

```
Switch#show ipv6 pim interface
Interface VIFindex Ver/   Nbr    DR
                   Mode   Count  Prior
Vlan2     0        v2/S   0      1
    Address       : fe80::203:fff:fee3:1244
    Global Address: 2000:1:111::100
    DR            : this system
Vlan3     2        v2/S   0      1
    Address       : fe80::203:fff:fee3:1244
    Global Address: 2000:10:1:13::1
    DR            : this system
```

Output	Description
Address	Interface address
Interface	Interface name
VIF index	Interface index
Ver/Mode	PIM version and mode: usually v2; S for sparse mode, D for dense mode
Nbr Count	Number of neighbors on the interface
DR Prior	DR priority
DR	DR address of the interface

13.8.3.35 show ipv6 pim mroute sparse-mode

Command: `show ipv6 pim mroute sparse-mode`

Function: Displays the PIM-SM multicast routing table.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the PIM-SM multicast routing entries maintained on the switch.

Example:

```
Switch#show ipv6 pim mr  group ff1e::15
IPv6 Multicast Routing Table
 (*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 1
(S,G,rpt) Entries: 1
FCR Entries: 0
 (*, ff1e::15)
RP: 2000:1:111::100
RPF nbr: ::
RPF idx: None
Upstream State: JOINED
```

```
 Local     ..l.............................
 Joined    ................................
 Asserted  ................................
FCR:
 (2000:1:111::11, ff1e::15)
RPF nbr: ::
RPF idx: None
SPT bit: 1
Upstream State: JOINED
 Local     ................................
 Joined    ................................
 Asserted  ................................
 Outgoing  ..o.............................
 (2000:1:111::11, ff1e::15, rpt)
RP: 2000:1:111::100
RPF nbr: ::
RPF idx: None
Upstream State: NOT PRUNED
 Pruned    ................................
 Outgoing  ..o.............................
```

Output	Description
Entries	Number of entries of each type
RP	RP address of the shared tree
RPF nbr	Upstream neighbor toward the RP or the source
RPF idx	Interface of the RPF neighbor
Upstream State	Upstream state: Joined (joined the tree; expects data from upstream) or Not Joined (left the tree; does not expect data from upstream). For (S,G,rpt) entries, RPT Not Joined, Pruned, and Not Pruned are also possible.
Local	Local join interface: the interface has received an MLD join
Joined	PIM join interface: the interface has received Join/Prune messages
Asserted	Assert state
Outgoing	Final outgoing interfaces of multicast data

13.8.3.36 show ipv6 pim neighbor

Command: `show ipv6 pim neighbor [detail|]`

Function: Displays PIM neighbor routers.

Parameters: None.

Default: None.

Command Mode: All Modes.

Usage Guidelines: Displays the multicast router neighbors maintained by PIM.

Example:

```
Switch(config)#show ipv6 pim neighbor
Neighbor                Interface          Uptime/Expires    Ver   DR
Address
Priority/Mode
Fe80::203:fff:fee3:1244     Vlan1            00:00:10/00:01:35  v2     1 /DR
fe80::20e:cff:fe01:facc      Vlan1            00:00:13/00:01:32  v2     1 /
```

Output	Description

Neighbor Address	Neighbor address
Interface	Interface on which the neighbor is located
Uptime/Expires	Uptime and expiration time
Ver	PIM version, usually v2
DR Priority/Mode	DR priority in the neighbor's Hello messages, and whether the neighbor is the DR of the interface

13.8.3.37 show ipv6 pim nexthop

Command: `show ipv6 pim nexthop`

Function: Displays the next-hop routers cached by PIM from the unicast routing table.

Parameters: None.

Default: None.

Command Mode: All Modes.

Usage Guidelines: Displays the next-hop router information cached by PIM.

Example:

```
Switch#show ipv6 pim nexthop
Flags: N = New, R = RP, S = Source, U = Unreachable      ….
Destination         Type  Nexthop Nexthop  ..Nexthop  Nexthop Metric Pref
Refcnt
                           Num    Addr     Ifindex    Name
2000:1:111::11       ..S.     1                2004             0     0
2
2000:1:111::100     .RS.     1                2004             0      0     2
```

Output	Description
Destination	Destination of the next-hop entry
Type	N: newly created next hop; RP and source directions not yet determined. R: RP direction. S: source direction. U: unreachable.
Nexthop Num	Number of next hops
Nexthop Addr	Next-hop address
Nexthop Ifindex	Next-hop interface index
Nexthop Name	Next-hop interface name
Metric	Metric to the next hop
Pref	Route preference
Refcnt	Reference count

13.8.3.38 show ipv6 pim rp-hash

Command: `show ipv6 pim rp-hash X:X::X:X`

Function: Displays the RP address for group X:X::X:X.

Parameters: X:X::X:X: The group address.

Default: None.

Command Mode: All Modes.

Usage Guidelines: Displays the RP address for the specified group address.

Example:

```
Switch#show ipv6 pim rp-hash ff1e::15
    RP: 2000:1:111::100
    Info source: 2000:1:111::100, via bootstrap
```

Output	Description

RP	RP of the queried group
Info source	Source of the Bootstrap information

13.8.3.39 show ipv6 pim rp mapping

Command: `show ipv6 pim rp mapping`

Function: Displays group-to-RP mappings and RPs.

Parameters: None.

Default: None.

Command Mode: All Modes.

Usage Guidelines: Displays the current RPs and group-to-RP mappings.

Example:

```
Switch#show ipv6 pim rp mapping
PIM Group-to-RP Mappings
This system is the Bootstrap Router (v2)
Group(s): ff00::/8
  RP: 2000:1:111::100
    Info source: 2000:1:111::100, via bootstrap, priority 192
         Uptime: 00:10:24, expires: 00:02:06
Group(s): ff00::/8, Static
    RP: 2000:1:111::100
         Uptime: 00:11:01
```

Output	Description
Group(s)	Group address range of the RP
Info source	Source of the Bootstrap messages
Priority	RP priority advertised in the Bootstrap messages

13.8.4 ANYCAST RP v6

13.8.4.1 debug ipv6 pim anycast-rp

Command: `debug ipv6 pim anycast-rp`
`no debug ipv6 pim anycast-rp`

Function: Enables Anycast RP debugging. The **no** form of this command disables it.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: This command enables Anycast RP debugging on the router; it displays information about PIM Register packet handling (packet) and events (event).

Example:

```
Switch#debug ipv6 pim anycast-rp
```

13.8.4.2 ipv6 pim anycast-rp

Command: `ipv6 pim anycast-rp`
`no ipv6 pim anycast-rp`

Function: Enables Anycast RP on the switch. The **no** form of this command disables it.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: This command enables Anycast RP globally. For Anycast RP to work, the self-rp-address and the set of other-rp-addresses must also be configured.

Example: Enable Anycast RP in Global Mode.

```
Switch(config)#ipv6 pim anycast-rp
```

13.8.4.3 ipv6 pim anycast-rp

Command: ipv6 pim anycast-rp <anycast-rp-addr> <other-rp-addr>
no ipv6 pim anycast-rp <anycast-rp-addr> <other-rp-addr>

Function: Configures the Anycast RP address (ARA) and the unicast addresses of the other RPs that communicate with this router (as an RP). The **no** form of this command removes the unicast address of the other RP for the configured RP address.

Parameters: <anycast-rp-addr>: The RP address. It can be configured even if the corresponding candidate interface does not yet exist.

<other-rp-addr>: The unicast address of another RP that communicates with this router (as an RP).

Command Mode: Global Mode.

Default: Not configured.

Usage Guidelines: 1. The **anycast-rp-addr** configured on this router (as an RP) is the RP address shared by multiple RPs in the network, corresponding to the address of the RP candidate interface (or loopback interface). It can be configured even if the candidate interface does not yet exist.

2. Configure the **other-rp-addr** of the other RPs that communicate with this router (as an RP). This unicast address identifies the other RP and is used to communicate with the local router.

3. When this router (as an RP) receives a Register message unicast from a DR, it forwards the message to the other RPs in the network to notify them of the (S,G) state. When forwarding, the router changes the destination address of the Register message to the **other-rp-addr**.

4. Multiple **other-rp-addr** values can be configured for one **anycast-rp-addr**; a Register message received from a DR is forwarded to each of these RPs in turn.

Example: Configure an other-rp-address in Global Mode.

```
Switch(config)#ipv6 pim anycast-rp 2000::1 2004::2
```

13.8.4.4 ipv6 pim anycast-rp self-rp-address

Command: ipv6 pim anycast-rp self-rp-address <self-rp-addr>
no ipv6 pim anycast-rp self-rp-address

Function: Configures the self-rp-address of this router (as an RP). This address uniquely identifies this router among the RPs and is used to communicate with the other RPs. The **no** form of this command removes the address.

Parameters: <self-rp-addr>: The unicast address used by this router (as an RP) to communicate with the other RPs.

Command Mode: Global Mode.

Default: Not configured.

Usage Guidelines: 1. When this router (as an RP) receives a Register message unicast from a DR, it forwards the message to all other RPs in the network to notify them of the (S,G) state. When forwarding, it changes the source address of the Register message to the self-rp-address.

2. When this router (as an RP) receives a Register message unicast from another RP, that is, a Register message whose destination is the self-rp-address of this router, it creates the (S,G) state and sends a Register-Stop message to the source address of the Register message.

3. The self-rp-address must be the address of a Layer 3 interface on this router, but it can be configured even if the interface does not yet exist.

Example: Configure the self-rp-address of this router in Global Mode.

```
Switch(config)#ipv6 pim anycast-rp self-rp-address 2000::1
```

13.8.4.5 ipv6 pim rp-candidate

Command: ipv6 pim rp-candidate {vlan<vlan-id> |loopback<index> |<ifname>} [<A:B::C:D>] [<priority>]
no ipv6 pim rp-candidate

Function: Extends the PIM-SM6 rp-candidate command so that a loopback interface can be a candidate RP interface. The **no** form of this command removes the candidate RP interface.

Parameters: <index>: The loopback interface index, ranging from 1 to 1024.

<vlan-id>: The VLAN ID.

<ifname>: The interface name.

<A:B::C:D>: The group prefix and prefix length.

<priority>: The RP election priority, ranging from 0 to 255. The default is 192; a smaller value means a higher priority.

Command Mode: Global Mode.

Default: No candidate RP interface is configured.

Usage Guidelines: To support Anycast RP, a loopback interface can be configured as the candidate RP interface. The candidate RP interface must be unique, and its address must be advertised by the routing protocol so that PIM routers can find the nearest RP. The **no ipv6 pim rp-candidate** command removes the candidate RP.

Example: Configure interface Loopback1 as the candidate RP interface in Global Mode.

```
Switch(config)# ipv6 pim rp-candidate loopback1
```

13.8.4.6 show debugging ipv6 pim

Command: show debugging ipv6 pim

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the current state of the Anycast RP debugging switch.

Example:

```
Switch(config)#show debugging ipv6 pim
Debugging status:
  PIM anycast-rp debugging is on
```

13.8.4.7 show ipv6 pim anycast-rp first-hop

Command: show ipv6 pim anycast-rp first-hop

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays Anycast RP state information, including the multicast routing table (MRT) entries created on the first-hop RP that the protocol currently maintains.

Example:

```
Switch(config)#show ipv6 pim anycast-rp first-hop
IP Multicast Routing Table
(*,G) Entries: 0
(S,G) Entries: 1
(E,G) Entries: 0
INCLUDE (2000:1:111::2, ffle::1)
 Local     .l.............................
```

Output	Description
Entries	Number of entries of each type

INCLUDE	MRT entries created on the first-hop RP

13.8.4.8 show ipv6 pim anycast-rp non-first-hop

Command: `show ipv6 pim anycast-rp non-first-hop`

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays Anycast RP state information, including the MRT entries created on a non-first-hop RP, that is, entries created after the first-hop RP forwarded a received Register message to this RP.

Example:

```
Switch(config)#show ip pim anycast-rp non-first-hop
IP Multicast Routing Table
(*,G) Entries: 0
(S,G) Entries: 1
(E,G) Entries: 0
INCLUDE (2002:1:111::2, ffle::2)
 Local     .l.............................
```

Output	Description
Entries	Number of entries of each type
INCLUDE	MRT entries created on this (non-first-hop) RP

13.8.4.9 show ipv6 pim anycast-rp status

Command: `show ipv6 pim anycast-rp status`

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the Anycast RP configuration: whether Anycast RP is enabled globally, whether the self-rp-address is configured, and the currently configured Anycast RP set.

Example:

```
Switch(config)#show ipv6 pim anycast-rp status
Anycast RP status:
anycast-rp:Enabled!
self-rp-address:2004::2
anycast-rp address: 2000:1:111::2
    other rp unicast rp address: 2002::1
other rp unicast rp address: 2005::1
anycast-rp address: 2003::1
    other rp unicast rp address: 2002::2
 -------------------------------
```

Output	Description
anycast-rp:	Whether Anycast RP is enabled globally
self-rp-address:	The configured self-rp-address
anycast-rp address:	The configured anycast-rp-address
other rp unicast rp address:	The other-RP communication addresses configured for the anycast-rp-address above
other rp unicast rp address:	The other-RP communication addresses configured for the anycast-rp-address above
anycast-rp address:	The configured anycast-rp-address
other rp unicast rp address:	The other-RP communication addresses configured for the anycast-rp-address above

13.8.5 PIM-SSM6

13.8.5.1 ipv6 pim ssm

Command: ipv6 pim ssm {default|range <access-list-name >}
no ipv6 pim ssm

Function: Configures the PIM SSM multicast group range. The **no ipv6 pim ssm** command deletes the configured SSM group range.

Parameters: default: The default PIM SSM group range, ff3x::/32.

<access-list-name>: The name of the access list to apply.

Default: No PIM SSM group range is configured.

Command Mode: Global Mode.

Usage Guidelines: 1. PIM SSM is available only after this command is configured.

2. Before configuring this command, make sure IPv6 PIM multicast routing is enabled.

3. Only access lists created with **ipv6 access-list** can be used.

4. This command can be configured before the corresponding ACL is created, and the ACL can be deleted while it is bound. Once bound, the binding can be released only with **no ipv6 pim ssm**.

5. To use SSM, configure this command on the relevant edge routers, for example on the local switch running MLD (required) and on the multicast source DR or RP (at least one of the two). Intermediate switches need only PIM-SM enabled.

Example: Enable PIM-SSM on the switch with the group range specified by access list 23.

```
Switch (config)#ipv6 pim ssm range 23
Switch(config)#ipv6 access-list standard myfilter
Switch(config_IPv6_Std-Nacl-myfilter)#permit ff1e::/48
```

13.8.6 IPv6 Multicast Source and Destination Control

13.8.6.1 ipv6 access-list(ipv6 multicast source control)

Command: ipv6 access-list <8000-8099> {deny|permit} {{<source/M> }|{host-source <source-host-ip>}|any-source} {{<destination/M> }|{host-destination <destination-host-ip>}|any-destination}
no ipv6 access-list <8000-8099> {deny|permit} {{<source/M>}|{host-source <source-host-ip>}|any-source} {{<destination/M> }|{host-destination <destination-host-ip>}|any-destination}

Function: Configures an IPv6 multicast source control access list. The **no** form of this command deletes the access list.

Parameters: <8000-8099>: The source control access list number.

{deny|permit}: Deny or permit.

<source/M>: The multicast source address and mask length.

<source-host-ip>: The multicast source host address.

<destination/M>: The multicast destination address and mask length.

<destination-host-ip>: The multicast destination host address.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: IPv6 multicast source control entries use ACLs numbered 8000-8099; this command configures such ACLs. The ACL specifies only the source IPv6 addresses and destination (group) IPv6 addresses to control. As with other ACLs, each can be an address range defined by a

mask length, a specific host address, or all addresses. For group addresses, "all addresses" means ff00::/8.

Example:

```
Switch(config)#ipv6 access-list 8000 permit fe80::203:228a/64 ff1e::1/64
```

13.8.6.2 ipv6 access-list(multicast destination control)

Command: ipv6 access-list <9000-10999> {deny|permit} {{<source/M> }| {host-source <source-host-ip>}|any-source} {{<destination/M> }| {host-destination <destination-host-ip>}|any-destination}
no ipv6 access-list <9000-10999> {deny|permit} {{<source/M> }| {host-source <source-host-ip>}|any-source} {{<destination/M> }| {host-destination <destination-host-ip>}|any-destination}

Function: Configures an IPv6 multicast destination control access list. The **no** form of this command deletes the access list.

Parameters: <9000-10999>: The destination control access list number.

{deny|permit}: Deny or permit.

<source/M>: The multicast source address and mask length.

<source-host-ip>: The multicast source host address.

<destination/M>: The multicast destination address and mask length.

<destination-host-ip>: The multicast destination host address.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: IPv6 multicast destination control entries use ACLs numbered 9000-10999; this command configures such ACLs. The ACL specifies only the source IPv6 addresses and destination (group) IPv6 addresses to control. As with other ACLs, each can be an address range defined by a mask length, a specific host address, or all addresses. For group addresses, "all addresses" means ff00::/8.

Example:

```
Switch(config)#ipv6 access-list 9000 permit fe80::203:228a/64 ff1e::1/64
```

13.8.6.3 ipv6 multicast destination-control access-group

Command: ipv6 multicast destination-control access-group <9000-10999>
no ipv6 multicast destination-control access-group <9000-10999>

Function: Configures the IPv6 multicast destination control access list used by the port. The **no** form of this command deletes the configuration.

Parameters: <9000-10999>: The destination control access list number.

Default: Not configured.

Command Mode: Port Mode.

Usage Guidelines: This command takes effect only when multicast destination control is enabled globally. After it is configured, if MLD snooping is enabled, a port joining a multicast group is matched against the configured access list; the port is added only if the match result is permit.

Example:

```
switch(config)#inter ethernet 1/0/4
switch(Config-If-Ethernet1/0/4)#ipv6 multicast destination-control access-
group 9000
switch(Config-If-Ethernet1/0/4)#
```

13.8.6.4 ipv6 multicast destination-control access-group (sip)

Command: ipv6 multicast destination-control <IPADDRESS/M> access-group <9000-10999>
no ipv6 multicast destination-control <IPADDRESS/M> access-group <9000-10999>

Function: Configures the multicast destination control access list used for the specified network segment. The **no** form of this command deletes the configuration.

Parameters: <IPADDRESS/M>: The IP address and mask length.

<9000-10999>: The destination control access list number.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: This command takes effect only when multicast destination control is enabled globally. After it is configured, if MLD snooping or MLD is enabled and an MLD report is received from the specified network segment, the member is matched against the configured access list and is added to the multicast group only if the match result is permit. If the related groups or sources already appear in **show ipv6 mld groups detail** before this command is run, clear them with **clear ipv6 mld group** in Admin Mode.

Example:

```
Switch(config)#ipv6 multicast destination-control 2008::8/64 access-group
9000
```

13.8.6.5 ipv6 multicast destination-control access-group (vmac)

Command: ipv6 multicast destination-control <1-4094> <macaddr> access-group <9000-10999>
no ipv6 multicast destination-control <1-4094> <macaddr> access-group <9000-10999>

Function: Configures the IPv6 multicast destination control access list used for the specified VLAN and MAC address. The **no** form of this command deletes the configuration.

Parameters: <1-4094>: The VLAN ID.

<macaddr>: The source MAC address of the MLD report, in the format xx-xx-xx-xx-xx-xx.

<9000-10999>: The destination control access list number.

Default: Not configured.

Command Mode: Global Mode.

Usage Guidelines: This command takes effect only when multicast destination control is enabled globally. After it is configured, if MLD snooping is enabled, a port joining a multicast group is matched against the configured access list; the port is added only if the match result is permit.

Example:

```
switch(config)#ipv6 multicast destination-control 1 00-01-03-05-07-09 access-
group 9000
```

13.8.6.6 ipv6 multicast policy

Command: ipv6 multicast policy <IPADDRSRC/M> <IPADDRGRP/M> cos <priority>
no ipv6 multicast policy <IPADDRSRC/M> <IPADDRGRP/M> cos

Function: Configures an IPv6 multicast policy. The **no** form of this command removes it.

Parameters: <IPADDRSRC/M>: The IPv6 multicast source address and mask length.

<IPADDRGRP/M>: The IPv6 multicast group address and mask length.

<priority>: The priority, ranging from 0 to 7.

Default: Not configured.

Command Mode: Global Mode.

Usage Guidelines: This command sets the priority of multicast data matched by the switch to the specified value and sets the ToS to the same value. The priority of packets sent untagged is not changed.

Example:

```
Switch(config)#ipv6 multicast policy 2008::1/64 ff1e::3/64 cos 4
```

13.8.6.7 ipv6 multicast source-control

Command: `ipv6 multicast source-control`
`no ipv6 multicast source-control`

Function: Enables IPv6 multicast source control globally. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Source control access lists can be applied to ports only when IPv6 multicast source control is enabled globally. After this command is configured, IPv6 multicast data received on any port is dropped unless it matches a source control entry; only data matched as permit is received and forwarded.

Example:

```
Switch(config)#ipv6 multicast source-control
```

13.8.6.8 ipv6 multicast source-control access-group

Command: `ipv6 multicast source-control access-group <8000-8099>`
`no ipv6 multicast source-control access-group <8000-8099>`

Function: Configures the multicast source control access list used by the port. The **no** form of this command deletes the configuration.

Parameters: <8000-8099>: The source control access list number.

Default: Not configured.

Command Mode: Port Mode.

Usage Guidelines: This command can be configured only when IPv6 multicast source control is enabled globally. After it is configured, all IPv6 multicast packets entering the port are matched against the access list; only packets matched as permit are received and forwarded, and the others are dropped.

Example:

```
switch(config)#inter ethernet 1/0/4
switch(Config-If-Ethernet1/0/4)#ipv6 multicast source-control access-group
8000
```

13.8.6.9 multicast destination-control

Command: `multicast destination-control`
`no multicast destination-control`

Function: Enables IPv4 and IPv6 multicast destination control globally; both take effect at the same time. The **no** form of this command disables them.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: Other destination control configuration takes effect only after multicast destination control is enabled globally; destination access lists can then be applied to ports, VLAN-MAC pairs, and source IP segments. After this command is configured, IGMP snooping, MLD snooping, IGMP, and MLD match against these rules when adding ports after receiving IGMP or MLD reports.

Example:

```
switch(config)# multicast destination-control
```

13.8.6.10 show ipv6 multicast destination-control

Command: show ipv6 multicast destination-control [detail]
show ipv6 multicast destination-control interface <Interfacename> [detail]
show ipv6 multicast destination-control host-address <ipv6addr> [detail]
show ipv6 multicast destination-control <vlan-id> <mac> [detail]

Function: Displays the IPv6 multicast destination control configuration.

Parameters: detail: Displays detailed information.

<Interfacename>: The interface name.

<ipv6addr>: The IPv6 address.

<vlan-id>: The VLAN ID.

<mac>: The MAC address.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays the configured multicast destination control rules; with **detail**, the details of the access lists in use are also displayed.

Example:

```
switch(config)#show ipv6 multicast destination-control
ipv6 multicast destination-control is enabled
ipv6 multicast destination-control 2003::1/64 access-group 9003
ipv6 multicast destination-control 1 00-03-05-07-09-11 access-group 9001
multicast destination-control access-group 6000 used on interface
Ethernet1/0/13
switch(config)#
```

13.8.6.11 show ipv6 multicast destination-control access-list

Command: show ip multicast destination-control access-list
show ip multicast destination-control access-list <9000-10999>

Function: Displays the configured IPv6 multicast destination control access lists.

Parameters: <9000-10999>: The access list number.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays the configured IPv6 multicast destination control access lists.

Example:

```
switch# sh ipv6 multicast destination-control acc
ipv6 access-list 9000 permit 2003::2/64 ff1e::3/64
ipv6 access-list 9000 deny 2008::1/64 ff1e::1/64
ipv6 access-list 9000 permit any-source any-destination
ipv6 access-list 9001 deny any-source host-destination ff1a::1
ipv6 access-list 9001 permit any-source any-destination
```

13.8.6.12 show ipv6 multicast policy

Command: show ipv6 multicast policy

Function: Displays the configured IPv6 multicast policies.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays the configured IPv6 multicast policies.

Example:

```
switch#show ipv6 multicast policy
ipv6 multicast-policy 2003::2/64 ff1e::3/64 cos 5
```

13.8.6.13 show ipv6 multicast source-control

Command: show ipv6 multicast source-control [detail]
show ipv6 multicast source-control interface <Interfacename> [detail]

Function: Displays the IPv6 multicast source control configuration.

Parameters: detail: Displays detailed information.

<Interfacename>: The port name.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays the configured multicast source control rules; with **detail**, the details of the access lists in use are also displayed.

Example:

```
Switch#show ipv6 multicast source-control detail
Ipv6 multicast source-control is enabled
Interface Ethernet 1/0/1 use multicast source control access-list 8000
ipv6 access-list 8000 permit 2003::2/64 ff1e::3/64
ipv6 access-list 8000 deny 2008::1/64 ff1e::1/64
ipv6 access-list 8000 permit any-source any-destination
```

13.8.6.14 show ipv6 multicast source-control access-list

Command: show ipv6 multicast source-control access-list
show ipv6 multicast source-control access-list <8000-8099>

Function: Displays the configured IPv6 multicast source control access lists.

Parameters: <8000-8099>: The access list number.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Displays the configured multicast source control access lists.

Example:

```
switch#sh ipv6 multicast source-control access-list
ipv6 access-list 8000 permit 2003::2/64 ff1e::3/64
ipv6 access-list 8000 deny 2008::1/64 ff1e::1/64
```

13.8.7 MLD

13.8.7.1 clear ipv6 mld group

Command: `clear ipv6 mld group [ X:X::X:X | IFNAME ]`

Function: Deletes the group records of a specific group or interface.

Parameters: X:X::X:X: The group address. **IFNAME**: The interface name.

Command Mode: Admin Mode.

Usage Guidelines: Use the show command to check that the group records are deleted.

Example: Delete all groups.

```
Switch#clear ipv6 mld group
```

Related Commands: show ipv6 mld group

13.8.7.2 debug ipv6 mld events

Command: `debug ipv6 mld events`
`no debug ipv6 mld events`

Function: Enables debugging of MLD events. The **no debug ipv6 mld events** command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Enable this debugging to obtain MLD event information.

Example:

```
Switch# debug ipv6 mld events
Switch#1970/01/01 07:30:13 IMI: MLD Report recv: src fe80::203:fff:fe12:3457
for ff1e::1:3
1970/01/01 07:30:13 IMI: Processing Report comes from Vlan1, ifindex 2003
1970/01/01 07:30:13 IMI: MLD(Querier) ff1e::1:3 (Vlan1): No Listeners -->
Listeners Present
```

13.8.7.3 debug ipv6 mld packet

Command: `debug ipv6 mld packet`
`no debug ipv6 mld packet`

Function: Enables debugging of MLD packets. The **no debug ipv6 mld packet** command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Enable this debugging to obtain MLD packet information.

Example:

```
Switch# deb ipv6 mld packet
Switch#1970/01/01 07:33:12 IMI: Recv MLD packet
1970/01/01 07:33:12 IMI:  Type: Listener Report (131)
1970/01/01 07:33:12 IMI:  Code: 0
1970/01/01 07:33:12 IMI:  Checksum: 3b7a
1970/01/01 07:33:12 IMI:  Max Resp Delay: 0
1970/01/01 07:33:12 IMI:  Reserved: 0
1970/01/01 07:33:12 IMI:  Multicast Address: ff1e::1:3
1970/01/01 07:33:12 IMI: MLD Report recv: src fe80::203:fff:fe12:3457 for
ff1e::1:3
```

```
1970/01/01 07:33:12 IMI: Processing Report comes from Vlan1, ifindex 2003
1970/01/01 07:33:12 IMI: MLD(Querier) ff1e::1:3 (Vlan1): Listeners Present --
> Listeners Present
```

13.8.7.4 ipv6 mld access-group

Command: ipv6 mld access-group {<acl_name>}
no ipv6 mld access-group

Function: Configures access control of MLD groups on the interface. The **no ipv6 mld access-group** command removes the access control.

Parameters: <acl_name> is the name of the IPv6 access list.

Default: No filter is configured.

Command Mode: Interface Mode.

Usage Guidelines: Configures the interface to filter MLD groups, permitting or denying joins to specific groups.

Example: Configure interface VLAN 1 to accept group FF1E::1:0/112 and deny all others.

```
Switch(config)#ipv6 access-list extended aclv6
Switch(config-ipv6-ext-nacl-aclv6)#permit ff1e::1:0/112 any-destination
Switch(config-ipv6-ext-nacl-aclv6)#deny any-source any-destination
Switch (config)#interface vlan 1
Switch(Config-If-Vlan1)#ipv6 mld access-group aclv6
```

13.8.7.5 ipv6 mld immediate-leave

Command: ipv6 mld immediate-leave group-list {<acl-name>}
no ipv6 mld immediate-leave

Function: Configures MLD immediate leave mode: when a host sends a report indicating that it is leaving a group, the router does not send a specific query and considers that the group has no members on the subnet. The **no ipv6 mld immediate-leave** command disables immediate leave mode.

Parameters: <acl-name> is the name of the IPv6 access list.

Default: No immediate leave group is configured.

Command Mode: Interface Mode.

Usage Guidelines: Use this command only when there is only one host on the subnet.

Example: Configure immediate leave mode for the groups in access list aclv6.

```
Switch(Config-if-Vlan1)#ipv6 mld immediate-leave group-list aclv6
```

13.8.7.6 ipv6 mld join-group

Command: ipv6 mld join-group <address>
no ipv6 mld join-group <address>

Function: Configures the interface to join a multicast group. The **no ipv6 mld join-group** command removes the join.

Parameters: <address> is a valid IPv6 multicast address.

Default: No multicast group is joined.

Command Mode: Interface Mode.

Usage Guidelines: The IPv6 multicast address range is FF00::/8; however, FF02::/16 contains permanent addresses that cannot be joined.

Example: Join interface VLAN 2 to multicast group ff1e::1:3.

```
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)#ipv6 mld join-group ff1e::1:3
```

13.8.7.7 ipv6 mld join-group mode source

Command: `ipv6 mld join-group <X:X::X:X> mode <include|exclude> source <.X:X::X:X>`
`no ipv6 mld join-group <X:X::X:X> source <.X:X::X:X>`

Function: Configures the sources of a multicast group that the interface joins. Because a client group has only INCLUDE and EXCLUDE modes, if the specified source mode differs from the current mode, the group mode is changed and the sources configured in the other mode are permanently cleared. The **no** form of this command cancels the join.

Parameters: <X:X::X:X> is a valid IPv6 multicast address.

<include|exclude>: The join mode.

<.X:X::X:X>: The source list; multiple sources can be configured.

Default: No multicast group is joined.

Command Mode: Interface Mode.

Usage Guidelines: The IPv6 multicast address range is FF00::/8; however, FF02::/16 contains permanent addresses that cannot be joined. Sources in the same mode as the existing ones are added; if the mode differs, the existing sources are cleared.

Example:

Join VLAN 2 to multicast group ff1e::1:3 with sources 2003::1 and 2003::2 in INCLUDE mode.

```
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)#ipv6 mld join-group ff1e::1:3 mode include source
2003::1 2003::2
```

13.8.7.8 ipv6 mld last-member-query-interval

Command: `ipv6 mld last-member-query-interval <interval>`
`no ipv6 mld last-member-query-interval`

Function: Configures the interval for sending group-specific queries on the interface. The **no ipv6 mld last-member-query-interval** command restores the default.

Parameters: <interval> is the group-specific query interval, ranging from 1000 to 25500 ms, in multiples of 1000 ms. Other values are converted to a multiple of 1000 ms.

Default: 1000 ms.

Command Mode: Interface Mode.

Example: Set the MLD last member query interval of interface VLAN 1 to 2000 ms.

```
Router(config)#int vlan 1
Router(Config-if-vlan1)#ipv6 mld last-member-query-interval 2000
```

13.8.7.9 ipv6 mld limit

Command: `ipv6 mld limit <state-count>`
`no ipv6 mld limit`

Function: Configures the MLD state limit of the interface. The **no ipv6 mld limit** command restores the default.

Parameters: <state-count>: The maximum number of MLD states maintained by the interface, ranging from 1 to 5000.

Default: 400.

Command Mode: Interface Mode.

Usage Guidelines: When the limit is configured, the number of states saved on the interface cannot exceed it; after the limit is reached, new membership reports are ignored. If MLD group states

already exist when this command is configured, they are removed, and an MLD general query is sent to collect membership reports up to the limit.

Example: Set the MLD state limit of interface VLAN 2 to 4000.

```
Switch(config)#interface vlan2
Switch(Config-if-Vlan2)#ipv6 mld limit 4000
```

13.8.7.10 ipv6 mld query-interval

Command: ipv6 mld query-interval <time_val>
no ipv6 mld query-interval

Function: Configures the interval for sending periodic MLD general queries. The **no ipv6 mld query-interval** command restores the default.

Parameters: <time_val> is the query interval, ranging from 0 to 65535 seconds.

Default: 125 seconds.

Command Mode: Interface Mode.

Usage Guidelines: When a multicast protocol is enabled on an interface, the interface sends MLD general queries periodically. This command configures the query interval.

Example: Set the MLD query interval to 10 seconds.

```
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 mld query-interval 10
```

13.8.7.11 ipv6 mld query-max-response-time

Command: ipv6 mld query-max-response-time <time_val>
no ipv6 mld query- max-response-time

Function: Configures the maximum response time of MLD queries. The **no ipv6 mld query-max-response-time** command restores the default.

Parameters: <time_val> is the maximum response time, ranging from 1 to 8000 seconds.

Default: 10 seconds.

Command Mode: Interface Mode.

Usage Guidelines: When a host receives a query, it starts a timer for each multicast group, with a value between 0 and the maximum response time. When a timer expires, the host sends a membership report for that group. A suitable maximum response time lets hosts respond quickly and lets the router learn group membership quickly.

Example: Set the maximum response time of MLD queries to 20 seconds.

```
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 mld query- max-response-time 20
```

13.8.7.12 ipv6 mld query-timeout

Command: ipv6 mld query-timeout <time_val>
no ipv6 mld query-timeout

Function: Configures the MLD querier timeout of the interface. The **no ipv6 mld query-timeout** command restores the default.

Parameters: <time_val> is the querier timeout, ranging from 60 to 300 seconds.

Default: 255 seconds.

Command Mode: Interface Mode.

Usage Guidelines: On a shared network with several switches running MLD, one switch is elected as the querier, and the others start a timer to monitor it. If no query is received before the timer expires, a new querier is elected.

Example: Set the MLD querier timeout to 100 seconds.

```
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 mld query-timeout 100
```

13.8.7.13 ipv6 mld static-group

Command: `ipv6 mld static-group <group_address> [source <source_address>]`
`no ipv6 mld static-group <group_address> [source <source_address>]`

Function: Configures a static group or static source on the interface. The **no** form of this command removes it.

Parameters: <group_address> is a valid IPv6 multicast address. **<source_address>** is a valid IPv6 unicast address.

Default: No static group or source is configured.

Command Mode: Interface Mode.

Usage Guidelines: The static group address must be within the dynamic multicast address range defined by IPv6. After a static group or source is configured, MLD considers the group or source present whether or not membership reports for it exist on the subnet. The configured static source is the source to be forwarded.

Example: Configure static MLD group ff1e::1:3 on interface VLAN 2.

```
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)#ipv6 mld static-group ff1e::1:3
```

Configure static source 2001::1 for group ff1e::1:3 on interface VLAN 2:

```
Switch(config)#int vlan2
Switch(Config-if-Vlan2)#ipv6 mld static-group ff1e::1:3 source 2001::1
```

13.8.7.14 ipv6 mld version

Command: `ipv6 mld version <version_no>`
`no ipv6 mld version`

Function: Configures the MLD version on the interface. The **no ipv6 mld version** command restores the default.

Parameters: <version_no> is the MLD version, 1 or 2.

Default: 2.

Command Mode: Interface Mode.

Usage Guidelines: If routers on the connected subnet do not support MLDv2, configure the interface with the corresponding version.

Example: Configure the MLD version to 2.

```
Swith(config)#interface vlan 1
Swith(config-if-vlan1)#ipv6 mld version 2
```

13.8.7.15 show ipv6 mld groups

Command: `show ipv6 mld groups [{<ifname | group_addr>}]`

Function: Displays MLD group information.

Parameters: <ifname> is the interface name; group information on that interface is displayed. **<group_addr>** is the group address; information about that group is displayed.

Default: None.

Command Mode: Admin Mode.

Example:

```
Switch#sh ipv6 mld group
```

```
MLD Connected Group Membership
Group Address                           Interface            Uptime
Expires
ff1e::1:3                               Vlan1                00:00:16
00:03:14
Switch#
```

Output	Description
Group Address	Multicast group IPv6 address
Interface	Interface of the multicast group
Uptime	Time the group has existed
Expires	Time remaining before the group times out

13.8.7.16 show ipv6 mld interface

Command: show ipv6 mld interface [<ifname>]

Function: Displays MLD information for an interface.

Parameters: <ifname> is the interface name; MLD information on that interface is displayed.

Default: None.

Command Mode: Admin Mode.

Example: Display the MLD information of interface VLAN 1.

```
Switch#show ipv6 mld interface Vlan1
Interface Vlan1(2003)
 Index 2003
 Internet address is fe80::203:fff:fe01:e4a
 MLD querier
 MLD query interval is 100 seconds
 MLD querier timeout is 205 seconds
 MLD max query response time is 10 seconds
 Last member query response interval is 1000 ms
 Group membership interval is 210 seconds
 MLD is enabled on interface
```

13.8.7.17 show ipv6 mld join-group

Command: show ipv6 mld join-group
show ipv6 mld join-group interface {vlan <vlan_id>|<ifname>}

Function: Displays the groups joined by the interfaces.

Parameters: <ifname> is the interface name; MLD join information on that interface is displayed.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Example: Display the MLD join information of VLAN 2.

```
Switch#show ipv6 mld join-groups vlan 2
Mld join group information:
INTERFACE: Vlan2
HOST VERSION: 2
MULTICAST ADDRESS: ff1e:: 1:3
GROUP STATE: EXCLUDE
SOURCE ADDRESS: 2003::1 mode: EXCLUDE
SOURCE ADDRESS: 2003::2 mode: EXCLUDE
SOURCE ADDRESS: 2003::6 mode: EXCLUDE
SOURCE ADDRESS: 2003::9 mode: EXCLUDE
```

13.8.8 MLD Snooping

13.8.8.1 clear ipv6 mld snooping vlan

Command: `clear ipv6 mld snooping vlan <1-4094> groups [X:X::X:X]`

Function: Deletes the group records of a specific VLAN.

Parameters: <1-4094>: The VLAN ID. **X:X::X:X**: The group address.

Command Mode: Admin Mode.

Usage Guidelines: Use the show command to check that the group records are deleted.

Example: Delete all groups.

```
Switch#clear ipv6 mld snooping vlan 1 groups
```

Related Commands: show ipv6 mld snooping vlan <1-4094>

13.8.8.2 clear ipv6 mld snooping vlan <1-4094> mrouter-port

Command: `clear ipv6 mld snooping vlan <1-4094> mrouter-port [ethernet IFNAME|IFNAME]`

Function: Deletes the mrouter ports of a specific VLAN.

Parameters: <1-4094>: The VLAN ID. **ethernet**: The Ethernet port name. **IFNAME**: The port name.

Command Mode: Admin Mode.

Usage Guidelines: Use the show command to check that the mrouter ports are deleted.

Example: Delete the mrouter port in vlan 1.

```
Switch# clear ipv6 mld snooping vlan 1 mrouter-port
```

Related Commands: show ipv6 mld snooping mrouter-port

13.8.8.3 debug mld snooping all/packet/event/timer/mfc

Command: `debug mld snooping all/packet/event/timer/mfc`
`no debug mld snooping all/packet/event/timer/mfc`

Function: Enables MLD snooping debugging on the switch. The **no** form of this command disables it.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: This command enables MLD snooping debugging, which displays MLD packets processed by the switch (packet), events (event), timers (timer), hardware entries delivered downstream (mfc), or all debugging messages (all).

13.8.8.4 ipv6 mld snooping

Command: `ipv6 mld snooping`
`no ipv6 mld snooping`

Function: Enables MLD snooping on the switch. The **no ipv6 mld snooping** command disables MLD snooping.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: This command enables MLD snooping globally, which allows MLD snooping to be configured on each VLAN. The **no** form of this command disables MLD snooping globally and on all VLANs.

Example: Enable MLD snooping in Global Mode.

```
Switch (config)#ipv6 mld snooping
```

13.8.8.5 ipv6 mld snooping vlan

Command: **`ipv6 mld snooping vlan <vlan-id>`**
`no ipv6 mld snooping vlan <vlan-id>`

Function: Enables MLD snooping on the specified VLAN. The **no** form of this command disables it.

Parameters: **<vlan-id>** is the VLAN ID, ranging from 1 to 4094.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: Global MLD snooping must be enabled before MLD snooping can be configured on a VLAN. Use **no ipv6 mld snooping vlan <vlan-id>** to disable MLD snooping on the VLAN.

Example: Enable MLD snooping on VLAN 100 in Global Mode.

```
Switch (config)#ipv6 mld snooping vlan 100
```

13.8.8.6 ipv6 mld snooping vlan immediately-leave

Command: **`ipv6 mld snooping vlan <vlan-id> immediately-leave`**
`no ipv6 mld snooping vlan <vlan-id> immediately-leave`

Function: Enables MLD immediate leave in the specified VLAN. The **no** form of this command disables it.

Parameters: **<vlan-id>** is the VLAN ID, ranging from 1 to 4094.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: Immediate leave speeds up the removal of a port from a multicast group: no group-specific query is sent, and the port is deleted directly.

Example: Enable MLD immediate leave on VLAN 100.

```
Switch (config)#ipv6 mld snooping vlan 100 immediately-leave
```

13.8.8.7 ipv6 mld snooping vlan l2-general-querier

Command: **`ipv6 mld snooping vlan < vlan-id > l2-general-querier`**
`no ipv6 mld snooping vlan < vlan-id > l2-general-querier`

Function: Configures the VLAN as a Layer 2 general querier.

Parameters: **<vlan-id>** is the VLAN ID, ranging from 1 to 4094.

Command Mode: Global Mode.

Default: The VLAN is not an MLD snooping Layer 2 general querier.

Usage Guidelines: Configuring one Layer 2 general querier per segment is recommended. If MLD snooping is not enabled on the VLAN, this command is not executed. Disabling the Layer 2 general querier does not disable MLD snooping. The main purpose of this command is to send general queries periodically so that switches in the segment can learn mrouter ports.

Note: MLD snooping learns mrouter ports in three ways:

1. Ports that receive MLD query messages
2. Ports that receive multicast protocol packets and support PIM
3. Statically configured ports

Example: Configure VLAN 100 as the Layer 2 general querier.

```
Switch (config)# ipv6 mld snooping vlan 100 l2-general-querier
```

13.8.8.8 ipv6 mld snooping vlan limit

Command: ipv6 mld snooping vlan < vlan-id > limit {group <g_limit> | source <s_limit>}
no ipv6 mld snooping vlan < vlan-id > limit

Function: Configures the maximum number of groups that MLD snooping can join and the maximum number of sources in each group.

Parameters: <vlan-id>: The VLAN ID, ranging from 1 to 4094.

<g_limit>: The maximum number of groups, ranging from 1 to 65535.

<s_limit>: The maximum number of source entries in each group, including include and exclude sources, ranging from 1 to 65535.

Command Mode: Global Mode.

Default: Up to 50 groups, each with up to 40 source entries.

Usage Guidelines: When the number of joined groups reaches the limit, new join requests are rejected to prevent attacks. MLD snooping must be enabled on the VLAN to use this command. The **no** form of this command restores the default rather than removing the limit; for security, no-limit cannot be configured. The default is recommended. If Layer 3 MLD is running, keep this setting consistent with the MLD configuration where possible.

Example: Limit the number of groups in VLAN 2 to 300.

```
Switch(config)#ipv6 mld snooping vlan 2 limit group 300
```

13.8.8.9 ipv6 mld snooping vlan mrouter-port interface

Command: ipv6 mld snooping vlan <vlan-id> mrouter-port interface [<ethernet>|<port-channel>] <ifname>
no ipv6 mld snooping vlan <vlan-id> mrouter-port interface [<ethernet>|<port-channel>] <ifname>

Function: Configures a static mrouter port of the VLAN. The **no** form of this command removes it.

Parameters: <vlan-id>: The VLAN ID, ranging from 1 to 4094.

ethernet: Ethernet port.

<ifname>: The interface name.

port-channel: Port aggregation group.

Command Mode: Global Mode.

Default: None. If a port is both a static and a dynamic mrouter port, the static property takes precedence. A static mrouter port can be deleted only with the **no** form of this command.

Example: Configure Ethernet 1/0/13 as a static mrouter port of VLAN 2.

```
Switch(config)#ipv6 mld snooping vlan 2 mrouter-port interface ethernet1/0/13
```

13.8.8.10 ipv6 mld snooping vlan mrouter-port learnpim6

Command: ipv6 mld snooping vlan <vlan-id> mrouter-port learnpim6
no ipv6 mld snooping vlan <vlan-id> mrouter-port learnpim6

Function: Enables the specified VLAN to learn mrouter ports from PIMv6 packets. The **no** form of this command disables it.

Parameters: <vlan-id>: The VLAN ID, ranging from 1 to 4094.

Command Mode: Global Mode.

Default: Enabled.

Usage Guidelines: When enabled, a port that receives PIMv6 packets is automatically set as an mrouter port.

Example: Disable mrouter port learning from PIMv6 packets in VLAN 100.

```
Switch(config)#no ipv6 mld snooping vlan 100 mrouter-port learnpim6
```

13.8.8.11 ipv6 mld snooping vlan mrpt

Command: ipv6 mld snooping vlan <vlan-id> mrpt <value>
no ipv6 mld snooping vlan <vlan-id> mrpt

Function: Configures the keepalive time of mrouter ports.

Parameters: <vlan-id>: The VLAN ID, ranging from 1 to 4094.

<value>: The mrouter port keepalive time, ranging from 1 to 65535 seconds.

Command Mode: Global Mode.

Default: 255 seconds.

Usage Guidelines: This setting applies to dynamic mrouter ports, not static ones. MLD snooping must be enabled on the VLAN to use this command.

Example: Set the mrouter port keepalive time of VLAN 2 to 100 seconds.

```
Switch(config)#ipv6 mld snooping vlan 2 mrpt 100
```

13.8.8.12 ipv6 mld snooping vlan query-interval

Command: ipv6 mld snooping vlan <vlan-id> query-interval <value>
no ipv6 mld snooping vlan <vlan-id> query-interval

Function: Configures the query interval.

Parameters: <vlan-id>: The VLAN ID, ranging from 1 to 4094.

<value>: The query interval, ranging from 1 to 65535 seconds.

Command Mode: Global Mode.

Default: 125 seconds.

Usage Guidelines: The default is recommended. If Layer 3 MLD is running, keep this setting consistent with the MLD configuration where possible.

Example:

```
Switch(config)#ipv6 mld snooping vlan 2 query-interval 130
```

13.8.8.13 ipv6 mld snooping vlan query-mrsp

Command: ipv6 mld snooping vlan <vlan-id> query-mrsp <value>
no ipv6 mld snooping vlan <vlan-id> query-mrsp

Function: Configures the maximum query response time. The **no** form of this command restores the default.

Parameters: <vlan-id>: The VLAN ID, ranging from 1 to 4094.

<value>: The maximum response time, ranging from 1 to 25 seconds.

Command Mode: Global Mode.

Default: 10 seconds.

Usage Guidelines: The default is recommended. If Layer 3 MLD is running, keep this setting consistent with the MLD configuration where possible.

Example:

```
Switch(config)#ipv6 mld snooping vlan 2 query-mrsp 18
```

13.8.8.14 ipv6 mld snooping vlan query-robustness

Command: ipv6 mld snooping vlan <vlan-id> query-robustness <value>
no ipv6 mld snooping vlan <vlan-id> query-robustness

Function: Configures the query robustness variable. The **no** form of this command restores the default.

Parameters: <vlan-id>: The VLAN ID, ranging from 1 to 4094.

<value>: The robustness variable, ranging from 2 to 10.

Command Mode: Global Mode.

Default: 2.

Usage Guidelines: The default is recommended. If Layer 3 MLD is running, keep this setting consistent with the MLD configuration where possible.

Example:

```
Switch(config)#ipv6 mld snooping vlan 2 query- robustness 3
```

13.8.8.15 ipv6 mld snooping vlan static-group

Command: ipv6 mld snooping vlan<vlan-id> static-group <X:X::X:X> [source< X:X::X:X>] interface [ethernet | port-channel] <IFNAME>
no ipv6 mld snooping vlan <vlan-id> static-group <X:X::X:X> [source< X:X::X:X>] interface [ethernet | port-channel] <IFNAME>

Function: Configures a static group on the specified port of the VLAN. The **no** form of this command removes it.

Parameters: <vlan-id>: The VLAN ID, ranging from 1 to 4094.

X:X::X:X: The group or source address.

ethernet: Ethernet port.

port-channel: Port aggregation group.

<IFNAME>: The interface name.

Command Mode: Global Mode.

Default: None.

Usage Guidelines: If a group is both static and dynamic, it is treated as a static group. A static group can be deleted only with the **no** form of this command.

Example:

```
Switch(config)#ip igmp snooping vlan 1 static-group ff1e::15 source 2000::1
interface ethernet 1/0/1
```

13.8.8.16 ipv6 mld snooping vlan suppression-query-time

Command: ipv6 mld snooping vlan <vlan-id> suppression-query-time <value>
no ipv6 mld snooping vlan <vlan-id> suppression-query-time

Function: Configures the query suppression time. The **no** form of this command restores the default.

Parameters: <vlan-id>: The VLAN ID, ranging from 1 to 4094.

<value>: The suppression time, ranging from 1 to 65535 seconds.

Command Mode: Global Mode.

Default: 255 seconds.

Usage Guidelines: This command can be configured only on a Layer 2 general querier. The suppression query time is the period during which the general querier stays suppressed after receiving queries from Layer 3 MLD in the segment. The query intervals of all switches in the same segment must be consistent. The default is recommended.

Example:

```
Switch(config)#ipv6 mld snooping vlan 2 suppression-query-time 270
```

13.8.8.17 show ipv6 mld snooping

Command: show ipv6 mld snooping [vlan <vlan-id>]

Function: Displays MLD snooping information.

Parameters: <vlan-id> is the VLAN whose MLD snooping information is displayed.

Command Mode: Admin Mode.

Usage Guidelines: Without a VLAN ID, the command shows whether global MLD snooping is enabled, whether a Layer 3 multicast protocol is running, and on which VLANs MLD snooping and the Layer 2 general querier are enabled. With a VLAN ID, detailed MLD snooping information for that VLAN is displayed.

Example:

1. Summary of MLD snooping on the switch:

```
Switch(config)#show ipv6 mld snooping
Global mld snooping status:  Enabled
L3 multicasting:             running
Mld snooping is turned on for vlan 1(querier)
Mld snooping is turned on for vlan 2
--------------------------------
```

Output	Description
Global mld snooping status	Whether global MLD snooping is enabled on the switch
L3 multicasting	Whether a Layer 3 multicast protocol is running on the switch
Mld snooping is turned on for vlan 1(querier)	VLANs on which MLD snooping is enabled, and whether each is a Layer 2 general querier

2. Detailed MLD snooping information for VLAN 1:

```
Switch#show ipv6 mld snooping vlan 1
Mld snooping information for vlan 1
Mld snooping L2 general querier                    :Yes(COULD_QUERY)
Mld snooping query-interval                        :125(s)
Mld snooping max reponse time                     :10(s)
Mld snooping robustness                           :2
Mld snooping mrouter port keep-alive time            :255(s)
Mld snooping query-suppression time                :255(s)
MLD Snooping Connect Group Membership
```

Note: * = all sources; (S) = include source; [S] = exclude source

```
Groups        Sources          Ports            Exptime  System Level
Ff1e::15       (2000::1)       Ethernet1/0/8         00:04:14     V2
              (2000::2)       Ethernet1/0/8         00:04:14     V2
Mld snooping vlan 1 mrouter port
```

Note: "!" = static mrouter port

```
!Ethernet1/0/2
```

Output	Description
Mld snooping L2 general querier	Whether the VLAN is a Layer 2 general querier; the querier status is COULD_QUERY or SUPPRESSED
Mld snooping query-interval	Query interval of the VLAN
Mld snooping max reponse time	Maximum response time of the VLAN
Mld snooping robustness	Robustness variable configured on the VLAN
Mld snooping mrouter port keep-alive time	Keepalive time of dynamic mrouter ports on the VLAN
Mld snooping query-suppression	Suppression time of the VLAN as a Layer 2 general

time	querier in the suppressed state
MLD Snooping Connect Group Membership	Group membership of the VLAN, that is, the mapping between ports and (S,G)
Mld snooping vlan 1 mrouter port	Mrouter ports of the VLAN, both static and dynamic

13.9 IPv6 Security RA

13.9.1 ipv6 security-ra enable

Command: `ipv6 security-ra enable`
`no ipv6 security-ra enable`

Function: Enables IPv6 security RA globally. RA messages are then not forwarded by hardware but sent to the CPU for processing. The **no** form of this command disables IPv6 security RA globally.

Parameters: None.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: Security RA can be enabled on a port only after it is enabled globally. Disabling security RA globally clears all configured security RA ports. Global security RA and global IPv6 SAVI are mutually exclusive and cannot be enabled at the same time.

Example: Globally enable IPv6 security RA.

```
Switch(config)#ipv6 security-ra enable
```

13.9.2 ipv6 security-ra enable

Command: `ipv6 security-ra enable`
`no ipv6 security-ra enable`

Function: Enables IPv6 security RA on a port so that the port does not forward received RA messages. The **no ipv6 security-ra enable** command disables IPv6 security RA on the port.

Parameters: None.

Command Mode: Port Mode.

Default: Disabled.

Usage Guidelines: Security RA can be enabled on a port only after it is enabled globally. Disabling security RA globally clears all configured security RA ports.

Example: Enable IPv6 security RA on a port.

```
Switch(Config-If-Ethernet1/0/2)#ipv6 security-ra enable
```

13.9.3 show ipv6 security-ra

Command: `show ipv6 security-ra [interface <interface-list>]`

Function: Displays the interfaces on which IPv6 security RA is enabled.

Parameters: Without a parameter, all untrusted ports are displayed; with **interface <interface-list>**, the specified untrusted ports are displayed.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch# show ipv6 security-ra
IPv6 security ra config and state information in the switch
Global IPv6 Security RA State: Enable
Ethernet1/0/1
IPv6 Security RA State: Yes
```

```
Ethernet1/0/3
IPv6 Security RA State: Yes
```

13.9.4 debug ipv6 security-ra

Command: `debug ipv6 security-ra`
`no debug ipv6 security-ra`

Function: Enables IPv6 security RA debugging. The **no** form of this command disables it.

Command Mode: Admin Mode.

Parameters: None.

Usage Guidelines: Use this command to follow how IPv6 security RA handles messages, which helps troubleshoot problems.

Example: Enable IPv6 security RA debugging.

```
Switch#debug ipv security-ra
```

13.10 SAVI

13.10.1 Commands for SAVI

13.10.1.1 ipv6 cps prefix

Command: `ipv6 cps prefix <ipv6-address> vlan <vid>`
`no ipv6 cps prefix<ipv6-address>`

Function: Configures the IPv6 address prefix of a link manually. The **no** form of this command deletes the prefix.

Parameters: <ipv6-address>: The address prefix of the link, for example 2001::/64.

<vid>: The VLAN ID of the link.

Command Mode: Global Mode.

Default: None.

Usage Guidelines: Before enabling link prefix matching, configure the link-local prefix fe80::/64 so that packets with link-local source addresses are accepted.

Example: Configure the link address prefix 2001::/64.

```
Switch(config)#ipv6 cps prefix 2001::/64 vlan 2
```

13.10.1.2 ipv6 cps prefix check enable

Command: `ipv6 cps prefix check enable`
`no ipv6 cps prefix check enable`

Function: Enables SAVI address prefix checking. The **no** form of this command disables it.

Parameters: None.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: When prefix checking is enabled, no IPv6 address binding is created for packets whose address prefix does not match the link prefix. If link prefix matching is enabled, first configure the link-local prefix fe80::/64 so that packets with link-local source addresses are accepted.

Example: Enable SAVI address prefix checking.

```
Switch(config)#ipv6 cps prefix check enable
```

13.10.1.3 ipv6 dhcp snooping trust

Command: `ipv6 dhcp snooping trust`
`no ipv6 dhcp snooping trust`

Function: Configures the port as a DHCPv6 trusted port; dynamic DHCPv6 bindings are no longer created on it, and all DHCPv6 protocol packets are allowed. The **no** form of this command removes the trusted setting.

Parameters: None.

Command Mode: Port Mode.

Default: Disabled.

Usage Guidelines: Configure the DHCPv6 trusted attribute on the uplink port of a SAVI-enabled switch, typically the port connected to the DHCPv6 server or DHCPv6 relay.

Example: Configure Ethernet 1/0/1 as a DHCPv6 trusted port.

```
Switch(config)#interface ethernet1/0/1
Switch(config-if-ethernet1/0/1)#ipv6 dhcp snooping trust
```

13.10.1.4 ipv6 nd snooping trust

Command: `ipv6 nd snooping trust`
`no ipv6 nd snooping trust`

Function: Configures the port as a SLAAC-trusted and RA-trusted port; dynamic SLAAC bindings are no longer created on it, and RA packets are forwarded. The **no** form of this command removes the trusted setting.

Parameters: None.

Command Mode: Port Mode.

Default: Disabled.

Usage Guidelines: If the trusted setting is disabled, the port is an RA-untrusted port and discards all RA packets. Configure the trusted attribute on the uplink port of a SAVI-enabled switch, or on ports interconnecting SAVI-enabled switches.

Example: Configure Ethernet 1/0/1 as an ND trusted port.

```
Switch(config)#interface ethernet1/0/1
Switch(config-if-etherne1/0/1)#ipv6 nd snooping trust
```

13.10.1.5 savi check binding

Command: `savi check binding <simple | probe> mode`
`no savi check binding mode`

Function: Configures the check mode for conflicting bindings. The **no** form of this command deletes the check mode.

Parameters: simple mode: Checks only the port state of the conflicting binding. If the port is up, the conflicting binding is kept and no new binding is created; if the port is down, the conflicting binding is deleted and a new one is created.

probe mode: In addition to checking the port state, sends NS packets to probe the user of the binding when the port is up. If NA responses are received, the existing binding is kept and no new binding is created; otherwise, the existing binding is deleted and a new one is created.

Command Mode: Global Mode.

Default: No check mode is configured; conflicting bindings are deleted directly and new ones are created.

Usage Guidelines: Probe mode is recommended to prevent spoofed address conflicts from deleting legitimate user bindings.

Example: Set the conflicting binding check mode to probe.

```
Switch(config)#savi check binding probe mode
```

13.10.1.6 savi enable

Command: **savi enable**
no savi enable

Function: Enables SAVI globally. The **no** form of this command disables it.

Parameters: None.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: Other SAVI commands can be configured only after SAVI is enabled globally. Because SAVI includes the security RA function, global SAVI and global security RA are mutually exclusive.

Example: Enable SAVI.

```
Switch(config)#savi enable
```

13.10.1.7 savi ipv6 binding num

Command: **savi ipv6 binding num <limit-num>**
no savi ipv6 binding num

Function: Configures the maximum number of bindings on the port. The **no** form of this command restores the default.

Parameters: <limit-num>: The maximum number of bindings, ranging from 0 to 65535. The default is 65535.

Command Mode: Port Mode.

Default: 65535.

Usage Guidelines: The limit applies only to dynamic SLAAC and DHCP bindings. When the number of bindings reaches the limit, no new dynamic bindings are created on the port; if the limit is 0, no dynamic bindings are created.

Example: Set the maximum number of bindings on Ethernet 1/0/1 to 100.

```
Switch(config)#interface ethernet1/0/1
Switch(config-if-ethernet1/0/1)# savi ipv6 binding num 100
```

13.10.1.8 savi ipv6 check source binding

Command: **savi ipv6 check source binding ip <ip-address> mac <mac-address> interface <if-name> {type [slaac | dhcp] lifetime <lifetime> | type static}**
no savi ipv6 check source binding ip <ip-address> interface <if-name>

Function: Configures a static or dynamic binding manually. The **no** form of this command deletes the binding.

Parameters: <ip-address>: A unicast IPv6 address, link-local or global unicast.

<mac-address>: The Ethernet MAC address.

<if-name>: The port name, for example ethernet 1/0/1.

slaac | dhcp: Creates a dynamic binding of SLAAC or DHCP type.

<lifetime>: The lifetime of the dynamic binding, in seconds.

static: Creates a static binding.

Command Mode: Global Mode.

Default: None.

Usage Guidelines: When a manually configured dynamic binding expires, the binding is deleted but the configuration is kept, so the binding is still displayed. To reactivate the binding, delete it and configure it again.

For a static binding, no lifetime is configured; the lifetime is infinite.

Example: Configure a SLAAC-type dynamic SAVI binding manually.

```
Switch(config)#savi ipv6 check source binding ip 2001::10 mac 00-25-64-BB-8F-
04 Interface ethernet1/0/1 type slaac lifetime 2010
```

Configure a static SAVI binding manually:

```
Switch(config)#savi ipv6 check source binding ip 2001::20 mac 00-25-64-BB-8F-
04
Interface ethernet1/0/1 type static
```

13.10.1.9 savi ipv6 check source ip-address mac-address

Command: savi ipv6 check source [ip-address mac-address | ip-address | mac-address]

no savi ipv6 check source

Function: Enables source checking of packets on the port. The **no** form of this command disables it.

Parameters: ip-address mac-address, **ip-address**, or **mac-address**: The fields checked.

Command Mode: Port Mode.

Default: Disabled.

Usage Guidelines: Global SAVI must be enabled before this command is configured.

Example: Enable source checking of packets on Ethernet 1/0/1.

```
Switch(config)#interface ethernet1/0/1
Switch(config-if-ethernet1/0/1)# savi ipv6 check source ip-address mac-
address
```

13.10.1.10 savi ipv6 {dhcp-only | slaac-only | dhcp-slaac} enable

Command: savi ipv6 {dhcp-only | slaac-only | dhcp-slaac} enable

no savi ipv6 {dhcp-only | slaac-only | dhcp-slaac} enable

Function: Enables a SAVI application scenario. The **no** form of this command disables it.

Parameters: dhcp-only: DHCP-only scenario.

slaac-only: SLAAC-only scenario.

dhcp-slaac: Combined DHCP and SLAAC scenario.

Command Mode: Global Mode.

Default: Disabled.

Usage Guidelines: In the dhcp-only scenario, SAVI checks DHCPv6 packets and DAD NS packets whose target is a link-local IPv6 address; DAD NS packets for non-link-local addresses are not checked. In the slaac-only scenario, DAD NS packets of all types are checked. In the dhcp-slaac scenario, all DHCPv6 and DAD NS packets are checked.

Example: Enable the dhcp-only SAVI scenario.

```
Switch(config)#savi ipv6 dhcp-only enable
```

13.10.1.11 savi ipv6 mac-binding-limit

Command: savi ipv6 mac-binding-limit <limit-num>
no savi ipv6 mac-binding-limit

Function: Configures the maximum number of dynamic bindings for the same MAC address. The **no** form of this command restores the default.

Parameters: <limit-num>: The maximum number, ranging from 1 to 10. The default is 32.

Command Mode: Global Mode.

Default: 32.

Usage Guidelines: This command prevents attacks that exhaust SAVI dynamic binding entries.

Example: Set the maximum number of dynamic bindings for the same MAC address to 5.

```
Switch(config)#isavi ipv6 mac-binding-limit 5
```

13.10.1.12 savi max-dad-delay

Command: savi max-dad-delay <max-dad-delay>
no savi max-dad-delay

Function: Configures how long a dynamic binding stays in the DETECTION state while DAD NS detection is performed. The **no** form of this command restores the default.

Parameters: <max-dad-delay>: The time, ranging from 1 to 65535 seconds. The default is 1 second.

Command Mode: Global Mode.

Default: 1 second.

Usage Guidelines: The default is recommended.

Example: Set the detection time to 2 seconds.

```
Switch(config)#savi max-dad-delay 2
```

13.10.1.13 savi max-dad-prepare-delay

Command: savi max-dad-prepare-delay <max-dad-prepare-delay>
no savi max-dad-prepare-delay

Function: Configures the redetection time of dynamic bindings. The **no** form of this command restores the default.

Parameters: <max-dad-prepare-delay>: The time, ranging from 1 to 65535 seconds. The default is 1 second.

Command Mode: Global Mode.

Default: 1 second.

Usage Guidelines: The default is recommended.

Example: Set the redetection time to 2 seconds.

```
Switch(config)#savi max-dad-prepare-delay 2
```

13.10.1.14 savi max-slaac-life

Command: savi max-slaac-life <max-slaac-life>
no savi max-slaac-life

Function: Configures the lifetime of SLAAC dynamic bindings in the BOUND state. The **no** form of this command restores the default.

Parameters: <max-slaac-life>: The lifetime, ranging from 1 to 31536000 seconds. The default is 4 hours.

Command Mode: Global Mode.

Default: 4 hours.

Usage Guidelines: None.

Example: Set the lifetime of SLAAC bindings in the BOUND state to 2010 seconds.

```
Switch(config)#savi max-slaac-life 2010
```

13.10.1.15 savi timeout bind-protect

Command: savi timeout bind-protect <protect-time>
no savi timeout bind-protect

Function: Configures the binding protection time for a port after it goes from up to down. The **no** form of this command restores the default.

Parameters: <protect-time>: The protection time, ranging from 1 to 300 seconds. The default is 30 seconds.

Command Mode: Global Mode.

Default: 30 seconds.

Usage Guidelines: If the port is still down when the protection time expires, its bindings are deleted. If the port comes up during the protection time, the bindings return to the lifetime of the BOUND state. If the configured value is 0 seconds, all bindings of the port are deleted immediately.

Example: Set the binding protection time to 20 seconds.

```
Switch(config)#savi timeout bind-protect 20
```

13.10.2 Commands for Monitor and Debug

13.10.2.1 Monitor and Debug

13.10.2.1.1 debug ipv6 dhcp snooping binding

Command: debug ipv6 dhcp snooping binding
no debug ipv6 dhcp snooping binding

Function: Enables debugging of DHCP-type SAVI bindings. The **no** form of this command disables it.

Parameters: None.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: When enabled, debugging information is printed for DHCP-type and static bindings, for troubleshooting.

Example: Enable debugging of DHCP-type bindings.

```
Switch#debug ipv6 dhcp snooping binding
```

13.10.2.1.2 debug ipv6 dhcp snooping event

Command: debug ipv6 dhcp snooping event
no debug ipv6 dhcp snooping event

Function: Enables debugging of DHCP-type SAVI events. The **no** form of this command disables it.

Parameters: None.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: When enabled, DHCP-type event information is printed for troubleshooting.

Example: Enable debugging of DHCP-type events.

```
Switch#debug ipv6 dhcp snooping event
```

13.10.2.1.3 debug ipv6 dhcp snooping packet

Command: **`debug ipv6 dhcp snooping packet`**
`no debug ipv6 dhcp snooping packet`

Function: Enables debugging of DHCPv6 packets. The **no** form of this command disables it.

Parameters: None.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: When enabled, the related DHCPv6 packets are printed for troubleshooting.

Example: Enable debugging of DHCPv6 packets.

```
Switch#debug ipv6 dhcp snooping packet
```

13.10.2.1.4 debug ipv6 nd snooping binding

Command: **`debug ipv6 nd snooping binding`**
`no debug ipv6 nd snooping binding`

Function: Enables debugging of SLAAC-type SAVI bindings. The **no** form of this command disables it.

Parameters: None.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: When enabled, debugging information is printed for SLAAC-type bindings, for troubleshooting.

Example: Enable debugging of SLAAC-type bindings.

```
Switch#debug ipv6 nd snooping binding
```

13.10.2.1.5 debug ipv6 nd snooping event

Command: **`debug ipv6 nd snooping event`**
`no debug ipv6 nd snooping event`

Function: Enables debugging of SLAAC-type SAVI events. The **no** form of this command disables it.

Parameters: None.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: When enabled, SLAAC-type event information is printed for troubleshooting.

Example: Enable debugging of SLAAC-type events.

```
Switch#debug ipv6 nd snooping event
```

13.10.2.1.6 debug ipv6 nd snooping packet

Command: **`debug ipv6 nd snooping packet`**
`no debug ipv6 nd snooping packet`

Function: Enables debugging of ND packets. The **no** form of this command disables it.

Parameters: None.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guidelines: When enabled, the related ND packets are printed for troubleshooting.

Example: Enable debugging of ND packets.

```
Switch#debug ipv6 nd snooping packet
```

13.10.2.1.7 show savi ipv6 check source binding

Command: show savi ipv6 check source binding [interface<if-name>]

Function: Displays the global SAVI binding table.

Parameters: <if-name>: The port name, for example ethernet 1/0/1.

Command Mode: Admin Mode.

Default: None.

Usage Guidelines: The fields are described below:

Field	Description
MAC	The bound MAC address
IP	The bound IP address
Vlan	VLAN to which the binding belongs
Port	Port to which the binding belongs
Type	Binding type
State	Binding state
Expires	Remaining lifetime of the binding

Example: Display the global SAVI binding status.

```
Switch(config)#show savi ipv6 check source binding
Static binding count: 0
Dynamic binding count: 3
Binding count: 3
MAC         IP        VLAN  Port         Type    State     Expires
------------------------------------------------------------------------------
--------------------------------
00-25-64-bb-8f-04  fe80::225:64ff:febb:8f04  1 Ethernet1/0/5 slaac  BOUND
14370
00-25-64-bb-8f-04  2001::13   1    Ethernet1/0/5  slaac   BOUND     14370
00-25-64-bb-8f-04  2001::10   1    Ethernet1/0/5  slaac   BOUND     14370
------------------------------------------------------------------------------
--------------------------------
```

13.11 IPv6 VRRPv3

13.11.1 advertisement-interval

Command: advertisement-interval <adver_interval>

Function: Configures the VRRPv3 advertisement interval.

Parameters: <adver_interval> is the interval for sending VRRPv3 advertisements, in centiseconds, ranging from 100 to 1000 in multiples of 100.

Command Mode: VRRPv3 Mode.

Default: 100 centiseconds (1 second).

Usage Guidelines: The master of a VRRPv3 backup group periodically sends VRRPv3 advertisements to notify the other routers (Layer 3 switches) in the group that it is working normally; the interval is **adver_interval**. If a backup receives no advertisement from the master within **master_down_interval**, it considers the master failed and changes its own state to master.

Use this command to adjust the interval of advertisements sent by the master. All members of the same backup group should use the same value. On a backup, **master_down_interval** should be more than three times **adver_interval**. If traffic is heavy or the routers (Layer 3 switches) use different timers, **master_down_interval** may expire and cause a state change; to avoid this, increase **adver_interval** or set a longer preemption delay.

Example: Set the VRRPv3 advertisement interval to 300 centiseconds.

```
Switch(config-router)# advertisement-interval 300
```

13.11.2 circuit-failover

Command: `circuit-failover {vlan<ID>| IFNAME} <value_reduced>`
`no circuit-failover`

Function: Configures the VRRPv3 monitored interface.

Parameters: {vlan<ID>| IFNAME} is the interface to monitor.

<value_reduced> is the amount by which the priority is decreased, ranging from 1 to 253.

Command Mode: VRRPv3 Mode.

Default: Not configured.

Usage Guidelines: Interface monitoring extends the backup function: VRRPv3 not only provides backup when a router (or Layer 3 switch) fails, but also lowers the priority of a router (or Layer 3 switch) when a monitored interface goes down, so that backup takes over smoothly.

When this command is used and a monitored interface goes from up to down, the priority of the router (or Layer 3 switch) in its backup group is decreased (if value_reduced exceeds the configured priority, the priority is decreased to 0), so that a backup is not prevented from taking over because its priority is lower than that of the failed master. When the monitored interface comes up again, the priority of the router (or Layer 3 switch) is restored.

Example: Configure VLAN 2 as the VRRPv3 monitored interface with a priority decrease of 10.

```
Switch(Config-router)# circuit-failover vlan 2 10
```

13.11.3 debug ipv6 vrrp

Command: `debug ipv6 vrrp [all | events | packet [recv | send]]`
`no debug ipv6 vrrp [all | events | packet [recv | send]]`

Function: Displays VRRPv3 backup group state changes and the messages sent and received. The **no** form of this command disables the debugging display.

Parameters: all, **events**, or **packet [recv | send]**: The debugging type.

Command Mode: Admin Mode.

Example:

```
Switch#debug ipv6 vrrp
Jan 01 01:03:13 2006 NSM: VRRP6 SEND[Hello]: Advertisement sent for vrid=[1],
virtual-ip=[fe80::2]
Jan 01 01:03:14 2006 NSM: VRRP6 SEND[Hello]: Advertisement sent for vrid=[1],
virtual-ip=[fe80::2]
Jan 01 01:03:15 2006 NSM: VRRP6 SEND[Hello]: Advertisement sent for vrid=[1],
virtual-ip=[fe80::2]
```

13.11.4 disable

Command: `disable`

Function: Disables the VRRPv3 virtual router.

Parameters: None.

Command Mode: VRRPv3 Mode.

Default: None.

Usage Guidelines: Disables the virtual router session. The configuration parameters can be changed only after the virtual router is disabled.

Example: Disable VRRPv3 virtual router 10.

```
Switch(config)#router ipv6 vrrp 10
Switch(config-router)#disable
```

13.11.5 enable

Command: `enable`

Function: Enables the VRRPv3 virtual router.

Parameters: None.

Command Mode: VRRPv3 Mode.

Default: None.

Usage Guidelines: Starts the virtual router session. Only interfaces of an enabled router (or Layer 3 switch) actually join the backup group. Configure the virtual IPv6 address and interface of VRRPv3 before enabling the virtual router.

Example: Enable VRRPv3 virtual router 10.

```
Switch(config)#router ipv6 vrrp 10
Switch(config-router)#enable
```

13.11.6 preempt-mode

Command: `preempt-mode {true | false}`

Function: Configures the VRRPv3 preemption mode.

Parameters: true: Preemption mode. **false**: Non-preemption mode.

Command Mode: VRRPv3 Mode.

Default: Preemption mode.

Usage Guidelines: Configure preemption mode if a router (or Layer 3 switch) with a higher priority should take over the master role.

Example: Configure VRRPv3 non-preemption mode.

```
Switch(config-router)# preempt-mode false
```

13.11.7 priority

Command: `priority <value>`

Function: Configures the VRRPv3 priority.

Parameters: <value> is the priority, ranging from 1 to 254.

Command Mode: VRRPv3 Mode.

Default: The priority of backup routers (or Layer 3 switches) is 100; the priority of the IP address owner is 255.

Usage Guidelines: The priority determines the state of a router (or Layer 3 switch) in the backup group; the higher the priority, the more likely it is to become master. The configurable range is 1 to 254; 255 is reserved for the IP address owner. Priority 0 has a special use: when a VRRP session is disabled, the master sends an advertisement with priority 0, and a backup that receives it starts a

new master election. If two or more routers (or Layer 3 switches) in a backup group have the same priority, the one with the highest link-local IPv6 address takes precedence.

Example: Set the VRRPv3 priority to 150.

```
Switch(config-router)# priority 150
```

13.11.8 router ipv6 vrrp

Command: `router ipv6 vrrp <vrid>`
`no router ipv6 vrrp <vrid>`

Function: Creates or deletes a VRRPv3 virtual router.

Parameters: <vrid> is the virtual router ID, ranging from 1 to 255.

Command Mode: Global Mode.

Default: None.

Usage Guidelines: A virtual router is uniquely identified by its ID and virtual IPv6 address. It must be created before it can be configured. For stability, configure no more than 64 virtual routers.

Example: Create virtual router 10.

```
Switch(config)# router ipv6 vrrp 10
```

13.11.9 show ipv6 vrrp

Command: `show ipv6 vrrp [<vrid>]`

Function: Displays the state and configuration of VRRPv3 backup groups.

Parameters: <vrid> is the virtual router ID, ranging from 1 to 255. Without it, the state and configuration of all backup groups are displayed.

Command Mode: Admin Mode and Configuration Mode.

Example:

```
Switch# show ipv6 vrrp
VrId 1
 State is Master
 Virtual IPv6 is fe80::2 (Not IPv6 owner)
 Interface is Vlan1
 Configured priority is 150, Current priority is 150
 Advertisement interval is 100 centisec
 Preempt mode is TRUE
 Circuit failover interface Vlan1, Priority Delta 3, Status UP
VrId 10
 State is Initialize
 Virtual IPv6 is fe80::3 (Not IPv6 owner)
 Interface is Vlan2
 Priority is 100
 Advertisement interval is 300 centisec
 Preempt mode is TRUE
Circuit failover interface Vlan2, Priority Delta 10, Status UP
```

Output	Description
State	State
Virtual IPv6	Virtual IPv6 address
Interface	Interface name
Priority	Priority
Advertisement interval	Interval of VRRPv3 advertisements
Preempt	Preemption mode
Circuit failover interface	Monitored interface information

13.11.10 virtual-ipv6 interface

Command: `virtual-ipv6 <ipv6-address> interface {Vlan <ID>| IFNAME}`
`no virtual-ipv6 interface`

Function: Configures the virtual IPv6 address and interface of VRRPv3.

Parameters: <ipv6-address> is the virtual IPv6 address, which must be an IPv6 link-local address.

{Vlan <ID>| IFNAME} is the interface name.

Command Mode: VRRPv3 Mode.

Default: None.

Usage Guidelines: This command adds a virtual IPv6 address and interface to an existing backup group. The **no** form of this command deletes the virtual IPv6 address and interface of the backup group. The virtual IPv6 address is a link-local unicast address, and a backup group can have only one. To avoid returning the physical MAC address when the virtual IPv6 address is pinged, the virtual IPv6 address must not be the real IPv6 address of the interface. Therefore, the interfaces of all VRRPv3 backup groups start as Backup, and a master is elected within each group.

Example: Set the virtual IPv6 address of the backup group to fe80::2 on interface VLAN 1.

```
Switch(config-router)# virtual-ipv6 fe80::2 interface vlan 1
```

Chapter 14 Commands for VPN

14.1 MPLS

14.1.1 mpls egress-ttl

Command: **`mpls egress-ttl <0-255>`**
`no mpls egress-ttl`

Function: Sets the TTL of IP packets passing through the egress LSR of an LSP. The **no** form of this command removes the configured value.

Parameters: <0-255>: The TTL value.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: The configured egress TTL is used as the TTL of all IP packets forwarded through this egress LSR.

Example: Set the egress TTL to 45.

```
Switch#config terminal
Switch(config)#mpls egress-ttl 45
```

Related Commands: mpls ingress-ttl

14.1.2 mpls enable

Command: **`mpls enable`**
`no mpls enable`

Function: Enables MPLS. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: This command enables MPLS.

Example:

```
Switch(config)#mpls enable
```

14.1.3 mpls ingress-ttl

Command: **`mpls ingress-ttl <0-255>`**
`no mpls ingress-ttl`

Function: Sets the TTL of IP packets passing through the ingress LSR of an LSP. The **no** form of this command removes the configured value.

Parameters: <0-255>: The TTL value.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: The configured ingress TTL is used as the TTL in the top label of all MPLS packets entering the LSP at this ingress LSR.

Example: Set the ingress TTL to 45.

```
Switch#config terminal
Switch(config)#mpls ingress-ttl 45
```

Related Commands: mpls egress-ttl

14.1.4 mpls local-packet-handling

Command: `mpls local-packet-handling`
`no mpls local-packet-handling`

Function: Enables MPLS forwarding of locally generated traffic.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: After this command is configured, traffic sent by the switch itself is forwarded over MPLS.

Example:

```
Switch(config)#mpls local-packet-handling
```

14.1.5 mpls mtu

Command: `mpls mtu <64-2000>`
`no mpls mtu`

Function: Configures the MPLS MTU.

Command Mode: Interface Mode.

Default: 1500.

Example: Set the MPLS MTU to 1400.

```
Switch(config-if-vlan1)#mpls mtu 1400
```

14.1.6 show mpls

Command: `show mpls`

Function: Displays all label information.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays all label information.

Example: Display all label information.

```
Switch#show mpls
  Minimum label configured: 16
  Maximum label configured: 1048575
  Per label-space information:
  Label-space 0 is using minimum label: 16 and maximum label: 1048575
  Custom ingress TTL configured: none
  Custom egress TTL configured: none
```

Output	Description
Minimum label configured	Configured minimum label
Maximum label configured	Configured maximum label
Per label-space information	Information for each label space
Label-space 0 is using minimum label	Minimum label that label space 0 can use
Label-space 0 is using maximum label	Maximum label that label space 0 can use
Custom ingress TTL configured	User-configured ingress TTL
Custom egress TTL configured	User-configured egress TTL

14.1.7 show mpls enable

Command: `show mpls enable`

Function: Displays whether MPLS is enabled.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays whether MPLS is enabled.

Example: Display whether MPLS is enabled.

```
Switch#show mpls enable
Switch#MPLS enable has been on
```

Related Commands: mpls enable

14.1.8 show mpls forwarding-table

Command: `show mpls forwarding-table`

Function: Displays all LSPs created by the switch as an ingress router, and the FTN (FEC-to-NHLFE) entries marked as selected.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays all LSPs created by the switch as an ingress router, and the FTN entries marked as selected.

Example: Display all LSPs created by the switch as an ingress router.

```
Switch#show mpls forwarding-table
Codes: > - selected FTN, B - BGP FTN, C - CR-LDP FTN, K - CLI FTN,
L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, U - unknownnnnn FTN
Code  FEC             FTN-ID     Pri  Nexthop         Out-Label     Out-Intf
L>    200.200.1.2/32      1         Yes  202.200.1.1      640          Vlan3
L>    202.200.1.0/24      2         Yes  0.0.0.0          3            Vlan3
L>    202.200.2.0/24      3         Yes  202.200.1.1      3            Vlan3
```

Output	Description
Code	Type
FEC	FEC address
FTN-ID	FTN ID
Pri	Whether the LSP is primary
Nexthop	Next-hop address
Out-Label	Outgoing label
Out-Intf	Outgoing interface

14.1.9 show mpls ftn-table brief

Command: `show mpls ftn-table brief`

Function: Displays brief information about the public network FTN entries created by MPLS on the switch.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays brief information about the public network FTN entries created by MPLS on the switch.

Example:

```
Switch#show mpls ftn-table brief
                              FTN Entry Brief Information
------------------------------------------------------------------------------
----------------------------------
    FEC           Out-Label Out-intf   Next hop       Oper-code   Op-State
Vrf
100.1.1.0/24         3       Vlan10    0.0.0.0         Push       Up       0
```

14.1.10 show mpls ftn-table detail

Command: `show mpls ftn-table detail`

Function: Displays detailed information about the public network FTN entries created by MPLS on the switch.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays detailed information about the public network FTN entries created by MPLS on the switch.

Example:

```
Switch#show mpls ftn-table detail
-------------------------------------------
 FTN ID              :     1
 VrfIndex            :     0
 Fec                 :     100.1.1.0/24
 Nexthop addr        :     0.0.0.0
 Owner               :     LDP
 Primary             :     Yes
 Row Status          :     Active
 Exp-bits            :     0X0
 Incoming DSCP       :     none
 Tunnel ID           :     0
 Protected LSP id    :     0
 QoS Resource id     :     0
 In-Label            :     0
 In-Interface        :     N/A
 Out-Label           :     3
 Out-Interface       :     Vlan10
 Admin Status        :     Up
 Oper Status         :     Up
 Oper Code           :     Push
```

Output	Description
FTN ID	FTN ID
VrfIndex	VRF index
Fec	FEC address
Nexthop addr	Next-hop address
Owner	Protocol that created the entry
Primary	Whether the entry is primary
Row Status	Row status
Exp-bits	EXP bits
Incoming DSCP	Incoming DSCP (Differentiated Services Code Point)
Tunnel ID	Tunnel ID

Protected LSP id	ID of the protected LSP
QoS Resource id	QoS resource ID
in label	Incoming label
In-Interface	Incoming interface
Out-Label	Outgoing label
Out-Interface	Outgoing interface
Admin Status	Administrative status
Oper Status	Operational status
Oper Code	Operation code

14.1.11 show mpls ilm-table

Command: `show mpls ilm-table`

Function: Displays the ILM (incoming label map) entries created by MPLS on the switch.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the ILM entries created by MPLS.

Example:

```
Switch#show mpls ilm-table
In-Label  Out-Label  In-Intf  Out-Intf  Nexthop         FEC
640       3          Vlan1    Vlan2     24.1.1.2        2.2.2.2/32
641       3          Vlan2    Vlan1     14.1.1.1        1.1.1.1/32
```

Output	Description
In-Label	Incoming label
Out-Label	Outgoing label
In-Intf	Incoming interface
Out-Intf	Outgoing interface
Nexthop	Next-hop address
FEC	FEC address

14.1.12 show mpls vrf-table

Command: `show mpls vrf-table [vrf-name]`

Function: Displays detailed information about all configured VRF entries.

Parameters: vrf-name: The VRF name.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays detailed information about all configured VRF entries. If a VRF is specified, only the details of that VRF are displayed.

Example:

```
Switch#show mpls vrf-table
Output for VRF table with id: 1
-------------------------------------------
 FTN ID              :     1
 VrfIndex             :     1
 Fec                 :     10.1.1.0/24
 Nexthop addr        :     0.0.0.0
 Owner               :     BGP
 Primary              :     Yes
 Row Status          :     Active
```

```
Exp-bits              :     0X0
Incoming DSCP      :     none
Tunnel ID             :     0
Protected LSP id     :     0
QoS Resource id     :     0
In-Label              :     0
In-Interface          :     N/A
Out-Label           :     0
Out-Interface         :     Vlan20
Admin Status        :     Up
Oper Status         :     Up
Oper Code           :     Deliver to IP
```

Output	Description
FTN ID	FTN ID
VrfIndex	VRF index
Fec	FEC address
Nexthop addr	Next-hop address
Owner	Protocol that created the entry
Primary	Whether the entry is primary
Row Status	Row status
Exp-bits	EXP bits
Incoming DSCP	Incoming DSCP (Differentiated Services Code Point)
Tunnel ID	Tunnel ID
Protected LSP id	ID of the protected LSP
QoS Resource id	QoS resource ID
in label	Incoming label
In-Interface	Incoming interface
Out-Label	Outgoing label
Out-Interface	Outgoing interface
Admin Status	Administrative status
Oper Status	Operational status
Oper Code	Operation code

14.2 LDP

14.2.1 advertisement-mode

Command: advertisement-mode {downstream-on-demand | downstream-unsolicited}
no advertisement-mode {downstream-on-demand | downstream-unsolicited}

Function: Configures the label advertisement mode. The **no** form of this command removes the configuration.

Parameters: downstream-on-demand: Downstream on demand (DoD). **downstream-unsolicited**: Downstream unsolicited (DU).

Default: Downstream unsolicited.

Command Mode: LDP Router Mode.

Usage Guidelines: The label advertisement mode determines how LDP advertises labels. In downstream-on-demand mode, the switch advertises a label to an upstream LSR only when the upstream LSR requests one. In downstream-unsolicited mode, the switch allocates labels to all upstream LSRs whether or not they request them. Use this mode together with matching label

retention and label control modes: downstream-unsolicited with liberal retention and independent control, and downstream-on-demand with conservative retention and ordered control. Avoid configuring these attributes independently. If a label advertisement mode is configured on the interface, this command has no effect on it.

Example: Configure the label advertisement mode as downstream-on-demand.

```
Switch(config)#router ldp
Switch(config-router)#advertisement-mode downstream-on-demand
```

Related Commands: ldp advertisement-mode, label-retention-mode, ldp label-retention-mode

14.2.2 clear ldp adjacency

Command: `clear ldp adjacency {<ip-addr>|*}`

Function: Clears LDP adjacencies.

Parameters: <ip-addr> is the IP address of the adjacency; ***** clears all adjacencies.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: This command clears the adjacency between the switch and its neighbor. With the configuration unchanged, the switch re-establishes the adjacency with the neighbor through negotiation.

Example: Clear the adjacency with neighbor 10.10.10.1.

```
Switch#clear ldp adjacency 10.10.10.1
```

14.2.3 clear ldp session

Command: `clear ldp session {<ip-addr> | *}`

Function: Clears LDP sessions.

Parameters: <ip-addr> is the IP address of the neighbor; ***** clears all sessions.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: This command clears LDP sessions. With the configuration unchanged, the switch re-establishes the sessions. Note that one session can contain multiple adjacencies.

Example:

```
Switch#clear ldp session *
```

14.2.4 clear ldp statistics

Command: `clear ldp statistics`

Function: Clears LDP statistics.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: This command clears all LDP statistics.

Example:

```
Switch#clear ldp statistics
```

14.2.5 control-mode

Command: `control-mode {ordered | independent}`
`no control-mode`

Function: Configures the LSP control mode. The **no** form of this command removes the configuration.

Parameters: ordered: Ordered control. **independent**: Independent control.

Default: independent.

Command Mode: LDP Router Mode.

Usage Guidelines: LSP control has two modes: independent and ordered. In ordered mode, an LSR advertising a label mapping for an FEC to its upstream must first receive a label mapping for that FEC from downstream (unless it is the egress router for the FEC); independent mode does not require this. Hop-by-hop routing applications usually use independent control with DU advertisement. Ordered mode should be used with DoD advertisement.

Example: Set the LSP control mode to ordered.

```
Switch(config)#router ldp
Switch(config-router)#control-mode ordered
```

Related Commands: advertisement-mode, ldp advertisement-mode

14.2.6 debug ldp all

Command: `debug ldp all`
`no debug ldp all`

Function: Displays all LDP debugging information. When disabled, all LDP debugging is disabled.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Example: Enable all LDP debugging.

```
Switch#debug ldp all
Switch#
```

14.2.7 debug ldp dsm

Command: `debug ldp dsm`
`no debug ldp dsm`

Function: Displays debugging information for the LDP downstream state machine. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: When enabled, debugging information is displayed whenever an LDP change related to the downstream state machine occurs.

Example: Enable the debugging.

```
Switch#debug ldp dsm
Switch#
```

14.2.8 debug ldp error

Command: debug ldp error
no debug ldp error

Function: Displays debugging information for LDP errors. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: When enabled, debugging information is displayed for any LDP error.

Example: Enable the debugging.

```
Switch# debug ldp error
Switch#
```

14.2.9 debug ldp events

Command: debug ldp events
no debug ldp events

Function: Displays debugging information for LDP events. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: When enabled, debugging information is displayed for LDP events.

Example: Enable the debugging.

```
Switch#debug ldp events
Switch#
```

14.2.10 debug ldp fsm

Command: debug ldp fsm
no debug ldp fsm

Function: Displays debugging information for the LDP session finite state machine. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Enables or disables debugging information related to the LDP session finite state machine.

Example: Enable the debugging.

```
Switch#debug ldp fsm
Switch#
```

14.2.11 debug ldp hexdump

Command: debug ldp hexdump
no debug ldp hexdump

Function: Displays debugging information for LDP messages in hexadecimal. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Enables or disables hexadecimal debugging of the contents of LDP messages received and sent.

Example: Enable the debugging.

```
Switch#debug ldp hexdump
Switch#
```

14.2.12 debug ldp nsm

Command: `debug ldp nsm`
`no debug ldp nsm`

Function: Displays debugging information for messages exchanged between NSM and LDP. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Enables or disables NSM debugging information, mainly interface changes, route changes, and entry distribution.

Example: Enable the debugging.

```
Switch#debug ldp nsm
```

14.2.13 debug ldp packet

Command: `debug ldp packet [receive|send|detail]`
`no debug ldp packet [receive|send|detail]`

Function: Displays debugging information for LDP messages. The **no** form of this command disables it.

Parameters: receive, **send**, **detail**: The message types to debug.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Enables or disables debugging of LDP messages received and sent. When enabled, all sent and received messages are displayed. **receive**, **send**, and **detail** display received messages, sent messages, and detailed information, respectively.

Example: Enable the debugging.

```
Switch#debug ldp packet receive
```

14.2.14 debug ldp timer

Command: `debug ldp timer`
`no debug ldp timer`

Function: Displays debugging information for the LDP timers. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: When enabled, LDP timer debugging information is displayed.

Example: Enable the debugging.

```
Switch#debug ldp timer
```

14.2.15 debug ldp tsm

Command: `debug ldp tsm`
`no debug ldp tsm`

Function: Displays debugging information for the LDP state machine. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Displays LDP state machine debugging information.

Example: Enable the debugging.

```
Switch#debug ldp tsm
```

14.2.16 debug ldp usm

Command: `debug ldp usm`
`no debug ldp usm`

Function: Displays debugging information for the LDP upstream state machine. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Displays LDP upstream state machine debugging information.

Example: Enable the debugging.

```
Switch#debug ldp usm
```

14.2.17 ldp {enable|disable}

Command: `ldp {enable|disable}`

Function: Enables or disables LDP on the interface.

Parameters: enable: Enables LDP. **disable**: Disables LDP.

Default: Disabled.

Command Mode: Interface Mode.

Usage Guidelines: LDP is a label distribution protocol used for label switching in the public network, typically in a BGP VPN environment. **router ldp** enables LDP globally, but on each interface where LDP actually runs, **ldp enable** must be configured in Interface Mode and label switching must be enabled; together, these ensure that the protocol operates normally.

Example:

```
Switch(config)#int vlan 9
Switch(Config-if-Vlan9)#ldp enable
```

Related Commands: router ldp, label-Switching

14.2.18 global-merge-capability

Command: `global-merge-capability {merge-capable|non-merge-capable }`
`no global-merge-capability {merge-capable|non-merge-capable }`

Function: Enables or disables the LDP label merging capability globally. The **no** form of this command restores the default.

Parameters: merge-capable: Label merging enabled. **non-merge-capable**: Label merging disabled.

Default: Label merging is enabled globally.

Command Mode: LDP Router Mode.

Usage Guidelines: When an LSR maps multiple incoming labels for the same FEC to the same outgoing label and interface, packets that enter with different labels leave with the same label; this is called label merging. If the label merging capability of the interface changes, the switch restarts.

Example:

```
Switch(config)#router ldp
Switch(config-router)#global-merge-capability non-merge-capable
```

14.2.19 hello-interval

Command: `hello-interval <hello-interval>`
`no hello-interval`

Function: Sets the global interval between Hello messages. The **no** form of this command restores the default.

Parameters: <hello-interval> is the interval between Hello messages, ranging from 1 to 65535 seconds.

Default: 5 seconds.

Command Mode: LDP Router Mode.

Usage Guidelines: LDP discovers neighbors and maintains communication with them through multicast Hello messages. This command sets the interval for sending Hello messages. Set it to no more than one third of the hold time. If a hello interval is configured on an interface, the global configuration does not apply to that interface.

Example: Set the hello interval to 10 seconds.

```
Switch(config)#router ldp
Switch(config-router)#hello-interval 10
```

Related Commands: hold-time, ldp hello-interval, ldp hold-time

14.2.20 hold-time

Command: `hold-time <hold-time>`
`no hold-time`

Function: Configures the hold time of LDP multicast (link) peers. The default is 15 seconds. The **no** form of this command restores the default.

Parameters: <hold-time> is the hold time of multicast peers, ranging from 3 to 65535 seconds.

Default: 15 seconds.

Command Mode: LDP Router Mode.

Usage Guidelines: LDP discovers neighbors and maintains communication with them through multicast Hello messages. This command sets the hold time. Set it to at least three times the hello interval. If a hold time is configured on an interface, the global configuration does not apply to that interface.

Example: Set the hold time to 50 seconds.

```
Switch(config)#router ldp
Switch(config-router)#hold-time 50
```

Related Commands: hello-interval, ldp hold-time, ldp hello-interval

14.2.21 import-bgp-routes

Command: `import-bgp-routes`
`no import-bgp-routes`

Function: Configures LDP to import BGP routes. The **no** form of this command restores the default.

Parameters: None.

Default: LDP does not import BGP routes.

Command Mode: LDP Router Mode.

Usage Guidelines: Normally, LDP obtains routes from the system routing table, except default routes and BGP routes. Importing default routes may cause problems and is never allowed. If security can be ensured, BGP routes can be imported with this command and labels allocated to them.

Example: Import BGP routes and allocate labels to them.

```
Switch(config)#router ldp
Switch(config-router)#import-bgp-routes
```

14.2.22 keepalive-interval

Command: `keepalive-interval <interval>`
`no keepalive-interval`

Function: Configures the interval between LDP keepalive messages. The default is 10 seconds. The **no** form of this command restores the default.

Parameters: <interval> is the interval between keepalive messages, ranging from 1 to 65535 seconds.

Default: 10 seconds.

Command Mode: LDP Router Mode.

Usage Guidelines: After a TCP session is established, LDP peers exchange keepalive messages to maintain the session when there is no other data. This command sets the keepalive interval. Make the value large enough to avoid excessive keepalive messages. If the value is configured on an interface, the global configuration does not apply to that interface.

Example: Set the global keepalive interval to 50 seconds.

```
Switch(config)#router ldp
Switch(config-router)#keepalive-interval 50
```

Related Commands: keepalive-timeout, ldp keepalive-interval

14.2.23 keepalive-timeout

Command: `keepalive-timeout <time-val>`
`no keepalive-timeout`

Function: Configures the LDP session timeout. The default is 30 seconds. The **no** form of this command restores the default.

Parameters: <time-val> is the session timeout, ranging from 15 to 65535 seconds.

Default: 30 seconds.

Command Mode: LDP Router Mode.

Usage Guidelines: After a TCP session is established, LDP peers exchange keepalive messages to maintain the session when there is no other data. If no keepalive message is received within the timeout set by this command, the session is considered down. The timeout should normally be at least three times the keepalive interval. If the value is configured on an interface, the global configuration does not apply to that interface.

Example: Set the global session timeout.

```
Switch(config)#router ldp
Switch(config-router)#keepalive-timeout 50
```

Related Commands: keepalive-interval, ldp keepalive-timeout

14.2.24 label-retention-mode

Command: `label-retention-mode {conservative|liberal}`
`no label-retention-mode {conservative|liberal}`

Function: Configures the label retention mode. The **no** form of this command removes the configuration.

Parameters: conservative: Conservative retention. **liberal**: Liberal retention.

Default: liberal.

Command Mode: LDP Router Mode.

Usage Guidelines: The label retention mode determines how LDP handles label information. In conservative mode, only label information useful to the switch is retained and the rest is discarded. In liberal mode, all label information is retained. This mode works with the label advertisement mode: liberal with downstream-unsolicited, and conservative with downstream-on-demand. A manually configured liberal mode differs from the default liberal mode: when liberal mode is set manually, interfaces without their own configuration use the global mode; in the default liberal mode, the mode is adjusted according to the label advertisement mode of the interface. Normally, do not configure this attribute, because it follows the label advertisement mode and changes automatically with it; configuring it separately may cause mismatched attributes. If the label retention mode changes while sessions on the interface are established, the sessions are reconnected.

Example: Set the global label retention mode to liberal.

```
Switch(config)#router ldp
Switch(config-router)#label-retention-mode liberal
```

Related Commands: advertisement-mode, ldp advertisement-mode

14.2.25 label-switching

Command: `label-switching`
`no label-switching`

Function: Enables label switching. The **no** form of this command disables it.

Parameters: None.

Command Mode: Interface Mode.

Default: Disabled.

Usage Guidelines: This command enables label switching, which is required for LDP to operate normally.

Example: Enable label switching on interface VLAN 1.

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#label-switching
```

Related Commands: enable-ldp

14.2.26 ldp advertisement-mode

Command: `ldp advertisement-mode {downstream-on-demand | downstream-unsolicited}`
`no ldp advertisement-mode {downstream-on-demand | downstream-unsolicited}`

Function: Configures the label advertisement mode of the interface. The **no** form of this command removes the configuration.

Command Mode: Interface Mode.

Usage Guidelines: This command sets the label advertisement mode of the interface to downstream-unsolicited or downstream-on-demand, which can differ from the global configuration. By default, the interface uses the global default or global configuration unless it has its own setting. This mode works with two other modes, and changing it changes them as well: with downstream-unsolicited, the label retention mode is liberal and the LSP control mode is independent; with downstream-on-demand, the label retention mode is conservative and the LSP control mode is ordered.

Example: Set the label advertisement mode of the interface to downstream-unsolicited.

```
Switch(config)#int vlan 9
Switch(Config-if-Vlan9)#ldp advertisement-mode downstream-unsolicited
```

Related Commands: label-retention-mode, ldp label-retention-mode, advertisement-mode

14.2.27 ldp hello-interval

Command: `ldp hello-interval <hello-interval>`
`no ldp hello-interval`

Function: Sets the hello interval of the interface. The **no** form of this command removes the configuration.

Parameters: <hello-interval> is the interval between multicast Hello messages, ranging from 1 to 65535 seconds.

Default: The global configuration is used.

Command Mode: Interface Mode.

Usage Guidelines: This command sets the interval between multicast Hello messages on the interface, which can differ from the global configuration.

Example: Set the hello interval of the interface to 25 seconds.

```
Switch(config)#int vlan 9
Switch(Config-if-Vlan9)#ldp hello-interval 25
```

Related Commands: ldp hold-time, hold-time

14.2.28 ldp hold-time

Command: `ldp hold-time <hold-time>`
`no ldp hold-time`

Function: Sets the neighbor hold time of the interface. The **no** form of this command restores the default.

Parameters: <hold-time> is the neighbor hold time, ranging from 3 to 65535 seconds.

Default: The global configuration is used.

Command Mode: Interface Mode.

Usage Guidelines: LDP discovers neighbors and maintains communication with them through multicast Hello messages. This command sets the neighbor hold time on the interface. Set it to at

least three times the hello interval. When a hold time is configured on the interface, the global configuration does not apply to it.

Example: Set the neighbor hold time to 220 seconds.

```
Switch(config)#int vlan 9
Switch(Config-if-Vlan9)#ldp hold-time 220
```

Related Commands: ldp hello-interval, hello-interval

14.2.29 ldp keepalive-interval

Command: `ldp keepalive-interval <interval-time>`
`no ldp keepalive-interval`

Function: Configures the keepalive interval of the interface. The **no** form of this command restores the default.

Parameters: <interval-time> is the interval between keepalive messages, ranging from 1 to 65535 seconds.

Default: The global configuration is used.

Command Mode: Interface Mode.

Usage Guidelines: After a TCP session is established, LDP peers exchange keepalive messages to maintain the session when there is no other data. This command sets the keepalive interval on the interface, which can differ from the global configuration. Make the value large enough to avoid excessive keepalive messages.

Example: Set the keepalive interval of the interface to 33 seconds.

```
Switch(config)#int vlan 9
Switch(Config-if-Vlan9)#ldp keepalive-interval 33
```

Related Commands: ldp keepalive-timeout, keepalive-timeout

14.2.30 ldp keepalive-timeout

Command: `ldp keepalive-timeout <time-val>`
`no ldp keepalive-timeout`

Function: Configures the session timeout of the interface. The **no** form of this command restores the default.

Parameters: <time-val> is the session timeout, ranging from 15 to 65535 seconds.

Default: 30s.

Command Mode: LDP Router Mode.

Usage Guidelines: After a TCP session is established, LDP peers exchange keepalive messages to maintain the session when there is no other data. If no keepalive message is received within the timeout, the session is considered down. The timeout should normally be at least three times the keepalive interval. The interface value can differ from the global configuration.

Example: Configure the keepalive-interval of the interface as 200s.

```
Switch(config)#int vlan 9
Switch(Config-if-Vlan9)#ldp keepalive-timeout 200
```

Related Commands: ldp keepalive-interval, keepalive-interval

14.2.31 ldp label-retention-mode

Command: `ldp label-retention-mode {conservative | liberal}`
`no ldp label-retention-mode {conservative | liberal}`

Function: Configures the label retention mode of the interface. The **no** form of this command restores the default.

Parameters: conservative: Conservative retention. **liberal**: Liberal retention.

Default: liberal.

Command Mode: Interface Mode.

Usage Guidelines: This command sets the label retention mode of the interface to conservative or liberal. When the mode changes, all sessions on the interface are re-established. If the interface configuration differs from the global configuration, the global configuration is ignored for the interface.

Example: Set the label retention mode of the interface to conservative.

```
Switch(config)#int vlan 9
Switch(Config-if-Vlan9)#ldp label-retention-mode conservative
```

Related Commands: advertisement-mode, ldp advertisement-mode

14.2.32 ldp multicast-hellos

Command: `ldp multicast-hellos`
`no ldp multicast-hellos`

Function: Configures the interface to discover LDP neighbors with multicast Hello messages. The **no** form of this command removes the configuration.

Parameters: None.

Default: The global configuration is used.

Command Mode: Interface Mode.

Usage Guidelines: LDP discovers neighbors through multicast Hello messages, or through neighbors specified with the **targeted-peer** command. This command enables multicast Hello neighbor discovery. The **no** form stops sending and receiving multicast Hello messages, so neighbors can be discovered only with **targeted-peer**. The interface setting can differ from the global configuration.

Example:

```
Switch(config)#int vlan 9
Switch(Config-if-Vlan9)#ldp multicast-hellos
```

Related Commands: multicast-hellos

14.2.33 ldp targeted-peer-hello-interval

Command: `ldp targeted-peer-hello-interval <hello-interval>`
`no ldp targeted-peer-hello-interval`

Function: Sets the interval of Hello messages sent to specified targets. The **no** form of this command restores the global configuration.

Parameters: <hello-interval> is the interval of Hello messages sent to specified targets, ranging from 1 to 65535 seconds.

Default: The global configuration is used.

Command Mode: Interface Mode.

Usage Guidelines: LDP discovers neighbors and maintains communication with them by sending Hello messages to specified targets. This command sets the interval of these Hello messages. Set it

to no more than one third of the targeted peer hold time. The interface setting can differ from the global configuration.

Example: Set the interval of Hello messages to specified targets to 255 seconds.

```
Switch(config)#int vlan 9
Switch(Config-if-Vlan9)#ldp targeted-peer-hello-interval 255
```

Related Commands: ldp targeted-peer-hold-time, targeted-peer-hold-time

14.2.34 ldp targeted-peer-hold-time

Command: `ldp targeted-peer-hold-time <hold-time>`
`no ldp targeted-peer-hold-time`

Function: Sets the hold time for specified targets on the interface. The **no** form of this command restores the global configuration.

Parameters: <hold-time> is the hold time for specified targets, ranging from 3 to 65535 seconds.

Default: The global configuration is used.

Command Mode: Interface Mode.

Usage Guidelines: LDP maintains communication with neighbors by sending Hello messages to specified targets. This command sets the hold time for specified targets. Set it to at least three times the targeted hello interval. The interface setting can differ from the global configuration.

Example:

```
Switch(config)#int vlan 9
Switch(Config-if-Vlan9)#ldp targeted-peer-hold-time 50
```

Related Commands: ldp targeted-peer-hello-interval, targeted-peer-hello-interval

14.2.35 loop-detection

Command: `loop-detection`
`no loop-detection`

Function: Enables LDP loop detection. The **no** form of this command removes the configuration.

Parameters: None.

Default: Disabled.

Command Mode: LDP Router Mode.

Usage Guidelines: LDP loop detection can be enabled or disabled. When enabled, LDP uses two methods: checking whether the hop count exceeds the limit, and checking whether an LSR ID is repeated in the path vector.

Example:

```
Switch(config)#router ldp
Switch(config-router)#loop-detection
```

14.2.36 loop-detection-count

Command: `loop-detection-count <count>`

Function: Sets the maximum number of hops allowed in LDP loop detection. The **no** form of this command restores the default.

Parameters: <count> is the maximum hop count, ranging from 1 to 255.

Default: 255.

Command Mode: LDP Router Mode.

Usage Guidelines: This command sets the maximum hop count for LDP loop detection. It takes effect only when loop detection is enabled. The **no** form restores the default.

Example: Set the maximum hop count for LDP loop detection to 200.

```
Switch(config)#router ldp
Switch(config-router)#loop-detection-count 200
```

Related Commands: loop-detection

14.2.37 multicast-hellos

Command: `multicast-hellos`
`no multicast-hellos`

Function: Configures whether LDP discovers neighbors with multicast Hello messages globally. The **no** form of this command stops sending and receiving multicast Hello messages.

Parameters: None.

Default: Sending and receiving multicast Hello messages is enabled on LDP interfaces.

Command Mode: LDP Router Mode.

Usage Guidelines: LDP discovers neighbors through multicast Hello messages, or through neighbors specified with the **targeted-peer** command. This command enables multicast Hello neighbor discovery globally on all interfaces. The **no** form stops sending multicast Hello messages, so neighbors can be discovered only with **targeted-peer**. If the attribute is configured on an interface, the global configuration does not apply to it.

Example:

```
Switch(config)#router ldp
Switch(config-router)#multicast-hellos
```

14.2.38 propagate-release

Command: `propagate-release`
`no propagate-release`

Function: Configures LDP to propagate label releases to neighbors. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: LDP Router Mode.

Usage Guidelines: When a label is released, the switch does not propagate the release upstream unless this command is enabled.

Example:

```
Switch(config)#router ldp
Switch(config-router)#propagate-release
```

14.2.39 request-retry

Command: `request-retry`
`no request-retry`

Function: Configures LDP to retry five times after a label request is rejected. The **no** form of this command removes the configuration.

Parameters: None.

Default: No retry.

Command Mode: LDP Router Mode.

Usage Guidelines: When LDP sends a label request downstream and the request is rejected, LDP retries five times at the interval set by **request-retry-timeout** if request retry is configured.

Example:

```
Switch(config)#router ldp
Switch(config-router)#request-retry
```

Related Commands: request-retry-timeout

14.2.40 request-retry-timeout

Command: `request-retry-timeout <time-val>`
`no request-retry-timeout`

Function: Sets the retry interval after an LDP label request is rejected. The **no** form of this command restores the default.

Parameters: <time-val> is the retry interval, ranging from 1 to 65535 seconds.

Default: 5 seconds.

Command Mode: LDP Router Mode.

Usage Guidelines: When LDP sends a label request downstream and the request is rejected, LDP retries five times at the interval set by **request-retry-timeout** if request retry is configured.

Example: Set the retry interval to 10 seconds.

```
Switch(config)#router ldp
Switch(config-router)#request-retry-timeout 10
```

Related Commands: request-retry

14.2.41 router ldp

Command: `router ldp`
`no router ldp`

Function: Enables LDP globally. The **no** form of this command disables it.

Parameters: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guidelines: LDP is a label distribution protocol used for label switching in the public network, typically in a BGP VPN environment. This command enables LDP globally; on each interface where LDP actually runs, **ldp enable** must be configured in Interface Mode and label switching must be enabled. Together, these ensure that the protocol operates normally.

Example:

```
Switch(config)#router ldp
Switch(config-router)#
```

14.2.42 router-id

Command: `router-id <ip-addr>`
`no router-id`

Function: Sets the router ID used by LDP. The **no** form of this command removes the configuration.

Parameters: <ip-addr> is the router ID, in dotted decimal notation.

Default: Obtained automatically.

Command Mode: LDP Router Mode.

Usage Guidelines: The router ID uniquely identifies an LDP device in the network and is carried in Hello messages.

Example:

```
Switch(config)#router ldp
Switch(config-router)#router-id 10.10.10.10
```

14.2.43 show ldp

Command: show ldp

Function: Displays the basic LDP attributes of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the current LDP configuration.

Example:

```
Switch#show ldp
Router ID : 10.10.0.11
LDP Version : 1
Global Merge Capability : N/A
Label Advertisement Mode : Downstream Unsolicited
Label Retention Mode : Liberal
Label Control Mode : Independent
Loop Detection : Off
Loop Detection Count : 0
Request Retry : Off
Propagate Release : Disabled
Hello Interval : 5
Targeted Hello Interval : 15
Hold time : 15
Targeted Hold time : 45
Keepalive Interval : 10
Keepalive Timeout : 30
Request retry Timeout : 5
Multicast Hello : Enabled
Targeted Hello Accept : Disabled
Transport Interface : N/A
Import BGP routes : No
```

Output	Description
Router ID : 10.10.0.11	The router ID is 10.10.0.11.
LDP Version : 1	The LDP version is 1.
Global Merge Capability : N/A	Global label merging capability is not applicable (N/A).
Label Advertisement Mode : Downstream Unsolicited	The label advertisement mode is downstream unsolicited.
Label Retention Mode : Liberal	The label retention mode is liberal.
Label Control Mode : Independent	The label control mode is independent.
Loop Detection : Off	Loop detection is disabled.
Loop Detection Count : 0	The loop detection count is 0.
Request Retry : Off	The switch does not retry after a label request is rejected.
Propagate Release : Disabled	The switch does not propagate label release messages.
Hello Interval : 5	The interval between Hello messages is 5 seconds.

Targeted Hello Interval : 15	The interval between Hello messages to specified targets is 15 seconds.
Hold time : 15	The adjacency hold time is 15 seconds.
Targeted Hold time : 45	The adjacency hold time for specified targets is 45 seconds.
Keepalive Interval : 10	The interval between keepalive messages is 10 seconds.
Keepalive Timeout : 30	The keepalive timeout is 30 seconds.
Request retry Timeout : 5	The retry interval after a rejected label request is 5 seconds.
Multicast Hello : Enabled	Neighbors are discovered with multicast Hello messages.
Targeted Hello Accept : Disabled	The switch does not accept Hello messages from specified targets.
Transport Interface : N/A	No transport interface is configured.
Import BGP routes : No	The switch does not import BGP routes.

14.2.44 show ldp adjacency

Command: `show ldp adjacency`

Function: Displays all adjacencies of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays LDP adjacency information, for diagnosis and troubleshooting.

Example:

```
Switch#show ldp adjacency
IP Address   Interface Name  Holdtime   LDP ID
192.168.3.5  vlan1           15         10.10.0.18:0
192.168.4.5  vlan2           15         10.10.0.18:0
```

Output	Description
IP Address	IP address of the neighbor
Interface Name	Name of the interface connected to the neighbor
Holdtime	Hold time of the adjacency
LDP ID	LDP ID (LSR ID:label space)

14.2.45 show ldp downstream

Command: `show ldp downstream`

Function: Displays all downstream information of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the downstream information maintained by the protocol.

Example:

```
Switch#show ldp downstream
Session peer 192.168.11.50:
Downstream state: Established Label: impl-null RequestID: 0 Peer:
192.168.11.50 Attr:
```

```
Downstream state: Established Label: impl-null RequestID: 0 Peer:
192.168.11.50 Attr:
Downstream state: Established Label: impl-null RequestID: 0 Peer:
192.168.11.50 Attr:
Downstream state: Established Label: 20 RequestID: 0 Peer: 192.168.11.50 Attr
```

14.2.46 show ldp fec

Command: `show ldp fec`

Function: Displays all FECs (forwarding equivalence classes) of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays all FECs of this LSR.

Example:

```
Switch#show ldp fec
LSR codes    : E/N - LSR is egress/non-egress for this FEC,
               L - LSR received a label for this FEC,
               > - LSR will use this route for the FEC
Code    FEC                    Session     Out Label       Nexthop Addr
E >     3.3.3.1/32              Non-Existent    None            Connected
E >     4.4.4.1/32              Non-Existent    None            80.80.90.2
E >     80.80.90.0/24           Non-Existent    None            Connected
E >     80.90.70.0/24           Non-Existent    None            80.80.90.2
E >     80.90.70.10/32          Non-Existent    None            Connected
E >     80.90.70.78/32          Non-Existent    None            Connected
```

14.2.47 show ldp interface

Command: `show ldp interface [vlan <1-4094> | IFNAME]`

Function: Displays LDP information for all or specified interfaces of this LSR.

Parameters: <1-4094>: The VLAN ID.

IFNAME: The interface name.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays LDP information of interfaces. Specify parameters to display particular interfaces; without parameters, all interfaces are displayed.

Example:

```
Switch#show ldp interface
Interface LDP Identifier Label-switching Merge Capability
vlan0    10.10.0.11:0   Disabled      N/A
vlan1    10.10.0.11:0   Enabled       Merge capable
vlan2    10.10.0.11:0   Enabled       Merge capable
```

14.2.48 show ldp lsp

Command: `show ldp lsp`

Function: Displays the label switched paths (LSPs) of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the label switched paths of the switch.

Example:

```
 Switch#show ldp lsp
FEC IPV4:10.1.1.0/24 -> 0.0.0.0
  Downstream state: Established Label: none RequestID: 0 Peer: EGRESS Attr:
None
    Upstream state: Established Label: impl-null RequestID: 0 Peer: 15.1.1.70
Attr: None
    Upstream state: Established Label: impl-null RequestID: 0 Peer: 20.1.1.1
Attr: None
  Downstream state: Established Label: impl-null RequestID: 0 Peer: 15.1.1.70
Attr: None
FEC IPV4:11.1.1.0/24 -> 0.0.0.0
  Downstream state: Established Label: impl-null RequestID: 0 Peer: 15.1.1.70
Attr: None
  Downstream state: Established Label: none RequestID: 0 Peer: EGRESS Attr:
None
    Upstream state: Established Label: impl-null RequestID: 0 Peer: 15.1.1.70
Attr: None
  Downstream state: Established Label: impl-null RequestID: 0 Peer: 20.1.1.1
Attr: Hop Count: 1
```

14.2.49 show ldp session

Command: `show ldp session [<ip-addr>]`

Function: Displays information about specified or all LDP sessions of this LSR.

Parameters: <ip-addr>: The IP address of the neighbor, in dotted decimal notation.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the current LDP sessions of the switch.

Example:

```
Switch#show ldp session
Peer IP Address IF Name     My Role    State          KeepAlive
192.168.11.50  vlan1         Passive    OPERATIONAL 30
192.168.13.60  vlan2         Passive    OPERATIONAL 30
```

14.2.50 show ldp statistics

Command: `show ldp statistics`

Function: Displays the LDP statistics of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the current LDP statistics of the switch.

Example:

```
Switch#show ldp statistics
  PacketType                Sent      Received
  Notification               18          22
  Hello                  102589      103935
  Initialization             37          37
  Keepalive               45216       45224
  Address                    44          40
  Address Withdraw            3           1
  Label Mapping              97         152
  Label Request               0           0
```

```
  Label Withdraw              3          38
  Label Release              42           3
  Request About               0           0
```

Output		Description
PacketType		Packet types, as listed below
Total	Sent	Total number of packets of this type sent
	Received	Total number of packets of this type received

14.2.51 show ldp targeted-peers

Command: show ldp targeted-peers

Function: Displays the LDP targeted peers configured on this LSR.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the currently configured LDP targeted peers.

Example:

```
Switch#show ldp targeted-peers
IP Address          Interface
10.1.1.66           Vlan2
```

14.2.52 show ldp upstream

Command: show ldp upstream

Function: Displays all upstream information of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays all LDP upstream information maintained by the switch.

Example:

```
 Switch#show ldp upstream
Session peer 192.168.11.50:
Upstream state: Established Label: impl-null RequestID: 0 Peer: 192.168.11.50
Attr:
Upstream state: Established Label: impl-null RequestID: 0 Peer: 192.168.11.50
Attr:
```

14.2.53 show mpls ldp discovery

Command: show mpls ldp discovery [vlan <1-4094> | IFNAME]

Function: Displays the interfaces and label switching information of this LSR.

Parameters: <1-4094>: The VLAN ID.

IFNAME: The interface name.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays all or specified interfaces and their label switching information.

Example:

```
Switch#show mpls ldp discovery
Interface    LDP Identifier     Label-switching      Merge Capability
Vlan1        10.10.0.11:0      Enabled             Merge capable
```

```
Vlan2        10.10.0.11:0      Enabled             Merge capable
Loopback1    0.0.0.0:0       Disabled                N/A
```

14.2.54 show mpls ldp fec

Command: show mpls ldp fec

Function: Displays all FECs of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the FECs currently maintained.

Example:

```
Switch#show mpls ldp fec
LSR codes    : E/N - LSR is egress/non-egress for this FEC,
               L - LSR received a label for this FEC,
               > - LSR will use this route for the FEC
Code    FEC                 Session         Out Label       Nexthop Addr
E >     10.1.1.0/24             non-existent    none            15.1.1.68
NL      10.1.1.0/24             10.1.1.66       impl-null       15.1.1.68
E >     11.1.1.0/24             non-existent    none            15.1.1.68
E >     15.1.1.0/24             non-existent    none            connected
NL>     15.1.1.0/24             10.1.1.66       impl-null       connected
E >     20.1.1.0/24             non-existent    none            15.1.1.68
NL      30.1.1.0/24             10.1.1.66       impl-null       invalid
E >     100.1.1.0/24            non-existent    none            connected
NL      100.1.1.0/24            10.1.1.66       impl-null       connected
```

14.2.55 show mpls ldp neighbor

Command: show mpls ldp neighbor

Function: Displays all neighbors of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays LDP neighbor information, which is useful for troubleshooting.

Example:

```
Switch#show mpls ldp neighbor
IP Address    Interface Name    Holdtime    LDP ID
192.168.3.5   vlan1              15         10.10.0.18:0
192.168.4.5   vlan2              15         10.10.0.18:0
```

14.2.56 show mpls ldp parameter

Command: show mpls ldp parameter

Function: Displays the basic LDP attributes of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the current LDP configuration.

Example:

```
Switch#show mpls ldp parameter
```

```
Router ID : 10.10.0.11
LDP Version : 1
Global Merge Capability : N/A
Label Advertisement Mode : Downstream Unsolicited
Label Retention Mode : Liberal
Label Control Mode : Independent
Loop Detection : Off
Loop Detection Count : 0
Request Retry : Off
Propagate Release : Disabled
Hello Interval : 5
Targeted Hello Interval : 15
Hold time : 15
Targeted Hold time : 45
Keepalive Interval : 10
Keepalive Timeout : 30
Request retry Timeout : 5
 Targeted Hello Receipt : Disabled
Transport Address : N/A
Transport Interface : N/A
Import BGP routes : No
```

Output	Description
Router ID : 10.10.0.11	The router ID is 10.10.0.11.
LDP Version : 1	The LDP version is 1.
Global Merge Capability : N/A	Global label merging capability is not applicable (N/A).
Label Advertisement Mode : Downstream Unsolicited	The label advertisement mode is downstream unsolicited.
Label Retention Mode : Liberal	The label retention mode is liberal.
Label Control Mode : Independent	The label control mode is independent.
Loop Detection : Off	Loop detection is disabled.
Loop Detection Count : 0	The loop detection count is 0.
Request Retry : Off	The switch does not retry when a label request is rejected.
Propagate Release : Disabled	The switch does not propagate label release messages.
Hello Interval : 5	The interval between Hello messages is 5 seconds.
Targeted Hello Interval : 15	The interval between Hello messages to specified targets is 15 seconds.
Hold time : 15	The adjacency hold time is 15 seconds.
Targeted Hold time : 45	The adjacency hold time for specified targets is 45 seconds.
Keepalive Interval : 10	The interval between keepalive messages is 10 seconds.
Keepalive Timeout : 30	The keepalive timeout is 30 seconds.
Request retry Timeout : 5	The retry interval after a rejected label request is 5 seconds.
Targeted Hello Receipt : Disabled	Hello messages from specified targets are not accepted.
Transport Address : N/A	No transport address is configured.
Transport Interface : N/A	No transport interface is configured.
Import BGP routes : No	BGP routes are not imported.

14.2.57 show mpls ldp session

Command: `show mpls ldp session [<ip-addr>]`

Function: Displays all or specified LDP sessions of this LSR.

Parameters: <ip-addr> is the IP address of the neighbor, in dotted decimal notation.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the current LDP sessions of the switch.

Example:

```
Switch#show mpls ldp session
Peer IP Address IF Name     My Role    State          KeepAlive
192.168.11.50  vlan1         Passive    OPERATIONAL 30
192.168.13.60  vlan2         Passive    OPERATIONAL 30
```

14.2.58 targeted-hello-accept

Command: `targeted-hello-accept [filter <1-99>]`
`no targeted-hello-accept`

Function: Configures LDP to accept Hello messages from specified targets (extended discovery).

Parameters: <1-99>: The number of the access list to use.

Default: Targeted Hello messages are not accepted.

Command Mode: LDP Router Mode.

Usage Guidelines: Use this command with an access list to specify the targets from which LDP accepts Hello messages.

Example:

```
Switch(config)#router ldp
Switch(config-router)#targeted-hello-accept filter 1
```

14.2.59 targeted-peer

Command: `targeted-peer <ip-addr>`
`no targeted-peer <ip-addr>`

Function: Configures a targeted LDP neighbor. The **no** form of this command deletes it.

Parameters: <ip-addr> is the IP address of the neighbor, in dotted decimal notation.

Default: No targeted peer is configured.

Command Mode: LDP Router Mode.

Usage Guidelines: LDP discovers neighbors through multicast Hello messages or manual configuration. This command adds a targeted peer and establishes an adjacency with it. Configuring a targeted peer establishes an extended session.

Example: Configure 10.10.10.10 as a targeted LDP neighbor.

```
Switch(config)#router ldp
Switch(config-router)#targeted-peer 10.10.10.10
```

14.2.60 targeted-peer-hello-interval

Command: `targeted-peer-hello-interval <hello-interva>`
`no targeted-peer-hello-interval`

Function: Configures the global interval between Hello messages sent to specified targets. The **no** form of this command restores the default.

Parameters: <hello-interval> is the interval, ranging from 1 to 65535 seconds.

Default: 15 seconds.

Command Mode: LDP Router Mode.

Usage Guidelines: LDP discovers and maintains communication with neighbors by sending Hello messages to specified targets. This command sets the interval of these messages. Set it to no more than one third of the targeted peer hold time. If an interface has its own configuration, this command does not apply to it.

Example: Set the targeted Hello interval to 50 seconds.

```
Switch(config)#router ldp
Switch(config-router)#targeted-peer-hello-interval 50
```

Related Commands: targeted-peer-hold-time, ldp targeted-peer-hold-time, ldp targeted-peer-hello-Interval

14.2.61 targeted-peer-hold-time

Command: `targeted-peer-hold-time <hold-time>`
`no targeted-peer-hold-time`

Function: Configures the global hold time for specified targets. The **no** form of this command restores the default.

Parameters: <hold-time> is the hold time, ranging from 3 to 65535 seconds.

Default: 45 seconds.

Command Mode: LDP Router Mode.

Usage Guidelines: LDP discovers and maintains communication with neighbors by sending Hello messages to specified targets. This command sets the hold time of neighbors discovered through targeted Hello messages. Set it to at least three times the targeted hello interval. If an interface has its own configuration, this command does not apply to it.

Example: Set the targeted neighbor hold time to 50 seconds.

```
Switch(config)#router ldp
Switch(config-router)#targeted-peer-hold-time 50
```

Related Commands: targeted-peer-hello-interval, ldp targeted-peer-hold-time, ldp targeted-peer-hello-interval

14.2.62 transport-address

Command: `transport-address <ip-addr>`
`no transport-address`

Function: Configures the IP address that LDP uses to establish TCP connections. The **no** form of this command removes the configuration.

Parameters: <ip-addr> is the IP address, in dotted decimal notation. It should be the address of a loopback interface.

Default: Obtained automatically.

Command Mode: LDP Router Mode.

Usage Guidelines: After discovering a neighbor through multicast or targeted Hello messages, LDP does not use the address of the interface that sent the messages as the TCP source address; instead, it uses the transport address carried in the Hello messages, to ensure that the connection is unique. LDP usually uses an interface address as the transport address. This command configures the transport address. The **no** form removes the configuration, and an interface address is again used automatically.

Example: Use 10.10.10.10 as the source address of TCP connections.

```
Switch(config)#router ldp
Switch(config-router)#transport-address 10.10.10.10
```

14.3 MPLS VPN

14.3.1 address-family ipv4

Command: address-family ipv4 [unicast | vrf <vrf-name>| multicast]
no address-family ipv4 vrf <vrf-name>

Function: Configures a BGP VPN address family. The **no** form of this command removes it. The VRF must be created and configured with an RD before the BGP VPN address family is entered.

Parameters: unicast: Unicast address family.

<vrf-name>: The VPN routing and forwarding instance name.

Default: No BGP VPN address family is configured.

Command Mode: BGP Mode.

Example:

```
Switch(config)#router bgp 100
Switch(config-router)#address-family ipv4 vrf VRF-A
Switch(config-router-af)#
```

14.3.2 address-family vpnv4

Command: address-family vpnv4 [unicast]

Function: Configures the BGP VPNv4 address family.

Parameters: unicast: Unicast address family.

Default: No BGP VPNv4 address family is configured.

Command Mode: BGP Mode.

Example:

```
Switch(config)#router bgp 100
Switch(config-router)#address-family vpnv4 unicast
Switch(config-router-af)#
```

14.3.3 aggregate-address

Command: aggregate-address <ip-address/M> [summary-only] [as-set]
no aggregate-address <ip-address/M> [summary-only] [as-set]

Function: Configures address aggregation to reduce route advertisement. The **no** form of this command removes the configuration.

Parameters: <ip-address/M>: The IP address and mask length.

summary-only: Advertises only the summary route and suppresses the more specific routes.

as-set: Lists each AS in the path only once, as a set.

Default: Not configured.

Command Mode: BGP Mode and VRF Address Family Mode.

Usage Guidelines: Address aggregation reduces route advertisement. With **summary-only**, only the summary route is advertised and the more specific routes are suppressed. With **as-set**, each AS of the routes covered by the aggregate is listed once, without repetition.

Example:

```
Switch(config-router)#aggregate-address 100.1.0.0/16 summary-only
Switch(config-router)#aggregate-address 100.2.0.0/16 summary-only as-set
Switch(config-router)#aggregate-address 100.3.0.0/16 as-set
```

Related Commands: bgp aggregate-nexthop-check, no bgp aggregate-nexthop-check

14.3.4 clear ip bgp

Command: `clear ip bgp * [vrf <vrf-name>] [in | out | soft [in | out ]]`

Function: Resets the BGP process of the specified VRF and the connections with all its peers.

Parameters: <vrf-name>: The configured VPN instance name, 1 to 64 characters.

in: Soft reset for inbound updates.

out: Soft reset for outbound updates.

soft: Soft reset.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: clear ip bgp * restarts the BGP process. With **in**, route refresh requests are sent to neighbors; with **out**, the switch resends its routes to neighbors; with **soft**, the BGP process is not restarted.

Example:

```
Switch#clear ip bgp * vrf VRF-A
Switch#
```

14.3.5 debug bgp mpls

Command: `debug bgp mpls`
`no debug bgp mpls`

Function: Displays information about processing VRF FTN, global FTN, and global ILM entries while BGP VPN is running. The **no** form of this command disables the display.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Enable this debugging to view how VRF FTN, global FTN, and global ILM entries are processed while BGP VPN is running.

Example:

```
Switch#debug bgp mpls
Switch#
```

14.3.6 debug bgp update

Command: `debug bgp update`
`no debug bgp update`

Function: Displays the route updates received by BGP VPN. The **no** form of this command disables the display.

Parameters: None.

Default: Disabled.

Command Mode: Admin Mode.

Example:

```
Switch#debug bgp update
Switch#
```

14.3.7 description

Command: `description <text>`
`no description`

Function: Configures a VRF description, for example to record the relationship between the VPN instance and a VPN. The **no** form of this command removes the description.

Parameters: <text>: The description, 1 to 256 characters.

Default: None.

Command Mode: VRF Mode.

Usage Guidelines: The text after **description** is displayed under the corresponding VRF for reference.

Example: Set the VRF description to "associate with VRF-B VRF-C".

```
Switch(config)#ip vrf VRF-A
Switch(config-vrf)#description associate with VRF-B VRF-C
```

14.3.8 import map

Command: `import map <route-map-name>`
`no import map`

Function: Applies an import route map to the specified VPN instance.

Parameters: <route-map-name>: The route map name.

Default: None.

Command Mode: VRF Mode.

Usage Guidelines: Use an import route map when finer control than the extended community attribute is needed for importing routes into a VPN instance. By default, imported routes are filtered by their VPN target extended community. The import route map can reject routes selected by the communities in the import list.

Example: Apply route map map-a to VRF instance VRF-A.

```
Switch(config)#ip vrf VRF-A
Switch(config-vrf)#import map map-a
Switch(config-vrf)#
```

14.3.9 ip route vrf

Command: `ip route vrf <vrf-name>{<ip-prefix> <mask>|<ip-prefix/prefix-length>}`
`{<gateway-address>|null0} [<1-255>]`
`no ip route vrf <vrf-name>{<ip-prefix> <mask>|<ip-prefix/prefix-length>}`
`{<gateway-address>|null0} [<1-255>]`

Function: Configures static routes for the specified VRF. The VPN forwarding instance must already exist. The **no** form of this command deletes the static routes.

Parameters: <vrf-name>: The VRF name.

<ip-prefix>: The destination IP address.

<mask>: The subnet mask, in dotted decimal notation.

<prefix-length>: The prefix length.

<gateway-address>: The next-hop address.

null0: Black hole route.

<1-255>: The administrative distance.

Example:

```
Switch(config)#ip route vrf VRF-A 10.1.1.10 255.255.255.0 10.1.1.1
Switch(config)#
```

14.3.10 ip vrf

Command: ip vrf <vrf-name>
no ip vrf <vrf-name>

Function: Creates a VPN instance with the specified name. The **no** form of this command deletes the instance.

Parameters: <vrf-name> is the VPN instance name, 1 to 64 characters.

Default: None.

Command Mode: Global Mode.

Usage Guidelines: There is no default VPN instance on a PE; multiple VPN instances can be created. The VPN instance name is case-sensitive. The VPN instance takes effect only after an RD is configured.

Example:

```
Switch(config)#ip vrf VRF-A
Switch(config-vrf)#
```

14.3.11 ip vrf forwarding vrfName

Command: ip vrf forwarding <vrfName>
no ip vrf forwarding <vrfName>

Function: Binds the interface to the specified VRF.

Parameters: <vrfName> is the VRF name, less than 32 characters.

Command Mode: Interface Mode.

Usage Guidelines: Use this command when the interface must access the VPN. Each interface can be bound to only one VRF, and a VRF can be bound to multiple interfaces. An IGP that supports VPN records the binding by adding routes received on the bound interface to the routing table of the bound VRF. By default, an interface is not bound to any VRF and is a public network interface.

Example:

```
Switch(config)#int vlan 9
Switch(Config-if-Vlan9)#ip vrf forwarding vpn1
```

14.3.12 neighbor remote-as

Command: neighbor <ip-address> remote-as <as-num>
no neighbor <ip-address> remote-as <as-num>

Function: Adds a BGP neighbor. The **no** form of this command deletes it.

Parameters: <ip-address>: The BGP neighbor address. For a neighbor switch, use its loopback interface IP address.

<as-num>: The AS number of the BGP neighbor.

Default: No BGP neighbor is configured.

Command Mode: VRF Address Family Mode.

Usage Guidelines: This command adds a neighbor to the switch.

Example:

```
Switch(config)#router bgp 100
Switch(config-router)#address-family ipv4 vrf VRF-A
Switch(config-router-af)#neighbor 3.0.0.1 remote-as 65001
Switch(config-router-af)#
```

14.3.13 neighbor as-override

Command: neighbor {<ip-address> | <TAG>} as-override
no neighbor {<ip-address> | <TAG>} as-override

Function: Overrides the AS path (replaces the previous AS number). The neighbor must be created first. The **no** form of this command removes the configuration.

Parameters: <ip-address>: The BGP neighbor address.

<TAG>: The BGP peer group name.

Default: Not configured.

Command Mode: VRF Address Family Mode.

Usage Guidelines: After this command is configured, the AS number in routes advertised to the neighbor that matches the neighbor's AS is replaced with the local AS number.

Example:

```
Switch(config)#router bgp 100
Switch(config-router)#address-family ipv4 vrf VRF-A
Switch(config-router-af)#neighbor 3.0.0.1 remote-as 65001
Switch(config-router-af)#neighbor 3.0.0.1 as-override
Switch(config-router-af)#
```

14.3.14 neighbor soo

Command: neighbor <ip-addr> soo <soo-val>
no neighbor <ip-addr> soo <soo-val>

Function: Configures the site of origin (SoO) for routes from the neighbor. The **no** form of this command removes the configuration.

Parameters: <ip-addr>: The IP address of the neighbor, in dotted decimal notation.

<soo-val>: The site of origin, in the same format as an RD.

Default: Not configured.

Command Mode: VRF Address Family Mode.

Usage Guidelines: If a customer AS is connected to multiple ISP devices, this attribute prevents customer routes from returning to the customer after passing through the provider network. Once set, the attribute is propagated. Routes carrying the SoO attribute are not advertised to a neighbor configured with the same attribute.

Example:

```
Switch(config)#router bgp 100
Switch(config-router)#address-family ipv4 vrf test
Switch(config-router-af)#neighbor 11.1.1.64 remote 200
Switch(config-router-af)#neighbor 11.1.1.64 soo 100:10
```

After this configuration, the switch does not advertise remote routes carrying RT attribute 100:10 to 11.1.1.64. Note that the SoO attribute is checked together with the other RT attributes: if an RT matches, the neighbor is treated as the origin regardless of whether it is. In practice, the SoO is usually set to a value different from the RT and RD and unique within the reachable area, so that the origin is identified accurately.

14.3.15 rd

Command: `rd <ASN:nn_or_IP-address:nn>`

Function: Configures the route distinguisher (RD) of the VRF.

Parameters: <ASN:nn_or_IP-address:nn>: ASN is the AS number, ranging from 1 to 4294967295, in decimal notation (such as 6553700) or dotted notation (such as 100.100). IP-address is a 4-byte IP address. nn is an arbitrary 2-byte number.

Default: Not configured.

Command Mode: VRF Mode.

Usage Guidelines: The RD uniquely identifies VPN routes. VPN instances keep their address spaces independent through the RD, which allows address overlap between different VPNs. The RD usually consists of the AS number and an arbitrary number. The RD cannot be deleted directly.

Example:

```
Switch(config)#ip vrf VRF-A
Switch(config-vrf)#rd 300:3
Switch(config-vrf)#
```

14.3.16 route-target

Command: `route-target {import | export | both} <rt-value>`
`no route-target {import | export | both} <rt-value>`

Function: Configures the route targets of the specified VRF. The **no** form of this command deletes the configuration.

Parameters: import: Filters imported routes, that is, determines whether a VPN route can be added to the VRF.

export: The route target added to routes of this VRF when VPNv4 routes are advertised, used for import filtering by other sites.

both: Import and export use the same route target.

<rt-value>: The route target value, in the format ASN:nn_or_IP-address:nn. ASN is the AS number, ranging from 1 to 4294967295, in decimal notation (such as 6553700) or dotted notation (such as 100.100). IP-address is a 4-byte IP address. nn is an arbitrary 2-byte number.

Default: Not configured.

Command Mode: VRF Mode.

Usage Guidelines: A route target (RT) is a BGP extended community used to filter VPN routes and control the VPN membership of directly connected sites and route policies. For the import rule, the BGP process checks all received routes, adds routes whose export RT matches the import RT of this VRF to the BGP process of this VRF, and advertises route updates to the private network BGP neighbors of this VRF. For the export rule, the BGP process adds the export RT to all BGP routes of this VRF and advertises route updates to the public network BGP neighbors. If the import RT of another VRF matches the export RT, the routes are copied to that VRF and route updates are advertised to its private network BGP neighbors.

Example:

```
Switch(config)#ip vrf VRF-A
Switch(config-vrf)#route-target both 100:1
Switch(config-vrf)#
```

14.3.17 show ip bgp vpnv4

Command: `show ip bgp vpnv4 {all|rd <rd-val>|vrf <vrf-name>}`

Function: Displays the routes of all VRFs on this switch or of a specified VRF.

Parameters: all: All VPNv4 routes.

<rd-val>: The route distinguisher, usually numeric (AS number or IP address), such as 100:10.

<vrf-name>: The VPN instance name, 1 to 64 characters.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays information for a specified RD or VRF.

Example:

```
Switch#show ip bgp vpn4 all
Network Next Hop Metric LocPrf Weight Path
Route Distinguisher: 100:10 (Default for VRF test)
*> 11.1.1.0/24 11.1.1.64 0 0 200 ?
*> 20.1.1.0/24 11.1.1.64 0 0 200 ?
```

14.3.18 show ip route vrf

Command: show ip route vrf <vrf-name> [bgp|datebase]

Function: Displays the routes of the specified VRF.

Parameters: <vrf-name>: The VRF name created with the **ip vrf <vrf-name>** command.

bgp: Routes learned through BGP.

database: The IP routing table database.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Displays the routes of the specified VRF.

Example:

```
 Switch#show ip route vrf vrf-a bgp
Network Next Hop Metric LocPrf Weight Path
Route Distinguisher: 100:10 (Default for VRF test)
*> 11.1.1.0/24 11.1.1.64 0 0 200 ?
*> 20.1.1.0/24 11.1.1.64 0 0 200 ?
```

14.3.19 show ip vrf

Command: show ip vrf [<vrf-name>]

Function: Displays the routing protocol instances (such as RIP) associated with the VPN routing and forwarding instance, and the interfaces bound to the VRF.

Parameters: <vrf-name>: The name of the VPN routing and forwarding instance.

Default: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guidelines: Information about other related routing protocol processes is also displayed.

Example: Display the RIP instances associated with VRF IPI.

```
Switch#show ip vrf IPI
VRF IPI, FIB ID 1
Router ID: 11.1.1.1 (automatic)
Interfaces:
Vlan1
!
VRF IPI; (id=1); RIP enabled Interfaces:
 Ethernet1/0/8
Name             Interfaces
IPI                 Vlan1
```

```
Name                    Default RD          Interfaces
IPI                                           Vlan1
```

14.4 VPLS and VPWS

14.4.1 clear mac-address-table

Command: `clear mac-addresse-table [vfi <vfi-name>]`

Function: Clears the MAC address table used for forwarding in VPLS instances. If a VFI is specified, only its MAC address table is cleared; otherwise, all MAC address tables are cleared.

Parameters: vfi <vfi-name>: The VPLS instance name, 1 to 32 characters.

Default: None.

Command Mode: Admin Mode.

Usage Guidelines: Clears all MAC addresses (both VFI and non-VFI addresses) when no VFI is specified, or the MAC addresses of the specified VFI.

Example:

```
Switch#clear mac-address-table vfi v1
```

14.4.2 debug vpls packet

Command: `debug vpls packet [send | receive | detial]`
`no debug vpls packet`

Function: Enables debugging of packets sent and received by VPLS. The **no** form of this command disables it.

Parameters: send: Information about sent packets.

receive: Information about received packets.

detail: Detailed information about sent and received packets.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guidelines: Displays the VPLS packets forwarded by software, including VPWS and VPLS packets and the Layer 2 and Layer 3 packets processed by VPLS and VPWS.

Example:

```
Switch#debug vpls packet send
```

14.4.3 description

Command: `description <text>`
`no description`

Function: Adds a description to the VPLS instance. The **no** form of this command deletes it.

Parameters: <text>: The VFI description, 1 to 128 characters, not case-sensitive.

Default: None.

Command Mode: VFI Mode.

Usage Guidelines: Adds a description to the VPLS instance in VFI Mode.

Example:

```
Switch(config)#vfi v1 100
Switch(config-vfi)#description vpn1
```

14.4.4 encapsulation

Command: `encapsulation {ethernet | vlan}`

Function: Sets the encapsulation type of the VPLS instance. By default, the instance uses VLAN mode and the PW uses tagged mode. This command can specify or change the encapsulation type whenever the VFI exists.

Parameters: ethernet: Ethernet encapsulation for the VPLS instance, with raw mode for the PW.

vlan: VLAN encapsulation for the VPLS instance, with tagged mode for the PW.

Default: VLAN encapsulation for the VPLS instance, with tagged mode for the PW.

Command Mode: VFI Mode.

Usage Guidelines: Use this command to change the VFI encapsulation mode. It cannot be changed after the PW is established.

Example:

```
Switch(config)#vfi v1 100
Switch(config-vfi)#encapsulation ethernet
```

14.4.5 l2-vc

Command: `l2-vc <ip-address> pw-id <pw-id> [group <group-id>] [pw-class <class-name>]`
`no l2-vc <ip-address> pw-id <pw-id>`

Function: Configures the peer PE for VPWS. The **no** form of this command deletes it.

Parameters: <ip-address>: The address of the peer PE in VPWS, usually the router ID or a loopback interface address of the peer PE.

<pw-id>: The PW ID, ranging from 1 to 4294967295. The PW ID must be the same on both PEs.

<group-id>: The group ID of the VPWS neighbor, ranging from 1 to 4294967295.

<class-name>: The PW class used by the VPWS neighbor, 1 to 32 characters, not case-sensitive.

Default: The group ID is 0. If no PW class is specified, the transport mode is tagged.

Command Mode: Global Mode.

Usage Guidelines: This command creates a VPWS; the peer address and the PW ID must be specified.

Example:

```
Switch(config)#l2-vc 192.168.0.1 pw-id 1 pw-class c1
```

14.4.6 mac-address-table limit

Command: `mac-address-table vfi <vfi-name> limit <num>`
`no mac-address-table vfi <vfi-name> limit`

Function: Sets the limit on the total number of MAC addresses in a VPLS instance. When the limit is exceeded, the system stops learning MAC addresses. The **no** form of this command restores the default.

Parameters: <num>: The maximum number of MAC addresses.

Default: No limit.

Command Mode: Global Mode.

Usage Guidelines: Use this command to limit the total number of MAC addresses in a VFI. When the limit is exceeded, the system stops learning MAC addresses.

Example:

```
Switch(config)#mac-address-table vfi v1 limit 100
Switch(config)#no mac-address-table vfi v1 limit
```

14.4.7 mac-address-table static address

Command: mac-address-table static address <FF-FF-FF-FF-FF-FF> vfi <vfi-name> {interface [ethernet | port-channel] <IFNAME> [svid <1-4094>] | peer <peer-address>}

no mac-address-table {static | dynamic} [address <FF-FF-FF-FF-FF-FF>] vfi <vfi-name> [interface [ethernet | port-channel] <IFNAME> | peer <peer-address>]

Function: Configures static MAC addresses in a VPLS instance, either local or remote. The **no** form of this command deletes them.

Parameters: static: Specifies static MAC addresses; currently, only static VFI MAC addresses can be configured.

<FF-FF-FF-FF-FF-FF>: The static MAC address.

vfi: Specifies the VPLS instance.

<vfi-name>: The VPLS instance name, 1 to 32 characters.

<IFNAME>: The interface of the static MAC address, 1 to 32 characters.

peer: Specifies the remote site of the static MAC address.

<peer-address>: The IP address of the remote site for the static MAC address.

Default: No static MAC address is configured.

Command Mode: VFI Mode.

Usage Guidelines: Use this command to add or delete static MAC addresses in a VFI; they are processed in the same way as non-VFI MAC addresses.

Example: Configure a static MAC address for the local site.

```
Switch(config)#mac-address-table static address 00-00-00-00-00-01 vfi v1
interface Ethernet1/0/1 svid 200
```

14.4.8 mtu

Command: mtu <mtu>

no mtu

Function: Specifies the MTU (maximum transmission unit) of the VPLS instance. The **no** form of this command restores the default.

Parameters: <mtu>: The MTU of the VPLS instance, ranging from 576 to 10218.

Default: 1500.

Command Mode: VFI Mode.

Usage Guidelines: Sets the MTU for VPLS forwarding; the appropriate value depends on the application. Normally, the MTU is not changed; change it if small packets pass but large packets do not.

Example:

```
Switch(config)#vfi v1 100
Switch(config-vfi)#mtu 1600
```

14.4.9 peer

Command: peer <ip-address> [pw-id <pw-id>] [no-split-horizon] [pw-class <class-name>]
no peer <ip-address>

Function: Configures a peer PE of the VPLS instance. Split horizon is enabled by default. A neighbor without split horizon is treated as a spoke VC; otherwise, it is treated as a mesh VC. The **no** form of this command deletes the specified neighbor.

Parameters: <ip-address>: The address of the peer PE in VPLS, usually the router ID or a loopback interface address of the peer PE.

pw-id <pw-id>: The PW ID, ranging from 1 to 4294967295. The PW ID must be the same on both PEs.

no-split-horizon: Disables split horizon. Split horizon must be enabled for mesh neighbors.

pw-class <class-name>: The PW class used by the VPLS neighbor, 1 to 32 characters, not case-sensitive.

Default: No PW class is specified, the PW ID is the VPLS ID, and split horizon is enabled. Split horizon must be enabled for mesh neighbors to avoid loops.

Command Mode: VFI Mode.

Example:

```
Switch(config)#vfi v1 100
Switch(config-vfi)#peer 192.168.0.1 pw-class pw1
```

14.4.10 pw-class

Command: pw-class <class-name>
no pw-class <class-name>

Function: Creates a PW class (template) and enters PW Class Mode. The **no** form of this command deletes an existing PW class.

Parameters: <class-name>: The PW class name, 1 to 32 characters, not case-sensitive.

Default: No PW class is configured.

Command Mode: Global Mode.

Usage Guidelines: Use this command to create a PW class, in which the PW encapsulation mode can be set.

Example:

```
Switch(config)#pw-class pw1
Switch(config-class)#
```

14.4.11 show mpls l2-vc

Command: show mpls l2-vc [<vc-id>]

Function: Displays summary information about VCs.

Parameters: <vc-id>: The virtual circuit ID, ranging from 1 to 4294967295.

Default: None.

Command Mode: All Modes.

Usage Guidelines: Displays VPWS information.

Example:

```
Switch#show mpls l2-vc
VC ID       State     Type    In Label    Out Label      Endpoint
```

```
--------       -------     --------   -----------    ------------
------------
10         UP       VLAN   645        650          2.2.2.2
14         UP       VLAN   645        650          2.2.2.2
```

14.4.12 show pw-class

Command: show pw-class [<class-name>]

Function: Displays PW classes.

Parameters: <class-name>: The PW class name, 1 to 32 characters.

Default: None.

Command Mode: All Modes.

Usage Guidelines: Displays PW class information.

Example:

```
Switch#show pw-class
PW-Class Name : class1, encapsulated mode : VLAN
```

14.4.13 show vpls

Command: show vpls [<vfi-name> | detail]

Function: Displays VPLS instances. Without a VFI name, all VPLS instances are displayed. With **detail**, detailed information is displayed; otherwise, summary information is displayed.

Parameters: <vfi-name>: The VPLS instance name, 1 to 32 characters.

detail: Displays detailed information.

Default: None.

Command Mode: All Modes.

Usage Guidelines: Displays VPLS information.

Example:

```
Switch#show vpls
Name    VPLS-ID     Type     MTU      Peers      State
govern 100         Ethernet  1500     2         Active
```

14.4.14 show vpls fib

Command: show vpls fib [<vfi-name>]

Function: Displays the forwarding table of VPLS instances.

Parameters: <vfi-name>: The VPLS instance name, 1 to 32 characters.

Default: None.

Command Mode: All Modes.

Usage Guidelines: Displays the VPLS forwarding entries.

Example:

```
<Sysname> show vpls fib vfi vpna
VfiName PwId Inlabel OutLabel NextHop
vpna     1  103    102     6.1.1.1
```

Output	Description
VfiName	VPLS instance name
PwId	PW ID in the VPLS instance
Inlabel	Incoming label of the VPLS instance
OutLabel	Outgoing label of the VPLS instance

NextHop	Next-hop address of the VPLS instance

14.4.15 show vfi mac-address-table

Command: show vfi mac-addresses-table [vfi <vfi-name>]

Function: Displays the MAC address table of VPLS instances. With a VFI specified, the MAC address table of that VFI is displayed; otherwise, all MAC address tables are displayed.

Parameters: vfi: Specifies the VPLS instance.

<vfi-name>: The VPLS instance name, 1 to 32 characters.

Default: None.

Command Mode: All Modes.

Usage Guidelines: Displays the MAC addresses learned by VPLS.

Example:

```
switch# show vfi mac-address-table vfi aaa
Vfi       MAC Address       Type       Creator       Ports
----      ------------------  ----------  ---------     --------------
aaa     00-01-02-03-04-05  Dynamic        ethernet1/0/1
```

Vfi	VPLS instance name
MAC Address	MAC address
Type	MAC address type: Static or Dynamic
Creator	Creator of the MAC address
Ports	Port name; N/A if empty

14.4.16 show vfi mac-address-table count

Command: show vfi mac-addresses-table count [vfi <vfi-name>]

Function: Displays the number of MAC addresses in VPLS instances. With a VFI specified, the count for that VFI is displayed; otherwise, the counts for all VFIs are displayed.

Parameters: vfi: Specifies the VPLS instance.

<vfi-name>: The VPLS instance name, 1 to 32 characters.

Default: None.

Command Mode: All Modes.

Usage Guidelines: Displays the number of MAC addresses learned in each VFI.

Example:

```
switch# show vfi mac-address-table count
Vfi       MAC count
------    ---------------
vpna    100
vpnb    90
```

14.4.17 show vpls peer

Command: show vpls peer [<vfi-name>] {mesh | spoke}

Function: Displays PW summary information of VPLS instances. Without a VFI name, all mesh or spoke neighbors of VPLS instances are displayed.

Parameters: <vfi-name>: The VPLS instance name, 1 to 32 characters.

mesh: Displays mesh neighbors.

spoke: Displays spoke neighbors.

Default: None.

Command Mode: All Modes.

Usage Guidelines: Displays the VPLS peers of the specified type.

Example:

```
switch#show vpls peer aaa mesh
PW-ID    Peer Addr  In-Intf    In-Label   Out-Intf   Out-Label  Lkps/St
---------    -----------   ---------    -----------   ---------   -----------
----------
100         2.2.2.2  N/A       650      N/A     651       1/UP
```

PW-ID	PW ID
Peer Addr	Peer address
In-Intf	Incoming interface name; N/A if empty
In-Label	Incoming label; none if empty
Out-Intf	Outgoing interface name; N/A if empty
Out-Label	Outgoing label; none if empty
Lkps	Lookup type: 0, 1, or 2; 1 means PUSH_FOR_VC, and 2 means PUSH_AND_LOOKUP_FOR_VC
St	PW state: UP or DOWN

14.4.18 transport-mode

Command: `transport-mode {ethernet | vlan}`
`no transport-mode`

Function: Configures the packet encapsulation mode of the PW class. The **no** form of this command restores the default.

Parameters: ethernet: Packets in the PW are in Ethernet mode, without a VLAN tag.

vlan: Packets in the PW are VLAN-tagged; untagged packets are dropped.

Default: VLAN.

Command Mode: PW Class Mode.

Usage Guidelines: Use this command in a PW class to set the PW encapsulation mode. If it conflicts with the VFI encapsulation mode, the PW encapsulation mode takes precedence.

Example:

```
Switch(config)#pw-class pw1
Switch(config-class)#transport-mode vlan
```

14.4.19 ptag

Command: `ptag <vlan_id>«br»no ptag`

Function: Configures the inner VLAN ID encapsulated in PW packets sent to the peer.

Parameters: <vlan_id>: The inner tag expected by the peer PW, ranging from 1 to 4094.

Default: The inner VLAN ID encapsulated in PW packets sent to the peer is 0.

Command Mode: PW Class Mode.

Usage Guidelines: Use this command in a PW class on the PE to set the inner VLAN expected by the peer PW. After configuration, in tagged mode, the inner tag of packets sent to the peer PW is the configured ptag.

Example:

```
Switch(config)#pw-class pw1
Switch(config-class)#ptag 10
```

14.4.20 vfi

Command: vfi <vfi-name> <vfi-id>
no vfi <vfi-name> <vfi-id>

Function: Creates a VPLS instance with a globally unique VFI name and VFI ID, which map one to one; either uniquely identifies the VPLS instance. The **no** form of this command deletes the VPLS instance.

Parameters: <vfi-name>: The VFI name, globally unique, 1 to 32 characters.

<vfi-id>: The VFI ID, ranging from 1 to 4294967295.

Default: No VPLS instance is configured.

Command Mode: Global Mode.

Usage Guidelines: Use this command to create a VFI and enter VFI Mode to configure VFI commands.

Example:

```
Switch(config)#vfi v1 1
Switch(config-vfi)#
```

14.4.21 vfi vfi-name

Command: vfi <vfi-name>

Function: Enters VFI Mode of an existing VPLS instance.

Parameters: <vfi-name>: The VFI name, globally unique, 1 to 32 characters.

Default: No VPLS instance is configured.

Command Mode: Global Mode.

Usage Guidelines: Use this command to enter the VFI Mode of the instance.

Example:

```
Switch(config)#vfi v1
Switch(config-vfi)#
```

14.4.22 xconnect l2-vc

Command: xconnect l2-vc pw-id <pw-id> [mode {ethernet | vlan [svid <svid>]}]
no xconnect l2-vc pw-id <pw-id>

Function: Binds the port to the specified PW and configures the AC access mode; in VLAN mode, the SVID can also be specified. This command binds the port and PW directly to establish a point-to-point connection for VPWS. The **no** form of this command deletes the binding.

Parameters: ethernet: Ethernet access mode.

vlan: VLAN-tagged access mode.

<pw-id>: The PW ID, ranging from 1 to 4294967295.

<svid>: The service VLAN ID, ranging from 1 to 4094.

Default: The port is not bound to any PW; the access mode is VLAN.

Command Mode: Port Mode.

Usage Guidelines: Use this command to bind the port to the specified PW for VPWS.

Example:

```
Switch(config)#interface Ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#xconnect l2-vc pw-id 1 mode vlan svid 200
```

14.4.23 xconnect vfi

Command: `xconnect vfi <vfi-id> [mode {ethernet | vlan [svid <svid>]}]`
`no xconnect vfi <vfi-id>`

Function: Binds the port to a VPLS instance and configures the AC access mode. The **no** form of this command deletes the binding.

Parameters: <vfi-id>: The VPLS instance ID, ranging from 1 to 4294967295.

svid: The service VLAN ID (outer tag), which specifies the outer VLAN matched by packets.

ethernet: Ethernet access mode.

vlan: VLAN-tagged access mode.

<svid>: The service VLAN ID, ranging from 1 to 4094.

Default: The port is not bound to any VFI; the access mode is VLAN and the default SVID is 0.

Command Mode: Port Mode.

Usage Guidelines: Use this command to bind the port to the specified VFI for VPLS.

Example:

```
Switch(config)#interface Ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#xconnect vfi 100 mode vlan svid 200
```