

Command Line Manual



Content

01-Commands For Basic Switch Configuration	43
1 Commands for Basic Configuration	44
<i>authentication dot1x</i>	44
<i>authentication line</i>	44
<i>banner</i>	45
<i>boot img</i>	45
<i>boot startup-config</i>	46
<i>clock set</i>	47
<i>config</i>	47
<i>disable</i>	48
<i>enable</i>	48
<i>enable password</i>	49
<i>end</i>	50
<i>exec-timeout</i>	50
<i>exit</i>	51
<i>help</i>	51
<i>hostname</i>	52
<i>ip host</i>	52
<i>ipv6 host</i>	53
<i>ip http server</i>	54
<i>login</i>	54
<i>password</i>	55
<i>privilege</i>	55
<i>reload</i>	56
<i>service advanced-vty</i>	56
<i>service password-encryption</i>	57
<i>set default</i>	57
<i>service terminal-length</i>	58
<i>sysContact</i>	59
<i>sysLocation</i>	59
<i>set boot password</i>	60
<i>setup</i>	60
<i>show clock</i>	61
<i>show cpu usage</i>	61
<i>show cpu utilization</i>	62
<i>show cpu monitor</i>	62
<i>show memory usage</i>	63
<i>show privilege</i>	64
<i>show privilege mode LINE</i>	64
<i>show tech-support</i>	65
<i>show version</i>	65
<i>username</i>	66
<i>web-auth privilege <1-15></i>	67
<i>write</i>	67
<i>write running-config</i>	68

2 Commands for Telnet	69
aaa authorization config-commands.....	69
accounting exec	69
accounting command	70
authentication enable	71
authentication ip access-class.....	72
authentication ipv6 access-class.....	72
authentication line login.....	73
authentication securityip.....	74
authentication securityipv6	74
authorization	75
authorization line vty command	76
clear line vty <0-31>.....	77
crypto key clear rsa	77
terminal length	78
telnet	78
telnet server enable	79
telnet-server max-connection	80
ssh-server authentication-retries.....	80
ssh-server enable	81
ssh-server host-key create rsa	81
ssh-server max-connection	82
ssh-server timeout.....	82
show crypto key	83
show ssh-server	83
show telnet login	84
show users.....	84
who.....	85
3 Commands for Configuring Switch IP	85
interface vlan.....	86
ip address.....	86
ipv6 address.....	87
ip bootp-client enable.....	88
ip dhcp-client enable.....	88
4 Commands for SNMP	90
rmon enable.....	90
show private-mib oid.....	90
show snmp.....	91
show snmp engineid	91
show snmp group	92
show snmp mib.....	92
show snmp status.....	93
show snmp user.....	93
show snmp view.....	94
snmp-server community.....	94
snmp-server enable.....	95
snmp-server enable traps	96

<i>snmp-server engineid</i>	97
<i>snmp-server group</i>	97
<i>snmp-server host</i>	98
<i>snmp-server securityip</i>	99
<i>snmp-server securityip enable</i>	100
<i>snmp-server trap-source</i>	100
<i>snmp-server user</i>	101
<i>snmp-server view</i>	102
<i>switchport updown notification enable</i>	103
5 Commands for Switch Upgrade	104
<i>copy (FTP)</i>	104
<i>copy (TFTP)</i>	105
<i>ftp-dir</i>	106
<i>ftp-server enable</i>	107
<i>ftp-server timeout</i>	107
<i>ip ftp</i>	108
<i>show ftp</i>	108
<i>show tftp</i>	109
<i>tftp-server enable</i>	109
<i>tftp-server retransmission-number</i>	110
<i>tftp-server transmission-timeout</i>	110
6 Commands for File System	112
<i>cd</i>	112
<i>copy</i>	112
<i>delete</i>	113
<i>dir</i>	114
<i>pwd</i>	114
<i>rename</i>	115
7 Commands for Mqtt Configuration	115
<i>ip mqtt client</i>	115
<i>ip mqtt server auto</i>	116
<i>ip mqtt server session-timeout</i>	116
<i>ip mqtt server domain</i>	117
<i>ip mqtt server</i>	117
<i>debug mqtt</i>	118
<i>show ip mqtt</i>	118
8 Commands for Netconf	119
<i>debug netconf</i>	119
<i>debug netconf notification</i>	119
<i>netconf enable</i>	120
<i>show netconf yang</i>	121
<i>show netconf-database yang WORD</i>	121
9 Commands for Packet Capture	122
<i>packet-capture setup buffer-size</i>	122
<i>packet-capture setup packet-num</i>	122
<i>packet-capture setup timeout</i>	123
<i>packet-capture setup file</i>	123

no packet-capture setup	124
packet-capture acl rule	124
packet-capture cpu rule.....	125
packet-capture point.....	125
packet-capture start.....	126
packet-capture stop.....	127
10 Commands for DNSv4/v6	127
clear dynamic-host.....	127
debug dns.....	128
dns-server.....	128
dns lookup	129
ip domain-lookup	130
ip domain-list.....	130
ip dns server.....	131
ip dns server queue maximum	131
ip dns server queue timeout.....	132
show dns name-server.....	132
show dns domain-list.....	133
show dns hosts.....	133
show dns config.....	134
show dns client.....	135
11 Commands for MDNS	135
mdns gateway enable.....	135
mdns gateway policy WORD.....	136
mdns gateway probe interval <60-38400>.....	136
mdns gateway source ip A.B.C.D.....	137
mdns relay gateway ip.....	137
mdns relay enable.....	138
mdns relay probe interval.....	139
mdns relay source ip	139
policy enable	140
service vlan vlan-id	141
show mdns gateway policy table.....	141
show mdns gateway cache	142
show mdns relay.....	142
show mdns relay statistics	143
user vlan vlan-id	143
02- Port Module Command Line Manual.....	145
1 Commands for Ethernet Port Configuration	146
bandwidth	146
clear counters interface	146
description	147
fec.....	147
flow control.....	148
interface ethernet.....	149
Loopback.....	149
Negotiation.....	150

<i>Port-rate-statistics interval</i>	150
<i>rate-violation</i>	151
<i>rate-violation control</i>	152
<i>show interface</i>	152
<i>shutdown</i>	153
<i>speed-duplex</i>	154
<i>storm-control</i>	154
<i>storm-control</i>	155
<i>storm-control bypass</i>	156
<i>virtual-cable-test</i>	156
<i>switchport discard packet</i>	157
<i>switchport flood-control</i>	158
<i>switchport flood-forwarding</i>	159
2 Commands for Port Isolation Function	159
<i>isolate-port group</i>	159
<i>isolate-port group switchport interface</i>	160
<i>isolate-port apply</i>	160
<i>show isolate-port group</i>	161
3 Commands for Port Loopback Detection Function	161
<i>loopback-detection control</i>	162
<i>loopback-detection control-recovery timeout</i>	162
<i>loopback-detection interval-time</i>	163
<i>loopback-detection specified-vlan</i>	163
<i>show loopback-detection</i>	164
5 Commands for LLDP Function	164
<i>clear lldp remote-table</i>	164
<i>lldp enable</i>	165
<i>lldp enable (port)</i>	165
<i>lldp management-address tlv</i>	166
<i>lldp mode</i>	166
<i>lldp msgTxHold</i>	167
<i>lldp neighbors max-num</i>	167
<i>lldp notification interval</i>	168
<i>lldp tooManyNeighbors</i>	168
<i>lldp transmit delay</i>	169
<i>lldp transmit optional tlv</i>	169
<i>lldp trap</i>	170
<i>lldp tx-interval</i>	170
<i>lldp dot1 pvid</i>	171
<i>lldp dot1 vlan-name</i>	172
<i>lldp dot3</i>	172
<i>show debugging lldp</i>	173
<i>show lldp</i>	173
<i>show lldp neighbors brif</i>	174
<i>show lldp interface ethernet</i>	175
<i>show lldp neighbors interface ethernet</i>	175
<i>show lldp traffic</i>	176

6 Commands for Port Channel	177
<i>interface port-channel.....</i>	<i>177</i>
<i>lacp port-priority.....</i>	<i>177</i>
<i>lacp system-priority.....</i>	<i>178</i>
<i>lacp timeout.....</i>	<i>178</i>
<i>port-group.....</i>	<i>179</i>
<i>port-group mode.....</i>	<i>179</i>
<i>show port-group.....</i>	<i>180</i>
7 Commands for MTU	181
<i>mtu</i>	<i>181</i>
<i>ip mtu.....</i>	<i>181</i>
8 Commands for EFM OAM.....	182
<i>clear ethernet-oam.....</i>	<i>182</i>
<i>ethernet-oam</i>	<i>182</i>
<i>ethernet-oam errored-frame threshold high.....</i>	<i>183</i>
<i>ethernet-oam errored-frame threshold low</i>	<i>183</i>
<i>ethernet-oam errored-frame window.....</i>	<i>184</i>
<i>ethernet-oam errored-frame-seconds threshold high</i>	<i>184</i>
<i>ethernet-oam errored-frame-seconds threshold Low.....</i>	<i>185</i>
<i>ethernet-oam errored-frame-seconds window.....</i>	<i>185</i>
<i>ethernet-oam errored-symbol-period threshold High.....</i>	<i>186</i>
<i>ethernet-oam errored-symbol-period threshold Low.....</i>	<i>187</i>
<i>ethernet-oam errored-symbol-period window.....</i>	<i>187</i>
<i>ethernet-oam link-monitor</i>	<i>188</i>
<i>ethernet-oam mode.....</i>	<i>188</i>
<i>ethernet-oam period.....</i>	<i>189</i>
<i>ethernet-oam remote-failure</i>	<i>189</i>
<i>ethernet-oam remote-loopback.....</i>	<i>190</i>
<i>ethernet-oam remote-loopback supported.....</i>	<i>190</i>
<i>ethernet-oam timeout.....</i>	<i>191</i>
<i>show ethernet-oam.....</i>	<i>191</i>
<i>show ethernet-oam events.....</i>	<i>192</i>
<i>show ethernet-oam link-events-configuration.....</i>	<i>193</i>
<i>show ethernet-oam loopback status.....</i>	<i>194</i>
9 Commands for PORT SECURITY	194
<i>clear port-security.....</i>	<i>194</i>
<i>show port-security.....</i>	<i>195</i>
<i>switchport port-security.....</i>	<i>195</i>
<i>switchport port-security mac-address</i>	<i>196</i>
<i>switchport port-security maximum.....</i>	<i>196</i>
<i>switchport port-security violation.....</i>	<i>197</i>
10 Commands for DDM	198
<i>clear transceiver threshold-violation</i>	<i>198</i>
<i>show transceiver</i>	<i>198</i>
<i>show transceiver threshold-violation</i>	<i>199</i>
<i>transceiver-monitoring.....</i>	<i>200</i>
<i>transceiver-monitoring interval.....</i>	<i>200</i>

transceiver threshold.....	201
11 Commands for LLDP-MED	202
civic location.....	202
{description-language province-state city county street locationNum location floor room postal otherInfo}.....	202
ecs location.....	203
lldp med device type endpoint.....	204
lldp med fast count.....	204
lldp med trap.....	205
lldp transmit med tlv all.....	205
lldp transmit med tlv capability	206
lldp transmit med tlv extendPoe	206
lldp transmit med tlv location	207
lldp transmit med tlv inventory.....	207
lldp transmit med tlv networkPolicy.....	208
network policy	208
show lldp	210
show lldp [interface ethernet <IFNAME>].....	210
show lldp neighbors	211
show lldp traffic.....	212
12 Commands for bpdu-tunnel	212
bpdu-tunnel-protocol.....	212
bpdu-tunnel-protocol group-mac.....	213
bpdu-tunnel-protocol protocol-mac	214
bpdu-tunnel-protocol ethernetii.....	214
bpdu-tunnel-protocol snap	215
bpdu-tunnel-protocol llc.....	216
13 Commands for EEE Energy-saving	217
eee enable.....	217
14 Commands for port-split	217
port-split.....	217
show port-split.....	219
03-MAC Address	220
1 MAC Address Table	221
clear collision-mac-address-table	221
clear mac-address-table dynamic.....	221
mac-address-learning enable disable	222
mac-address-table aging-time.....	222
mac-address-table static dynamic blackhole.....	223
mac-address-table static-multicast address.....	224
show collision-mac-address-table	224
show mac-address-table.....	225
show mac-address-table multicast.....	226
clear mac-notification statistics.....	226
mac-address-table notification.....	226
mac-address-table notification history-size	227
mac-address-table notification interval.....	227

<i>mac-notification</i>	227
<i>show mac-notification summary</i>	228
<i>snmp-server enable traps mac-notification</i>	229
04-Commands for VLAN Configuration	230
1 VLAN	231
<i>vlan</i>	231
<i>name (vlan)</i>	232
<i>switchport interface</i>	232
<i>switchport forbidden vlan</i>	233
<i>switchport mode</i>	235
<i>switchport hybrid native vlan</i>	236
<i>switchport hybrid allowed vlan</i>	237
<i>switchport access vlan</i>	238
<i>switchport trunk allowed vlan</i>	238
<i>switchport trunk native vlan</i>	239
<i>switchport mode trunk allow-null</i>	240
<i>vlan ingress enable</i>	240
<i>vlan-translation enable</i>	241
<i>vlan-translation</i>	242
<i>vlan-translation miss drop</i>	242
<i>dot1q-tunnel enable</i>	243
<i>dot1q-tunnel selective enable</i>	244
<i>dot1q-tunnel selective s-vlan</i>	245
<i>garp timer join</i>	246
<i>garp timer leave</i>	247
<i>garp timer leaveall</i>	247
<i>no garp timer</i>	248
<i>gvrp(Global)</i>	248
<i>gvrp(Port)</i>	249
<i>private-vlan</i>	250
<i>private-vlan association</i>	251
<i>show dot1q-tunnel</i>	252
<i>show garp timer</i>	252
<i>show gvrp fsm information</i>	253
<i>show gvrp leaveAll fsm information</i>	253
<i>show gvrp leavetimer running information</i>	254
<i>show gvrp port-member</i>	254
<i>show gvrp port registerd vlan</i>	255
<i>show gvrp timer running information</i>	255
<i>show gvrp vlan registerd port</i>	256
<i>show vlan</i>	256
<i>show vlan-translation</i>	257
<i>vlan-translation n-to-1</i>	257
<i>dynamic-vlan mac-vlan prefer</i>	258
<i>dynamic-vlan subnet-vlan prefer</i>	259
<i>mac-vlan vlan</i>	259
<i>mac-vlan</i>	260

<i>protocol-vlan</i>	261
<i>show dynamic-vlan prefer</i>	261
<i>show mac-vlan interface</i>	262
<i>show protocol-vlan</i>	262
<i>show subnet-vlan</i>	263
<i>show subnet-vlan interface</i>	263
<i>subnet-vlan</i>	264
<i>switchport mac-vlan enable</i>	265
<i>switchport subnet-vlan enable</i>	265
<i>show voice-vlan</i>	266
<i>switchport voice-vlan enable</i>	267
<i>voice-vlan</i>	267
<i>voice-vlan vlan</i>	269
05-Commands for Anti-ring Protocol	270
1 Commands for MSTP	227
<i>abort</i>	227
<i>exit</i>	227
<i>instance vlan</i>	227
<i>Name</i>	228
<i>revision-level</i>	228
<i>spanning-tree</i>	229
<i>spanning-tree tc-guard</i>	229
<i>spanning-tree bpdu</i>	230
<i>spanning-tree cost</i>	230
<i>spanning-tree digest-snooping</i>	231
<i>spanning-tree format</i>	232
<i>spanning-tree forward-time</i>	233
<i>spanning-tree hello-time</i>	233
<i>spanning-tree link-type p2p</i>	234
<i>spanning-tree maxage</i>	234
<i>spanning-tree max-hop</i>	235
<i>spanning-tree mcheck</i>	235
<i>spanning-tree mode</i>	236
<i>spanning-tree mst configuration</i>	236
<i>spanning-tree mst cost</i>	237
<i>spanning-tree cost-format</i>	239
<i>spanning-tree mst loopguard</i>	239
<i>spanning-tree mst port-priority</i>	240
<i>spanning-tree mst priority</i>	240
<i>spanning-tree mst rootguard</i>	241
<i>spanning-tree portfast</i>	241
<i>spanning-tree port-priority</i>	242
<i>spanning-tree priority</i>	242
<i>spanning-tree rootguard</i>	243
<i>spanning-tree tcflush (Global mode)</i>	243
<i>spanning-tree tcflush (Port mode)</i>	244
<i>spanning-tree transmit-hold-count</i>	245

<i>show mst-pending</i>	245
<i>show spanning-tree</i>	246
<i>show spanning-tree mst config</i>	248
<i>spanning-tree process</i>	248
<i>spanning-tree tc-notify process0</i>	248
<i>spanning-tree binding-process</i>	249
<i>spanning-tree binding-process link-share</i>	249
2 ERPS Configuration	250
<i>ethernet tcn-propagation erps to {erps stp}</i>	250
<i>erps-ring <ring-name></i>	251
<i>version {v1 v2}</i>	251
<i>open-ring</i>	252
<i>raps-virtual-channel {with without}</i>	252
<i>erps-ring <ring-name> port0 [port1-none]</i>	253
<i>erps-ring <ring-name> port1</i>	254
<i>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></i>	254
<i>erps-instance <instance-id></i>	255
<i>description</i>	256
<i>ring-id <ring-id></i>	257
<i>rpl {port0 port1} {owner neighbour}</i>	257
<i>non-revertive</i>	258
<i>guard-timer <guard-times></i>	258
<i>holdoff-timer < holdoff-times></i>	259
<i>wtr-timer <wtr-times></i>	259
<i>protected-instance</i>	260
<i>raps-mel <level-value></i>	260
<i>control-vlan <vlan-id></i>	261
<i>forced-switch {port0 port1}</i>	261
<i>manual-switch {port0 port1}</i>	262
<i>clear command</i>	263
<i>show erps ring {<ring-name> brief}</i>	264
<i>show erps instance [ring <ring-name> [instance <instance-id>]]</i>	264
<i>show erps status [ring <ring-name> [instance <instance-id>]]</i>	265
<i>show erps statistics [ring <ring-name> [instance <instance-id>]]</i>	267
<i>clear erps statistics [ring <ring-name> [instance <instance-id>]]</i>	268
06-Commands for QOS	269
1 QOS	270
<i>accounting</i>	270
<i>access-group redirect to interface ethernet</i>	270
<i>apply tail-drop-profile</i>	271
<i>class</i>	271
<i>class-map</i>	272
<i>clear mls qos statistics</i>	272
<i>drop</i>	273
<i>match</i>	273
<i>mls qos aggregate-policy</i>	274

<i>mls qos cos</i>	276
<i>mls qos map</i>	276
<i>mls qos queue depth</i>	278
<i>mls qos queue apply scheduling-profile</i>	279
<i>mls qos queue cir</i>	279
<i>mls qos trust</i>	280
<i>mls qos egress conform-action</i>	280
<i>Policy</i>	281
<i>Policy aggregate</i>	282
<i>Policy-map</i>	283
<i>priority-flow-control [queue <0-7>] enable [receive/send]</i>	283
<i>priority-flow-control queue <0-7> static-threshold <0-196608> dynamic-threshold <0-11></i>	284
<i>scheduling-profile</i>	284
<i>service-policy input</i>	285
<i>service-policy input vlan</i>	285
<i>service-policy output</i>	286
<i>service-policy output vlan</i>	286
<i>set</i>	287
<i>set-queue</i>	287
<i>show class-map</i>	288
<i>show policy-map</i>	288
<i>show priority-flow-control (interface ethernet IFNAME)</i>	289
<i>show scheduling-profile (interface ethernet IFNAME)</i>	290
<i>show tail-drop (interface ethernet IFNAME)</i>	291
<i>show mls qos interface</i>	291
<i>show mls qos in (interface <interface-name> policy) (vlan <vlan-id>)</i>	293
<i>show mls qos maps</i>	294
<i>show mls qos vlan</i>	296
<i>show mls qos aggregate-policy</i>	296
<i>show mls qos out (interface <interface-name> policy) (vlan <vlan-id>)</i>	297
<i>tail-drop-profile ecn</i>	297
<i>tail-drop-profile</i>	298
<i>tail-drop-wred-profile</i>	298
<i>tail-drop-wrtd-profile</i>	299
<i>transmit</i>	300
<i>show flow-based-redirect</i>	300
07-Commands for Layer 3 Forward and ARP	301
1 Commands for Layer 3 Interface	302
<i>description</i>	302
<i>interface vlan</i>	302
<i>no interface IFNAME</i>	303
<i>show ip route</i>	303
2 Commands for IPv4/v6 configuration	304
<i>clear ip traffic</i>	304
<i>clear ipv6 neighbor</i>	304
<i>ip address</i>	305
<i>ipv6 address</i>	305

<i>ipv6 nd dad attempts</i>	306
<i>ipv6 nd ns-interval</i>	307
<i>ipv6 neighbor</i>	307
<i>show ip interface</i>	308
<i>show ip traffic</i>	308
<i>show ipv6 interface</i>	310
<i>show ipv6 route</i>	311
<i>show ipv6 neighbors</i>	312
<i>show ipv6 traffic</i>	313
<i>ip route</i>	314
3 Commands for ARP Configuration	315
<i>arp</i>	315
<i>clear arp-cache</i>	316
<i>clear arp traffic</i>	316
<i>show arp</i>	316
<i>show arp traffic</i>	317
4 Commands for ARP Scanning Prevention	318
<i>anti-arpscan enable</i>	318
<i>anti-arpscan port-based threshold</i>	318
<i>anti-arpscan ip-based threshold</i>	319
<i>anti-arpscan trust</i>	319
<i>anti-arpscan trust ip</i>	320
<i>anti-arpscan recovery enable</i>	320
<i>anti-arpscan recovery time</i>	321
<i>anti-arpscan log enable</i>	321
<i>anti-arpscan trap enable</i>	322
<i>show anti-arpscan</i>	322
5 Commands for Preventing ARP Spoofing	323
<i>ip arp-security updateprotect</i>	323
<i>ip arp-security learnprotect</i>	324
<i>ip arp-security convert</i>	324
<i>clear ip arp dynamic</i>	325
<i>clear ipv6 nd dynamic</i>	325
6 Command for ARP GUARD	325
<i>arp-guard ip</i>	325
7 Commands for Gratuitous ARP Configuration	326
<i>ip gratuitous-arp</i>	326
<i>show ip gratuitous-arp</i>	327
8 Commands for Dynamic ARP Inspection	327
<i>ip arp inspection</i>	327
<i>ip arp inspection trust</i>	328
<i>ip arp inspection limit-rate</i>	328
08-Commands for DHCP	330
1 DHCP	331
<i>bootfile</i>	331
<i>clear ip dhcp binding</i>	331
<i>clear ip dhcp conflict</i>	332

<i>clear ip dhcp server statistics</i>	332
<i>client-identifier</i>	332
<i>default-router</i>	333
<i>dns-server</i>	333
<i>domain-name</i>	334
<i>hardware-address</i>	334
<i>host</i>	335
<i>ip dhcp conflict logging</i>	335
<i>ip dhcp disable</i>	336
<i>ip dhcp excluded-address</i>	336
<i>ip dhcp pool</i>	337
<i>ip dhcp conflict ping-detection enable</i>	337
<i>ip dhcp ping packets</i>	337
<i>ip dhcp ping timeout</i>	338
<i>lease</i>	338
<i>max-lease-time</i>	339
<i>netbios-name-server</i>	339
<i>netbios-node-type</i>	340
<i>network-address</i>	340
<i>next-server</i>	341
<i>option</i>	341
<i>service dhcp</i>	342
<i>show ip dhcp binding</i>	342
<i>show ip dhcp conflict</i>	343
<i>show ip dhcp relay information option</i>	343
<i>show ip dhcp server statistics</i>	344
<i>ip dhcp broadcast suppress</i>	345
<i>ip dhcp relay share-vlan <vlanid> sub-vlan <vlanlist></i>	345
<i>ip forward-protocol udp bootps</i>	346
<i>ip helper-address</i>	346
<i>show ip forward-protocol</i>	347
<i>show ip helper-address</i>	347
<i>clear ipv6 dhcp binding</i>	347
<i>clear ipv6 dhcp conflict</i>	348
<i>clear ipv6 dhcp statistics</i>	348
<i>dns-server</i>	348
<i>domain-name</i>	349
<i>excluded-address</i>	349
<i>ipv6 address</i>	350
<i>ipv6 dhcp client pd</i>	350
<i>ipv6 dhcp client pd hint</i>	351
<i>ipv6 dhcp pool</i>	351
<i>ipv6 dhcp relay destination</i>	352
<i>ipv6 dhcp server</i>	352
<i>ipv6 general-prefix</i>	353
<i>ipv6 local pool</i>	354
<i>lifetime</i>	354

<i>network-address</i>	355
<i>prefix-delegation</i>	355
<i>prefix-delegation pool</i>	356
<i>service dhcpv6</i>	357
<i>show ipv6 dhcp</i>	357
<i>show ipv6 dhcp binding</i>	357
<i>show ipv6 dhcp conflict</i>	358
<i>show ipv6 dhcp interface</i>	358
<i>show ipv6 dhcp pool</i>	359
<i>show ipv6 dhcp statistics</i>	359
<i>show ipv6 general-prefix</i>	360
<i>show ipv6 local pool</i>	361
<i>ip dhcp relay information option</i>	361
<i>ip dhcp relay information option delimiter</i>	362
<i>ip dhcp relay information option remote-id</i>	362
<i>ip dhcp relay information option remote-id format</i>	362
<i>ip dhcp relay information option self-defined remote-id</i>	363
<i>ip dhcp relay information option self-defined remote-id format</i>	364
<i>ip dhcp relay information option self-defined subscriber-id</i>	364
<i>ip dhcp relay information option self-defined subscriber-id format</i>	365
<i>ip dhcp relay information option subscriber-id</i>	365
<i>ip dhcp relay information option subscriber-id format</i>	365
<i>ip dhcp relay information policy</i>	366
<i>ip dhcp server relay information enable</i>	367
<i>show ip dhcp relay information option</i>	367
<i>option 43 ascii LINE</i>	368
<i>option 43 hex WORD</i>	368
<i>option 43 ip A.B.C.D</i>	369
<i>option 60 ascii LINE</i>	369
<i>option 60 hex WORD</i>	370
<i>option 60 ip A.B.C.D</i>	370
<i>address range</i>	370
<i>class</i>	371
<i>ipv6 dhcp class</i>	371
<i>ipv6 dhcp relay remote-id</i>	372
<i>ipv6 dhcp relay remote-id option</i>	372
<i>ipv6 dhcp relay subscriber-id</i>	373
<i>ipv6 dhcp relay subscriber-id option</i>	373
<i>ipv6 dhcp relay subscriber-id select delimiter</i>	374
<i>ipv6 dhcp server remote-id option</i>	374
<i>ip dhcp server select relay-forw</i>	375
<i>ipv6 dhcp server subscriber-id option</i>	375
<i>ipv6 dhcp snooping information option remote-id format</i>	376
<i>ipv6 dhcp snooping information option subscriber-id format</i>	376
<i>ipv6 dhcp snooping remote-id</i>	377
<i>ipv6 dhcp snooping remote-id option</i>	377
<i>ipv6 dhcp snooping remote-id policy</i>	378

<i>ipv6 dhcp snooping subscriber-id</i>	378
<i>ipv6 dhcp snooping subscriber-id optionen</i>	379
<i>ipv6 dhcp snooping subscriber-id policy</i>	379
<i>ipv6 dhcp snooping subscriber-id select delimiter</i>	380
<i>ipv6 dhcp use class</i>	380
<i>remote-id subscriber-id</i>	381
<i>show ipv6 dhcp relay option</i>	381
<i>show ipv6 dhcp snooping option</i>	382
<i>enable trustview key</i>	382
<i>ip dhcp snooping</i>	382
<i>ip dhcp snooping action</i>	383
<i>ip dhcp snooping action MaxNum</i>	383
<i>ip dhcp snooping binding</i>	384
<i>ip dhcp snooping binding dot1x</i>	384
<i>ip dhcp snooping binding user</i>	385
<i>ip dhcp snooping binding user-control</i>	385
<i>ip dhcp snooping binding user-control max-user</i>	386
<i>ip dhcp snooping information enable</i>	386
<i>ip dhcp snooping information option allow-untrusted (replace)</i>	387
<i>ip dhcp snooping information option delimiter</i>	387
<i>ip dhcp snooping information option remote-id</i>	388
<i>ip dhcp snooping information option self-defined remote-id</i>	388
<i>ip dhcp snooping information option self-defined remote-id format</i>	389
<i>ip dhcp snooping information option self-defined subscriber-id</i>	389
<i>ip dhcp snooping information option self-defined subscriber-id format</i>	390
<i>ip dhcp snooping information option subscriber-id</i>	390
<i>ipv6 dhcp snooping information option subscriber-id format</i>	391
<i>ip dhcp snooping limit-rate</i>	391
<i>ip dhcp snooping trust</i>	392
<i>ip dhcp snooping vlan</i>	392
<i>ip user helper-address</i>	393
<i>ip user private packet version two</i>	394
<i>show ip dhcp snooping</i>	394
<i>show ip dhcp snooping binding all</i>	396
<i>show trustview status</i>	396
<i>ip dhcp snooping information enable</i>	397
<i>ip dhcp snooping timeout quiet</i>	397
<i>ip dhcp snooping timeout detection</i>	398
<i>ip dhcp snooping mac-base control pass</i>	398
<i>ip dhcp snooping blocked record enable</i>	398
09-Multicast Protocol	400
1 IPv4 Multicast	401
<i>access-list (Multicast Destination Control)</i>	401
<i>access-list (Multicast Source Control)</i>	402
<i>ip multicast destination-control access-group</i>	402
<i>ip multicast destination-control access-group (sip)</i>	403
<i>ip multicast destination-control access-group (vmac)</i>	403

<i>ip multicast policy</i>	404
<i>ip multicast source-control</i>	404
<i>ip multicast source-control access-group</i>	405
<i>ip multicast destination-control</i>	405
<i>profile-id (Multicast Destination Control Rule List)</i>	405
<i>show ip multicast destination-control</i>	406
<i>show ip multicast destination-control access-list</i>	407
<i>show ip multicast destination-control filter-profile-list</i>	407
<i>show ip multicast policy</i>	407
<i>show ip multicast source-control</i>	408
<i>show ip multicast source-control access-list</i>	408
<i>clear ip igmp snooping vlan</i>	408
<i>clear ip igmp snooping vlan <1-4094> mrouter-port</i>	409
<i>ip igmp snooping</i>	409
<i>ip igmp snooping proxy</i>	410
<i>ip igmp snooping vlan</i>	410
<i>ip igmp snooping vlan immediate-leave</i>	410
<i>ip igmp snooping vlan <id> immediately-leave mac-based</i>	411
<i>ip igmp snooping vlan l2-general-querier</i>	411
<i>ip igmp snooping vlan l2-general-querier-source</i>	412
<i>ip igmp snooping vlan l2-general-querier-version</i>	412
<i>ip igmp snooping vlan limit</i>	413
<i>ip igmp snooping vlan interface (ethernet port-channel) IFNAME limit</i>	413
<i>ip igmp snooping vlan mrouter-port interface</i>	414
<i>ip igmp snooping vlan mrouter-port learnpim</i>	414
<i>ip igmp snooping vlan mrpt</i>	414
<i>ip igmp snooping vlan query-interval</i>	415
<i>ip igmp snooping vlan query-mrsp</i>	415
<i>ip igmp snooping vlan query-robustness</i>	416
<i>ip igmp snooping vlan report source-address</i>	416
<i>ip igmp snooping vlan specific-query-mrsp</i>	416
<i>ip igmp snooping vlan static-group</i>	417
<i>ip igmp snooping vlan suppression-query-time</i>	417
<i>show ip igmp snooping</i>	418
<i>clear ipv6 mld snooping vlan</i>	419
<i>clear ipv6 mld snooping vlan <1-4094> mrouter-port</i>	419
<i>ipv6 mld snooping</i>	420
<i>ipv6 mld snooping vlan</i>	420
<i>ipv6 mld snooping vlan immediate-leave</i>	421
<i>ipv6 mld snooping vlan l2-general-querier</i>	421
<i>ipv6 mld snooping vlan limit</i>	422
<i>ipv6 mld snooping vlan mrouter-port interface</i>	422
<i>ipv6 mld snooping vlan mrouter-port learnpim6</i>	422
<i>ipv6 mld snooping vlan mrpt</i>	423
<i>ipv6 mld snooping vlan query-interval</i>	423
<i>ipv6 mld snooping vlan query-mrsp</i>	424
<i>ipv6 mld snooping vlan query-robustness</i>	424

<i>ipv6 mld snooping vlan static-group</i>	424
<i>ipv6 mld snooping vlan suppression-query-time</i>	425
<i>show ipv6 mld snooping</i>	425
<i>multicast-vlan</i>	427
<i>multicast-vlan association</i>	427
<i>multicast-vlan association interface</i>	428
<i>multicast-vlan mode</i>	428
<i>switchport association multicast-vlan</i>	429
2 IGMP	430
<i>show ip mroute</i>	430
<i>show ipv6 mroute</i>	431
<i>clear ip igmp group</i>	432
<i>debug igmp event</i>	433
<i>debug igmp packet</i>	433
<i>ip igmp access-group</i>	434
<i>ip igmp immediate-leave</i>	434
<i>ip igmp join-group</i>	435
<i>ip igmp last-member-query-interval</i>	435
<i>ip igmp limit</i>	436
<i>ip igmp query-interval</i>	437
<i>ip igmp query-max-response-time</i>	437
<i>ip igmp query-timeout</i>	438
<i>ip igmp robust-variable</i>	438
<i>ip igmp static-group</i>	439
<i>ip igmp version</i>	439
<i>show ip igmp groups</i>	440
<i>show ip igmp interface</i>	441
3 PIM-DM	442
<i>debug pim timer sat</i>	442
<i>debug pim timer srt</i>	443
<i>ip mroute</i>	443
<i>ip pim bsr-border</i>	444
<i>ip pim dense-mode</i>	444
<i>ip pim dr-priority</i>	445
<i>ip pim exclude-genid</i>	445
<i>ip pim hello-holdtime</i>	446
<i>ip pim hello-interval</i>	446
<i>ip pim multicast-routing</i>	447
<i>ip pim neighbor-filter</i>	447
<i>ip pim scope-border</i>	448
<i>ip pim state-refresh origination-interval</i>	448
<i>show ip pim interface</i>	449
<i>show ip pim mroute dense-mode</i>	450
<i>show ip pim neighbor</i>	451
<i>show ip pim nexthop</i>	452
4 PIM-SM	453
<i>clear ip pim bsr rp-set</i>	453

<i>debug pim event</i>	453
<i>debug pim mfc</i>	454
<i>debug pim mib</i>	454
<i>debug pim nexthop</i>	455
<i>debug pim nsm</i>	455
<i>debug pim packet</i>	456
<i>debug pim state</i>	456
<i>debug pim packet</i>	457
<i>ip mroute</i>	458
<i>ip multicast unresolved-cache aging-time</i>	459
<i>ip pim accept-register</i>	459
<i>ip pim bsr-border</i>	459
<i>ip pim bsr-candidate</i>	460
<i>ip pim cisco-register-checksum</i>	461
<i>ip pim dr-priority</i>	461
<i>ip pim exclude-genid</i>	462
<i>ip pim hello-holdtime</i>	462
<i>ip pim hello-interval</i>	463
<i>ip pim ignore-rp-set-priority</i>	463
<i>ip pim jp-timer</i>	464
<i>ip pim multicast-routing</i>	464
<i>ip pim neighbor-filter</i>	465
<i>ip pim register-rate-limit</i>	465
<i>ip pim register-rp-reachability</i>	466
<i>ip pim register-source</i>	466
<i>ip pim register-suppression</i>	467
<i>ip pim rp-address</i>	468
<i>ip pim rp-candidate</i>	468
<i>ip pim rp-register-kat</i>	469
<i>ip pim scope-border</i>	469
<i>ip pim sparse-mode</i>	470
<i>show ip pim bsr-router</i>	470
<i>show ip pim interface</i>	471
<i>show ip pim mroute sparse-mode</i>	471
<i>show ip pim neighbor</i>	473
<i>show ip pim nexthop</i>	474
<i>show ip pim rp-hash</i>	475
<i>show ip pim rp mapping</i>	475
5 PIM-SSM	476
<i>ip multicast ssm</i>	476
6 PIM-DM6	477
<i>debug ipv6 pim timer sat</i>	477
<i>debug ipv6 pim timer srt</i>	477
<i>ipv6 mroute</i>	478
<i>ipv6 pim bsr-border</i>	478
<i>ipv6 pim dense-mode</i>	479
<i>ipv6 pim dr-priority</i>	479

<i>ipv6 pim exclude-genid</i>	480
<i>ipv6 pim hello-holdtime</i>	480
<i>ipv6 pim hello-interval</i>	481
<i>ipv6 pim multicast-routing</i>	481
<i>ipv6 pim neighbor-filter</i>	482
<i>ipv6 pim scope-border</i>	482
<i>ipv6 pim state-refresh origination-interval</i>	483
<i>show ipv6 pim interface</i>	483
<i>show ipv6 pim mroute dense-mode</i>	484
<i>show ipv6 pim neighbor</i>	486
<i>show ipv6 pim nexthop</i>	486
7 PIM-SM6	487
<i>clear ipv6 pim bsr rp-set</i>	487
<i>debug ipv6 pim event</i>	488
<i>debug ipv6 pim mfc</i>	488
<i>debug ipv6 pim mib</i>	489
<i>debug ipv6 pim nexthop</i>	489
<i>debug ipv6 pim nsm</i>	490
<i>debug ipv6 pim packet</i>	490
<i>debug ipv6 pim state</i>	491
<i>debug ipv6 pim packet</i>	492
<i>ipv6 mroute</i>	493
<i>ipv6 multicast unresolved-cache aging-time</i>	493
<i>ipv6 pim accept-register</i>	494
<i>ipv6 pim bsr-border</i>	494
<i>ipv6 pim bsr-candidate</i>	495
<i>ipv6 pim cisco-register-checksum</i>	495
<i>ipv6 pim dr-priority</i>	496
<i>ipv6 pim exclude-genid</i>	496
<i>ipv6 pim hello-holdtime</i>	497
<i>ipv6 pim hello-interval</i>	497
<i>ipv6 pim ignore-rp-set-priority</i>	498
<i>ipv6 pim jp-timer</i>	499
<i>ipv6 pim multicast-routing</i>	499
<i>ipv6 pim neighbor-filter</i>	499
<i>ipv6 pim register-rate-limit</i>	500
<i>ipv6 pim register-rp-reachability</i>	501
<i>ipv6 pim register-source</i>	501
<i>ipv6 pim register-suppression</i>	502
<i>ipv6 pim rp-address</i>	502
<i>ipv6 pim rp-candidate</i>	503
<i>ipv6 pim rp-register-kat</i>	503
<i>ipv6 pim scope-border</i>	504
<i>ipv6 pim sparse-mode</i>	504
<i>show ipv6 pim bsr-router</i>	505
<i>show ipv6 pim interface</i>	505
<i>show ipv6 pim mroute sparse-mode</i>	506

show ipv6 pim neighbor	507
show ipv6 pim nexthop	508
show ipv6 pim rp-hash.....	509
show ipv6 pim rp mapping.....	509
8 PIM-SSM6	510
ipv6 pim ssm	510
9 ANYCAST RP v4	511
debug pim anycast-rp	511
ip pim anycast-rp	511
ip pim anycast-rp	512
ip pim anycast-rp self-rp-address.....	513
ip pim rp-candidate.....	513
show debugging pim	514
show ip pim anycast-rp first-hop.....	514
show ip pim anycast-rp non-first-hop.....	515
show ip pim anycast-rp status.....	516
10 ANYCAST RP v6	517
debug ipv6 pim anycast-rp	517
ipv6 pim anycast-rp.....	517
ipv6 pim anycast-rp.....	518
ipv6 pim anycast-rp self-rp-address.....	519
ipv6 pim rp-candidate	519
show debugging ipv6 pim.....	520
show ipv6 pim anycast-rp first-hop	520
show ipv6 pim anycast-rp non-first-hop	521
show ipv6 pim anycast-rp status	522
10-Commands for Security Function	524
1 Commands for ACL	525
absolute-periodic/periodic	525
absolute start	526
access-list (ip extended)	527
access-list (ip standard)	529
access-list(mac extended)	529
access-list(mac-ip extended)	530
access-list (mac standard)	533
clear access-group statistic.....	534
firewall	534
ip access extended	535
ip access standard	535
ipv6 access-list	536
ipv6 access standard.....	537
ipv6 access extended.....	537
{ip ipv6 mac mac-ip} access-group	538
mac access extended	539
mac-ip access extended.....	539
permit deny (ip extended).....	540
permit deny (ip standard)	541

<i>permit deny (ipv6 extended)</i>	542
<i>permit deny (ipv6 standard)</i>	544
<i>permit deny (mac extended)</i>	544
<i>permit deny (mac-ip extended)</i>	546
<i>show access-lists</i>	548
<i>show access-group</i>	549
<i>show firewall</i>	549
<i>show ipv6 access-lists</i>	550
<i>show time-range</i>	551
<i>time-range</i>	551
2 Commands for 802.1x	552
<i>dot1x accept-mac</i>	552
<i>dot1x eapor enable</i>	552
<i>dot1x enable</i>	553
<i>dot1x ipv6 passthrough</i>	554
<i>dot1x guest-vlan</i>	554
<i>dot1x macfilter enable</i>	555
<i>dot1x macbased guest-vlan</i>	556
<i>dot1x macbased port-down-flush</i>	557
<i>dot1x max-req</i>	557
<i>dot1x user allow-movement</i>	558
<i>dot1x user free-resource</i>	558
<i>dot1x max-user macbased</i>	559
<i>dot1x max-user userbased</i>	560
<i>dot1x portbased mode single-mode</i>	560
<i>dot1x port-control</i>	561
<i>dot1x port-method</i>	562
<i>dot1x privateclient enable</i>	563
<i>dot1x privateclient protect enable</i>	563
<i>dot1x re-authenticate</i>	564
<i>dot1x re-authentication</i>	564
<i>dot1x timeout quiet-period</i>	565
<i>dot1x timeout re-authperiod</i>	565
<i>dot1x timeout tx-period</i>	566
<i>dot1x unicast enable</i>	566
<i>show dot1x</i>	567
3 Commands for the Number Limitation Function of MAC and IP in Port, VLAN	568
<i>ip arp dynamic maximum</i>	568
<i>ipv6 nd dynamic maximum</i>	569
<i>show arp-dynamic count</i>	570
<i>show mac-address dynamic count</i>	570
<i>show nd-dynamic count</i>	571
<i>switchport arp dynamic maximum</i>	572
<i>switchport mac-address dynamic maximum</i>	573
<i>switchport mac-address violation</i>	573
<i>switchport nd dynamic maximum</i>	574
<i>vlan mac-address dynamic maximum</i>	575

4 Commands for AM Configuration	575
<i>am enable</i>	<i>576</i>
<i>am port.....</i>	<i>576</i>
<i>am ip-pool.....</i>	<i>577</i>
<i>am mac-ip-pool.....</i>	<i>577</i>
<i>no am all.....</i>	<i>578</i>
<i>show am</i>	<i>578</i>
5 Commands for Security Feature.....	579
<i>dosattack-check srcip-equal-dstip enable</i>	<i>579</i>
<i>dosattack-check tcp-flags enable.....</i>	<i>579</i>
<i>dosattack-check srcport-equal-dstport enable</i>	<i>580</i>
6 Commands for TACACS+.....	581
<i>tacacs-server authentication host.....</i>	<i>581</i>
<i>tacacs-server key</i>	<i>582</i>
<i>tacacs-server nas-ipv4</i>	<i>582</i>
<i>tacacs-server timeout</i>	<i>583</i>
7 Commands for RADIUS.....	583
<i>aaa enable.....</i>	<i>584</i>
<i>aaa-accounting enable.....</i>	<i>584</i>
<i>aaa-accounting update.....</i>	<i>585</i>
<i>radius nas-ipv4</i>	<i>585</i>
<i>radius nas-ipv6</i>	<i>586</i>
<i>radius-server accounting host</i>	<i>587</i>
<i>radius-server authentication host.....</i>	<i>588</i>
<i>radius-server dead-time</i>	<i>589</i>
<i>radius-server key</i>	<i>589</i>
<i>radius-server retransmit</i>	<i>590</i>
<i>radius-server timeout</i>	<i>591</i>
<i>radius-server accounting-interim-update timeout.....</i>	<i>591</i>
<i>show aaa authenticated-user.....</i>	<i>592</i>
<i>show aaa authenticating-user</i>	<i>593</i>
<i>show aaa config</i>	<i>593</i>
<i>show radius authenticated-user count.....</i>	<i>594</i>
<i>show radius authenticating-user count</i>	<i>594</i>
8 Commands for SSL Configuration.....	595
<i>ip http secure-server</i>	<i>595</i>
<i>ip http secure-port</i>	<i>595</i>
<i>ip http secure- ciphersuite</i>	<i>596</i>
<i>show ip http secure-server status.....</i>	<i>597</i>
9 Commands for IPv6 Security RA	597
<i>ipv6 security-ra enable</i>	<i>597</i>
<i>ipv6 security-ra enable</i>	<i>598</i>
<i>show ipv6 security-ra</i>	<i>598</i>
10 Commands for MAB	599
<i>authentication mab.....</i>	<i>599</i>
<i>clear mac-authentication-bypass binding</i>	<i>600</i>
<i>mac-authentication-bypass binding-limit</i>	<i>600</i>

<i>mac-authentication-bypass enable</i>	601
<i>mac-authentication-bypass guest-vlan</i>	601
<i>mac-authentication-bypass spoofing-garp-check</i>	602
<i>mac-authentication-bypass timeout linkup-period</i>	603
<i>mac-authentication-bypass timeout offline-detect</i>	603
<i>mac-authentication-bypass timeout quiet-period</i>	604
<i>mac-authentication-bypass timeout reauth-period</i>	604
<i>mac-authentication-bypass timeout stale-period</i>	605
<i>mac-authentication-bypass username-format</i>	606
<i>show mac-authentication-bypass</i>	606
11 Commands for MAB PPPoE Intermediate Agent	607
<i>pppoe intermediate-agent</i>	607
<i>pppoe intermediate-agent (Port)</i>	608
<i>pppoe intermediate-agent circuit-id</i>	608
<i>pppoe intermediate-agent delimiter</i>	609
<i>pppoe intermediate-agent format</i>	609
<i>pppoe intermediate-agent remote-id</i>	610
<i>pppoe intermediate-agent trust</i>	611
<i>pppoe intermediate-agent type self-defined circuit-id</i>	611
<i>pppoe intermediate-agent type self-defined remoteid</i>	612
<i>pppoe intermediate-agent type tr-101 circuit-id access-node-id</i>	612
<i>pppoe intermediate-agent type tr-101 circuit-id identifier-string option delimiter</i>	613
<i>pppoe intermediate-agent vendor-tag strip</i>	614
<i>show pppoe intermediate-agent access-node-id</i>	615
<i>show pppoe intermediate-agent identifier-string option delimiter</i>	615
<i>show pppoe intermediate-agent info</i>	616
12 Commands for VLAN-ACL	616
<i>clear vacl statistic vlan</i>	616
<i>show vacl vlan</i>	617
<i>vacl ip access-group</i>	618
<i>vacl ipv6 access-group</i>	619
<i>vacl mac access-group</i>	619
<i>vacl mac-ip access-group</i>	620
13 Commands for SAVI	621
<i>ipv6 cps prefix</i>	621
<i>ipv6 cps prefix check enable</i>	621
<i>ipv6 dhcp snooping trust</i>	622
<i>ipv6 nd snooping trust</i>	623
<i>savi check binding</i>	623
<i>savi enable</i>	624
<i>savi ipv6 binding num</i>	624
<i>savi ipv6 check source binding</i>	625
<i>savi ipv6 check source ip-address mac-address</i>	626
<i>savi ipv6 {dhcp-only slaac-only dhcp-slaac} enable</i>	627
<i>savi ipv6 mac-binding-limit</i>	627
<i>savi max-dad-dalay</i>	628
<i>savi max-dad-prepare-delay</i>	628

<i>savi max-slaac-life</i>	629
<i>savi timeout bind-protect</i>	629
<i>show savi ipv6 check source binding</i>	630
14 Commands for IPSG	631
<i>ip-source-guard</i>	631
<i>ip-source-guard max-entry</i>	631
<i>ip-source-guard binding</i>	632
<i>clear ip-source-guard binding</i>	632
<i>show ip-source-guard</i>	633
<i>show ip-source-guard binding</i>	633
11-Commands for Reliability	635
1 Commands for MRPP	636
<i>control-vlan</i>	636
<i>clear mrpp statistics</i>	636
<i>enable</i>	637
<i>errp domain</i>	637
<i>fail-timer</i>	638
<i>hello-timer</i>	638
<i>mrpp eaps compatible</i>	639
<i>mrpp enable</i>	639
<i>mrpp errp compatible</i>	640
<i>mrpp poll-time</i>	640
<i>mrpp ring</i>	641
<i>mrpp ring primary-port</i>	641
<i>mrpp ring secondary-port</i>	642
<i>node-mode</i>	642
<i>show mrpp</i>	643
<i>show mrpp statistics</i>	643
2 Commands for ULPP	643
<i>clear ulpp flush counter interface</i>	644
<i>control vlan</i>	644
<i>description</i>	644
<i>flush {enable disable} arp</i>	645
<i>flush {enable disable} mac</i>	645
<i>flush {enable disable} mac-vlan</i>	646
<i>preemption delay</i>	646
<i>preemption mode</i>	647
<i>protect vlan-reference-instance</i>	647
<i>show ulpp flush counter interface</i>	648
<i>show ulpp flush-receive-port</i>	648
<i>show ulpp group</i>	648
<i>ulpp control vlan</i>	649
<i>ulpp flush {enable disable} arp</i>	650
<i>ulpp flush {enable disable} mac</i>	650
<i>ulpp flush {enable disable} mac-vlan</i>	650
<i>ulpp group</i>	651
<i>ulpp group {master slave}</i>	651

ulpp group <integer> {master slave}.....	651
no ulpp group <integer> {master slave}.....	651
3 Commands for ULSM.....	652
show ulsm group.....	652
ulsm group.....	652
ulsm group {uplink downlink}.....	653
4 Commands for NQA.....	653
nqa agent enable.....	653
nqa server instance enable.....	654
nqa server instance	654
nqa entry domain tag	655
type.....	656
community read WORD.....	656
destination IP	657
destination port.....	657
filename	658
ftp-operation	658
ftp-password (cipher simple).....	658
ftp-username	659
mode.....	659
http-operation.....	660
out interface vlan.....	660
source IP	661
source port.....	661
version	662
test.....	662
show nqa result.....	663
12-Commands for Mirroring Configuration	665
1 Commands for Mirroring Configuration.....	666
monitor session source interface	666
monitor session source interface access-list.....	666
monitor session destination interface	667
show monitor.....	668
2 Commands for sFlow	668
sflow agent-address.....	668
sflow analyzer sflowtrend	669
sflow counter-interval.....	669
sflow data-len.....	670
sflow destination.....	670
sflow header-len.....	671
sflow rate	671
show sflow.....	672
3 Commands for RSPAN Configuration	673
remote-span	673
monitor session remote vlan	674
monitor session reflector-port.....	674
13-Commands for Network Time Management	676

1 Commands for SNTP	677
<i>clock timezone</i>	677
<i>sntp polltime</i>	677
<i>sntp server</i>	678
<i>show sntp</i>	678
2 Commands for NTP.....	679
<i>ntp access-group server</i>	679
<i>ntp authenticate</i>	679
<i>ntp authentication-key</i>	680
<i>ntp broadcast server count</i>	680
<i>ntp disable</i>	681
<i>ntp enable</i>	682
<i>ntp ipv6 multicast client</i>	682
<i>ntp multicast client</i>	683
<i>ntp server</i>	683
<i>ntp syn-interval</i>	684
<i>ntp trusted-key</i>	685
<i>show ntp status</i>	685
<i>show ntp session</i>	686
3 Commands for Summer Time	687
<i>clock summer-time absolute</i>	687
<i>clock summer-time recurring</i>	688
<i>clock summer-time recurring</i>	689
4 Commands for PTP	690
<i>ptp profile</i>	690
<i>ptp mode</i>	691
<i>ptp clock-step</i>	692
<i>ptp enable</i>	692
<i>ptp delay-mechanism</i>	693
<i>ptp clock-class</i>	693
<i>ptp clock-accuracy</i>	694
<i>ptp priority1</i>	694
<i>ptp priority2</i>	695
<i>ptp domain</i>	695
<i>ptp transport-protocol</i>	696
<i>ptp source ip-address</i>	696
<i>ptp dscp</i>	697
<i>ptp announce-interval</i>	697
<i>ptp announce-timeout multiple-value</i>	698
<i>ptp sync-interval</i>	698
<i>ptp pdelay-req-interval</i>	699
<i>ptp vlan</i>	699
<i>ptp force-state</i>	699
<i>show ptp clock</i>	700
<i>show ptp config</i>	700
<i>show ptp packet-statistics</i>	701
<i>show ptp port</i>	701

<i>show ptp parent</i>	702
14-Debugging and Diagnosis	703
1 SHOW	704
<i>clear history all-users</i>	704
<i>clear logging</i>	704
<i>history all-users max-length</i>	704
<i>logging</i>	705
<i>logging executed-commands</i>	706
<i>logging loghost sequence-number</i>	706
<i>logging source-ip</i>	706
<i>ping</i>	707
<i>ping6</i>	708
<i>show boot-files</i>	710
<i>show flash</i>	710
<i>show history</i>	711
<i>show history all-users</i>	711
<i>show logging buffered</i>	712
<i>show logging executed-commands state</i>	712
<i>show logging source</i>	713
<i>show running-config</i>	713
<i>show running-config current-mode</i>	713
<i>show startup-config</i>	714
<i>show switchport interface</i>	714
<i>show tcp</i>	715
<i>show tcp ipv6</i>	715
<i>show telnet login</i>	716
<i>show udp</i>	716
<i>show udp ipv6</i>	717
<i>show version</i>	717
<i>Traceroute</i>	718
<i>traceroute6</i>	719
<i>reload</i>	719
<i>reload after</i>	720
<i>reload cancel</i>	720
<i>show reload</i>	720
<i>clear cpu-rx-stat protocol</i>	721
<i>cpu-rx-ratelimit protocol</i>	721
<i>cpu-rx-ratelimit channel-rate</i>	722
<i>cpu-rx-ratelimit channel-skb-threshold</i>	722
<i>cpu-rx-ratelimit total</i>	723
<i>show cpu-rx protocol</i>	723
15-Commands for Routing Protocol	724
1 Commands for RIP	725
<i>accept-lifetime</i>	725
<i>clear ip rip route</i>	726
<i>default-information originate</i>	726
<i>default-metric</i>	727

<i>distance</i>	727
<i>distribute-list</i>	728
<i>ip rip aggregate-address</i>	728
<i>ip rip authentication key-chain</i>	729
<i>ip rip authentication mode</i>	730
<i>ip rip authentication string</i>	730
<i>ip rip authentication string <text></i>	730
<i>no ip rip authentication string</i>	730
<i>ip rip authentication cisco-compatible</i>	731
<i>ip rip receive-packet</i>	731
<i>ip rip receive version</i>	732
<i>ip rip send-packet</i>	732
<i>ip rip send version</i>	733
<i>ip rip split-horizon</i>	733
<i>key</i>	734
<i>key chain</i>	734
<i>key-string</i>	735
<i>maximum-prefix</i>	735
<i>neighbor</i>	736
<i>network</i>	736
<i>offset-list</i>	737
<i>passive-interface</i>	738
<i>recv-buffer-size</i>	738
<i>redistribute</i>	739
<i>route</i>	740
<i>router rip</i>	740
<i>send-lifetime</i>	741
<i>timers basic</i>	742
<i>version</i>	742
<i>show ip protocols rip</i>	743
<i>show ip rip</i>	744
<i>show ip rip database</i>	745
<i>show ip rip interface</i>	745
<i>show ip rip aggregate</i>	746
<i>show ip rip redistribute</i>	746
<i>debug rip</i>	747
<i>debug rip redistribute route receive</i>	747
<i>debug rip redistribute message send</i>	748
<i>rip restart grace-period</i>	748
2 Commands for OSPF	749
<i>area authentication</i>	749
<i>area default-cost</i>	749
<i>area filter-list</i>	750
<i>area nssa</i>	750
<i>area range</i>	751
<i>area stub</i>	752
<i>area virtual-link</i>	752

<i>auto-cost reference-bandwidth</i>	753
<i>compatible rfc1583</i>	754
<i>clear ip ospf process</i>	754
<i>default-information originate</i>	755
<i>default-metric</i>	756
<i>distance</i>	756
<i>distribute-list</i>	757
<i>host area</i>	758
<i>ip ospf authentication</i>	758
<i>ip ospf authentication-key</i>	759
<i>ip ospf cost</i>	759
<i>ip ospf database-filter</i>	760
<i>ip ospf dead-interval</i>	760
<i>ip ospf disable all</i>	761
<i>ip ospf hello-interval</i>	761
<i>ip ospf message-digest-key</i>	762
<i>ip ospf mtu</i>	763
<i>ip ospf mtu-ignore</i>	763
<i>ip ospf network</i>	764
<i>ip ospf priority</i>	764
<i>ip ospf retransmit-interval</i>	765
<i>ip ospf transmit-delay</i>	765
<i>ispf enable</i>	766
<i>key</i>	766
<i>key chain</i>	767
<i>log-adjacency-changes detail</i>	767
<i>max-concurrent-dd</i>	768
<i>neighbor</i>	768
<i>network area</i>	769
<i>ospf abr-type</i>	769
<i>ospf router-id</i>	770
<i>overflow database</i>	770
<i>overflow database external</i>	771
<i>passive-interface</i>	771
<i>redistribute</i>	772
<i>redistribute ospf</i>	773
<i>router ospf</i>	773
<i>refresh timer</i>	774
<i>summary-address</i>	774
<i>timers</i>	775
<i>show ip ospf</i>	776
<i>show ip ospf border-routers</i>	777
<i>show ip ospf database</i>	778
<i>show ip ospf interface</i>	779
<i>show ip ospf ispf status</i>	779
<i>show ip ospf neighbor</i>	780
<i>show ip ospf redistribute</i>	781

<i>show ip ospf route</i>	781
<i>show ip ospf virtual-links</i>	782
<i>show ip route process-detail</i>	783
<i>show ip protocols</i>	783
<i>debug ospf events</i>	784
<i>debug ospf ifsm</i>	784
<i>debug ospf lsa</i>	785
<i>debug ospf nfm</i>	785
<i>debug ospf nsm</i>	786
<i>debug ospf packet</i>	786
<i>debug ospf route</i>	787
<i>debug ospf redistribute message send</i>	787
<i>debug ospf redistribute route receive</i>	788
<i>capability</i>	788
<i>debug ospf events gr</i>	789
3 Commands for BGP	789
<i>aggregate-address</i>	789
<i>bgp aggregate-nexthop-check</i>	790
<i>bgp always-compare-med</i>	791
<i>bgp asnotation asdot</i>	791
<i>bgp bestpath as-path ignore</i>	792
<i>bgp bestpath compare-confed-aspath</i>	792
<i>bgp bestpath compare-routerid</i>	793
<i>bgp bestpath med</i>	793
<i>bgp client-to-client reflection</i>	794
<i>bgp cluster-id</i>	794
<i>bgp confederation identifier</i>	795
<i>bgp confederation peers</i>	795
<i>bgp dampening</i>	796
<i>bgp default</i>	797
<i>bgp deterministic-med</i>	797
<i>bgp enforce-first-as</i>	798
<i>bgp fast-external-failover</i>	798
<i>bgp inbound-route-filter</i>	798
<i>bgp inbound-max-route-num</i>	799
<i>bgp log-neighbor-changes</i>	799
<i>bgp network import-check</i>	800
<i>bgp rfc1771-path-select</i>	800
<i>bgp rfc1771-strict</i>	801
<i>bgp router-id</i>	801
<i>bgp scan-time</i>	802
<i>clear ip bgp</i>	802
<i>clear ip bgp dampening</i>	803
<i>clear ip bgp flap-statistics</i>	803
<i>distance</i>	804
<i>distance bgp</i>	804
<i>ip as-path access-list</i>	805

<i>ip community-list</i>	805
<i>ip extcommunity-list</i>	806
<i>neighbor activate</i>	806
<i>neighbor advertisement-interval</i>	807
<i>neighbor allowas-in</i>	807
<i>neighbor attribute-unchanged</i>	808
<i>neighbor capability</i>	809
<i>neighbor capability orf prefix-list</i>	809
<i>neighbor collide-established</i>	810
<i>neighbor default-originate</i>	811
<i>neighbor description</i>	811
<i>neighbor distribute-list</i>	812
<i>neighbor dont-capability-negotiate</i>	812
<i>neighbor ebgp-multihop</i>	813
<i>neighbor enforce-multihop</i>	814
<i>neighbor filter-list</i>	814
<i>neighbor interface</i>	815
<i>neighbor maximum-prefix</i>	815
<i>neighbor next-hop-self</i>	816
<i>neighbor override-capability</i>	816
<i>neighbor passive</i>	817
<i>neighbor peer-group (Creating)</i>	818
<i>neighbor peer-group(Configuring group members)</i>	818
<i>neighbor port</i>	819
<i>neighbor prefix-list</i>	819
<i>neighbor remote-as</i>	820
<i>neighbor remove-private-AS</i>	820
<i>neighbor route-map</i>	821
<i>neighbor route-reflector-client</i>	821
<i>neighbor route-server-client</i>	822
<i>neighbor send-community</i>	823
<i>neighbor shutdown</i>	823
<i>neighbor soft-reconfiguration inbound</i>	824
<i>neighbor strict-capability-match</i>	824
<i>neighbor timers</i>	825
<i>neighbor timers connect</i>	825
<i>neighbor unsuppress-map</i>	826
<i>neighbor update-source</i>	826
<i>neighbor version 4</i>	827
<i>neighbor weight</i>	827
<i>network (BGP)</i>	828
<i>redistribute (BGP)</i>	828
<i>redistribute ospf</i>	829
<i>router bgp</i>	830
<i>timers bgp</i>	830
<i>show ip bgp</i>	831
<i>show ip bgp attribute-info</i>	831

<i>show ip bgp community</i>	832
<i>show ip bgp community-info</i>	832
<i>show ip bgp community-list</i>	833
<i>show ip bgp dampening</i>	833
<i>show ip bgp filter-list</i>	834
<i>show ip bgp inconsistent-as</i>	835
<i>show ip bgp neighbors</i>	835
<i>show ip bgp paths</i>	836
<i>show ip bgp prefix-list</i>	837
<i>show ip bgp quote-regexp</i>	838
<i>show ip bgp redistribute</i>	838
<i>show ip bgp neighbors</i>	839
<i>show ip bgp regexp</i>	839
<i>show ip bgp route-map</i>	840
<i>show ip bgp scan</i>	840
<i>show ip bgp summary</i>	841
<i>debug bgp</i>	842
<i>debug bgp redistribute message send</i>	842
<i>debug bgp redistribute route receive</i>	842
<i>bgp graceful-restart</i>	843
<i>bgp graceful-restart restart-time</i>	843
<i>bgp graceful-restart stale-path-time</i>	844
<i>bgp selection-deferral-time</i>	844
<i>neighbor restart-time</i>	845
<i>maximum-paths</i>	845
<i>load-balancing</i>	846
<i>neighbor password</i>	846
4 Commands for RIPv6	847
<i>clear ipv6 rip route</i>	847
<i>default-information originate</i>	847
<i>default-metric</i>	848
<i>distance</i>	848
<i>distribute-list</i>	849
<i>debug ipv6 rip</i>	849
<i>debug ipv6 rip redistribute message send</i>	850
<i>debug ipv6 rip redistribute route receive</i>	851
<i>ipv6 rip aggregate-address</i>	851
<i>ipv6 rip split-horizon</i>	851
<i>ipv6 router rip</i>	852
<i>neighbor</i>	853
<i>offset-list</i>	853
<i>passive-interface</i>	854
<i>redistribute</i>	854
<i>redistribute ospf</i>	855
<i>route</i>	855
<i>router ipv6 rip</i>	856
<i>show debugging ipv6 rip</i>	856

<i>show ipv6 rip interface</i>	857
<i>show ipv6 rip redistribute</i>	858
<i>show ipv6 protocols rip</i>	858
<i>show ipv6 rip</i>	859
<i>show ipv6 rip database</i>	860
<i>show ipv6 rip aggregate</i>	860
<i>timers basic</i>	861
5 Commands for OSPFv3	862
<i>area default-cost</i>	862
<i>area range</i>	862
<i>area stub</i>	863
<i>area virtual-link</i>	863
<i>abr-type</i>	864
<i>default-metric</i>	865
<i>debug ipv6 ospf events</i>	865
<i>debug ipv6 ospf ifsm</i>	866
<i>debug ipv6 ospf lsa</i>	866
<i>debug ipv6 ospf n fsm</i>	867
<i>debug ipv6 ospf nsm</i>	868
<i>debug ipv6 ospf packet</i>	868
<i>debug ipv6 ospf redistribute message send</i>	869
<i>debug ipv6 ospf redistribute route receive</i>	869
<i>debug ipv6 ospf route</i>	870
<i>ipv6 ospf cost</i>	870
<i>ipv6 ospf dead-interval</i>	871
<i>ipv6 ospf display route single-line</i>	871
<i>ipv6 ospf hello-interval</i>	872
<i>ipv6 ospf network</i>	872
<i>ipv6 ospf priority</i>	873
<i>ipv6 ospf retransmit-interval</i>	874
<i>ipv6 ospf transmit-delay</i>	874
<i>ipv6 router ospf</i>	875
<i>max-concurrent-dd</i>	876
<i>passive-interface</i>	876
<i>redistribute</i>	877
<i>redistribute ospf</i>	877
<i>router-id</i>	878
<i>router ipv6 ospf</i>	878
<i>show ipv6 ospf</i>	879
<i>show ipv6 ospf database</i>	880
<i>show ipv6 ospf interface</i>	881
<i>show ipv6 ospf neighbor</i>	883
<i>show ipv6 ospf route</i>	883
<i>show ipv6 ospf redistribute</i>	884
<i>show ipv6 ospf topology</i>	885
<i>show ipv6 ospf virtual-links</i>	885
<i>show ipv6 route process-detail</i>	886

<i>timers spf</i>	886
6 Commands for MBGP4+	887
<i>debug ipv6 bgp redistribute message send</i>	887
<i>debug ipv6 bgp redistribute route receive</i>	887
<i>redistribute ospf (MBGP4+)</i>	888
<i>show ipv6 bgp redistribute</i>	888
7 Commands for ISIS.....	889
<i>router isis</i>	889
<i>net</i>	889
<i>is-type</i>	890
<i>area-password</i>	890
<i>domain-password</i>	891
<i>ignore-lsp-error</i>	891
<i>lsp-gen-interval</i>	892
<i>lsp-refresh-interval</i>	892
<i>max-area-addresses</i>	893
<i>max-lsp-lifetime</i>	893
<i>spf-interval</i>	894
<i>dynamic-hostname</i>	894
<i>adjacency-check</i>	895
<i>summary-address</i>	895
<i>set-overload-bit suppress</i>	895
<i>metric-style</i>	896
<i>mpls traffic-eng</i>	897
<i>capability cspf</i>	897
<i>debug isis all</i>	898
<i>debug isis ifsm</i>	898
<i>debug isis nfm</i>	898
<i>debug isis pdu</i>	899
<i>debug isis lsp</i>	899
<i>debug isis spf</i>	900
<i>debug isis events</i>	900
<i>debug isis nsm</i>	900
<i>show debugging isis</i>	901
<i>debug ospf redistribute route receive</i>	901
<i>redistribute</i>	902
<i>redistribute isis</i>	903
<i>default-information</i>	903
<i>is-name</i>	904
<i>ip router isis</i>	904
<i>isis circuit-type</i>	904
<i>isis csnp-interval</i>	905
<i>isis hello-interval</i>	905
<i>isis hello-interval minimal</i>	906
<i>isis hello-multiplier</i>	906
<i>isis hello padding</i>	907
<i>isis lsp-interval</i>	907

<i>isis metric</i>	908
<i>isis wide-metric</i>	908
<i>isis password</i>	909
<i>isis priority</i>	909
<i>isis retransmit-interval</i>	910
<i>isis mesh-group</i>	910
<i>isis mesh-group blocked</i>	911
<i>restart-timer</i>	911
<i>show isis database</i>	912
<i>show isis topology</i>	912
<i>show ip isis route</i>	912
<i>show clns neighbors</i>	913
<i>show clns is-neighbors</i>	914
<i>show isis interface</i>	914
<i>show isis counter</i>	915
<i>show isis interface counter</i>	916
<i>show cspf lsp</i>	917
<i>clear ip isis</i>	917
8 Commands for IPV6 ISIS	918
<i>address-family ipv6</i>	918
<i>summary-prefix</i>	918
<i>multi-topology</i>	919
<i>redistribute</i>	919
<i>default-information</i>	920
<i>adjacency-check</i>	921
<i>ipv6 router isis</i>	921
<i>show ipv6 isis topology</i>	922
<i>show ipv6 isis route</i>	922
9.Commands for BFD	923
<i>bfd authentication key</i>	923
<i>bfd authentication key md5</i>	923
<i>bfd authentication key text</i>	924
<i>bfd echo</i>	924
<i>bfd echo-source-ip</i>	925
<i>bfd echo-source-ipv6</i>	925
<i>bfd enable</i>	926
<i>bfd interval</i>	927
<i>bfd min-echo-recv-interval</i>	927
<i>bfd mode</i>	928
<i>debug bfd</i>	928
<i>ip ospf bfd enable</i>	929
<i>ip route bfd</i>	929
<i>ipv6 ospf bfd enable</i>	930
<i>ipv6 ospf bfd enable instance-id</i>	930
<i>ipv6 rip bfd enable</i>	931
<i>ipv6 route bfd</i>	931
<i>neighbor</i>	932

<i>rip bfd enable</i>	933
<i>show bfd neighbor</i>	933
<i>show bfd interface</i>	934
16-Commands for Stacking	935
1 Commands for Vsf Configuration	936
<i>switch convert mode</i>	936
<i>vsf port-group</i>	936
<i>vsf port-group interface ethernet</i>	937
<i>vsf domain</i>	937
<i>vsf member</i>	938
<i>vsf priority</i>	938
<i>vsf auto-merge enable</i>	939
<i>vsf member description</i>	939
<i>vsf link delay</i>	940
2 Commands for Mad Configuration	940
<i>vsf mad lacp enable</i>	941
<i>vsf mad bfd enable</i>	941
<i>vsf mad ip address</i>	942
<i>vsf mad exclue</i>	942
<i>vsf mad restore</i>	943
<i>show mad config</i>	943
3 Commands for Vsf Debug	944
<i>show vsf</i>	944
<i>show vsf config</i>	945
<i>show vsf cpu-database all-member brief-information</i>	945
<i>show vsf cpu-database member basic-information</i>	946
<i>show vsf cpu-database member running-information</i>	946
<i>show vsf cpu-database member port-information</i>	947
<i>show vsf cpu-database member port-link-information</i>	948
<i>debug vsf packet detail <alive all config member-infor probe routing topo></i>	948
<i>debug vsf packet</i>	950
<i>debug vsf event</i>	950
<i>debug vsf error</i>	951
<i>debug vsf atp</i>	951
<i>debug vsf detail</i>	951
<i>debug vsf fsm</i>	952
<i>debug vsf restart</i>	952
<i>debug vsf timer</i>	953
<i>debug vsf warn</i>	953
4 Commands for devsm configuration	953
<i>debug devsm</i>	954
<i>force runcfg-sync</i>	954
<i>force switchov</i>	955
<i>reset slot</i>	955
<i>runcfg-sync</i>	956
<i>show slot</i>	956
17-Evpn vxlan+Mlag+Esi	958

1 Commands for Basic Configuration	959
<i>address-family l2vpn evpn.....</i>	<i>959</i>
<i>arp-cache disable.....</i>	<i>959</i>
<i>arp-nd flood-suppress.....</i>	<i>960</i>
<i>arp proxy-send enable.....</i>	<i>960</i>
<i>clear nvo vxlan mac-table dynamic.....</i>	<i>961</i>
<i>evpn irb-forwarding anycast-gateway-mac.....</i>	<i>961</i>
<i>evpn NAME.....</i>	<i>962</i>
<i>evpn-vlan-service</i>	<i>963</i>
<i>interface irb.....</i>	<i>963</i>
<i>Local-proxy-arp enable</i>	<i>964</i>
<i>l3vni.....</i>	<i>964</i>
<i>mac.....</i>	<i>965</i>
<i>mac vrf.....</i>	<i>966</i>
<i>map vnid.....</i>	<i>966</i>
<i>nvo vxlan access-if.....</i>	<i>967</i>
<i>nvo vxlan disable</i>	<i>967</i>
<i>nvo vxlan enable.....</i>	<i>968</i>
<i>nvo vxlan id.....</i>	<i>968</i>
<i>nvo vxlan irb.....</i>	<i>969</i>
<i>nvo vxlan vtep-ip-global.....</i>	<i>969</i>
<i>track WORD evpn peer A.B.C.D.....</i>	<i>970</i>
<i>vxlan host-reachability-protocol evpn-bgp NAME.....</i>	<i>970</i>
<i>vxlan static-entry host-mac.....</i>	<i>971</i>
2.Commands for Show	971
<i>show evpn l3vni-map</i>	<i>971</i>
<i>show evpn track.....</i>	<i>972</i>
<i>show interface irb.....</i>	<i>972</i>
<i>show nvo vxlan.....</i>	<i>973</i>
<i>show nvo vxlan access-if brief.....</i>	<i>973</i>
<i>show nvo vxlan access-if-config.....</i>	<i>974</i>
<i>show nvo vxlan arp-cache.....</i>	<i>974</i>
<i>show nvo vxlan dynamic-tunnel.....</i>	<i>975</i>
<i>show nvo vxlan fdb-entry.....</i>	<i>976</i>
<i>show nvo vxlan mac-table</i>	<i>976</i>
<i>show nvo vxlan static host.....</i>	<i>977</i>
<i>show nvo vxlan vlan-vnid.....</i>	<i>977</i>
<i>show running-config interface irb.....</i>	<i>978</i>
<i>show running-config nvo vxlan.....</i>	<i>978</i>
<i>show running-config track.....</i>	<i>978</i>
3.Commands for Mclag.....	979
<i>Authentication</i>	<i>979</i>
<i>connection timer.....</i>	<i>980</i>
<i>dad ip vrf.....</i>	<i>980</i>
<i>dad keepalive-interval timer.....</i>	<i>981</i>
<i>dad link.....</i>	<i>981</i>
<i>dad local.....</i>	<i>982</i>

<i>dad session-timeout timer ms</i>	982
<i>delay-restore timer</i>	983
<i>domain</i>	983
<i>ip vrf</i>	984
<i>Keepalive</i>	984
<i>nvo vxlan mlag-vip-global</i>	984
<i>orphan-port ethernet-port</i>	985
<i>orphan-port port-channel</i>	985
<i>port-channel</i>	986
<i>priority</i>	987
<i>role swap</i>	987
<i>session timeout</i>	987
<i>show mclag-arp domain</i>	988
<i>show mclag configuration</i>	988
<i>show mclag-mac domain</i>	989
<i>show mclag-state domain</i>	989
<i>source A.B.C.D peer A.B.C.D interface port-channel WORD</i>	990
<i>vxlan mlag-virtual-mac</i>	990
4.Commands for ESI	991
<i>evpn esi hold-time</i>	991
<i>evpn multi-homed esi</i>	991
<i>evpn vxlan multihoming enable</i>	992
<i>show bgp l2vpn evpn esi-vni-hash</i>	992
<i>show bgp l2vpn evpn route-type es-route</i>	992
<i>show bgp l2vpn evpn route-type ethernet-ad-per-es</i>	993
<i>show bgp l2vpn evpn route-type ethernet-ad-per-evi</i>	994
<i>show evpn multi-homing</i>	994
5.Commands for Evpn Show	995
<i>show bgp l2vpn evpn</i>	995
<i>show bgp l2vpn evpn detail</i>	995
<i>show bgp l2vpn evpn irb-vni-hash vrf</i>	996
<i>show bgp l2vpn evpn peer-group</i>	996
<i>show bgp l2vpn evpn route-type mac-ip</i>	997
<i>show bgp l2vpn evpn route-type mcast</i>	997
<i>show bgp l2vpn evpn route-type prefix-route</i>	998
<i>show bgp l2vpn evpn summary</i>	998
<i>show bgp l2vpn evpn time</i>	999
<i>show bgp l2vpn evpn vni-ipvrf-hash</i>	999
<i>show bgp l2vpn evpn vni-mac-table</i>	1000
<i>show bgp l2vpn evpn vni-vrf-hash</i>	1000
6.Commands for Static Vxlan	1000
<i>tunnel mode vxlan</i>	1000
<i>tunnel map vnid</i>	1001
<i>show nvo vxlan static-tunnel</i>	1002
18.Commands for MPLS	1004
1 MPLS Configuration	1005
<i>mpls enable</i>	1005

<i>mpls forward soft</i>	1005
<i>mpls ingress-ttl</i>	1006
<i>mpls local-packet-handling</i>	1006
<i>show mpls</i>	1006
<i>show mpls forwarding-table</i>	1007
<i>show mpls ftn-table brief</i>	1008
<i>show mpls ftn-tabledetail</i>	1008
<i>show mpls ilm-table</i>	1009
<i>show mpls vrf-table</i>	1010
2 Commands for LDP	1012
<i>advertisement-mode</i>	1012
<i>clear ldp adjacency</i>	1012
<i>clear ldp session</i>	1013
<i>clear ldp statistics</i>	1013
<i>control-mode</i>	1014
<i>ldp enable/disable</i>	1014
<i>global-merge-capability</i>	1015
<i>hello-interval</i>	1016
<i>hold-time</i>	1016
<i>import-bgp-routes</i>	1017
<i>keepalive-interval</i>	1017
<i>keepalive-timeout</i>	1018
<i>label-retention-mode</i>	1018
<i>label-switching</i>	1019
<i>ldp advertisement-mode</i>	1020
<i>ldp hello-interval</i>	1020
<i>ldp hold-time</i>	1021
<i>ldp keepalive-interval</i>	1021
<i>ldp keepalive-timeout</i>	1022
<i>ldp label-retention-mode</i>	1023
<i>ldp multicast-hellos</i>	1023
<i>ldp targeted-peer-hello-interval</i>	1024
<i>ldp targeted-peer-hold-time</i>	1024
<i>loop-detection</i>	1025
<i>loop-detection-count</i>	1025
<i>multicast-hellos</i>	1026
<i>propagate-release</i>	1027
<i>request-retry</i>	1027
<i>request-retry-timeout</i>	1028
<i>router ldp</i>	1028
<i>router-id</i>	1029
<i>show ldp</i>	1029
<i>show ldp adjacency</i>	1030
<i>show ldp downstream</i>	1030
<i>show ldp fec</i>	1031
<i>show ldp interface</i>	1032
<i>show ldp lsp</i>	1032

<i>show ldp session</i>	1033
<i>show ldp statistics</i>	1033
<i>show ldp targeted-peers</i>	1034
<i>show ldp upstream</i>	1035
<i>show mpls ldp discovery</i>	1035
<i>show mpls ldp fec</i>	1036
<i>show mpls ldp neighbor</i>	1036
<i>show mpls ldp parameter</i>	1037
<i>show mpls ldp session</i>	1038
<i>targeted-hello-accept</i>	1038
<i>targeted-peer</i>	1039
<i>targeted-peer-hello-interval</i>	1039
<i>targeted-peer-hold-time</i>	1040
<i>transport-address</i>	1040
3 Commands for Static LSP	1042
<i>nsm mpls ftn add</i>	1042
<i>nsm mpls ftn mask add</i>	1042
<i>nsm mpls ilm add</i>	1043
<i>nsm mpls ilm delete</i>	1044
4 Commands for VPLS&VPWS	1045
<i>set PW ptag</i>	1045
<i>create/delete PW class</i>	1045
<i>PW class transport mode</i>	1046
<i>create/delete VFI</i>	1046
<i>create/delete PW</i>	1047
<i>create/delete back PW</i>	1047
<i>enable/disable BFD</i>	1048
<i>switch PW redundancy mode</i>	1049
<i>PW MTU</i>	1049
<i>create/delete l2-vc</i>	1050
<i>xconnect</i>	1051
<i>show mpls forwarding-table</i>	1051
<i>show mpls ftn</i>	1052
<i>show mpls ilm</i>	1054
<i>show mpls l2-vc</i>	1054
<i>show mpls ldp</i>	1055
<i>show ldp vpls</i>	1056
<i>show ldp mpls-l2-circuit</i>	1057
<i>show vpls</i>	1057
<i>show vpls fib</i>	1058
<i>show vfi mac-address-table</i>	1058
<i>show vpls peer</i>	1058
5 MPLS L3VPN Table	1059
<i>address-family ipv4</i>	1059
<i>address-family vpnv4</i>	1059
<i>address-family vpnv4 unicast</i>	1059
<i>allocate-label all</i>	1060

<i>exit-address-family</i>	1060
<i>ip route</i>	1061
<i>ip route vrf</i>	1061
<i>ip vrf <vrf-name></i>	1062
<i>ip vrf forwarding vrfNAME</i>	1062
<i>neighbor A.B.C.D active</i>	1062
<i>neighbor A.B.C.D remote-as</i>	1063
<i>neighbor A.B.C.D send-label</i>	1063
<i>mpls label mode vpnv4</i>	1064
<i>rd</i>	1064
<i>route-target</i>	1064
<i>show ip bgp vpv4 all</i>	1065
<i>show ip bgp vpv4 all A.B.C.D</i>	1065
<i>show ip bgp vpv4 all tags</i>	1066
<i>show ip bgp vpv4 vrf NAME</i>	1066
<i>show ip bgp vpv4 vrf NAME A.B.C.D</i>	1067
<i>show ip bgp vpv4 vrf NAME label</i>	1067
<i>show ip bgp vpv4 rd WORD</i>	1068
<i>show ip bgp vpv4 rd WORD A.B.C.D</i>	1068
<i>show ip bgp vpv4 rd WORD label</i>	1068
<i>show ip bgp vpv4 all summary</i>	1069
<i>show ip bgp vpv4 rd WORD summary</i>	1070
<i>show ip bgp vpv4 vrf NAME summary</i>	1070
<i>show ip bgp labeled-unicast</i>	1071
<i>show ip route vrf</i>	1071
<i>show ip vrf</i>	1072
6 Commands for Rsvp Configuration	1073
<i>router rsvp</i>	1073
<i>enable-rsvp</i>	1073
<i>rsvp-trunk</i>	1074
<i>rsvp-path</i>	1074
<i>reservable-bandwidth</i>	1075
<i>A.B.C.D loose</i>	1075
<i>A.B.C.D strict</i>	1076
<i>ext-tunnel-id A.B.C.D</i>	1076
<i>from A.B.C.D</i>	1077
<i>to A.B.C.D</i>	1077
<i>map-route A.B.C.D</i>	1078
<i>primary cspf</i>	1078
<i>secondary cspf</i>	1079
<i>primary bandwidth</i>	1079
<i>secondary bandwidth</i>	1080
<i>primary path</i>	1080
<i>secondary path</i>	1080
<i>rsvp-trunk-restart</i>	1081
<i>primary cspf-retry-limit</i>	1081
<i>secondary cspf-retry-limit</i>	1082

<i>primary cspf-retry-timer</i>	1082
<i>secondary cspf-retry-timer</i>	1083
<i>primary retry-limit</i>	1083
<i>secondary retry-limit</i>	1084
<i>primary cretry-timer</i>	1084
<i>primary cspf-retry-timer</i>	1085
<i>primary record</i>	1085
<i>secondary record</i>	1086
<i>primary affinity</i>	1086
<i>secondary affinity</i>	1087
<i>primary hop-limit</i>	1087
<i>secondary hop-limit</i>	1087
<i>update-type</i>	1088
<i>ack-wait-timeout</i>	1089
<i>php</i>	1089
<i>cspf</i>	1090
<i>show rsvp</i>	1090
<i>show rsvp session</i>	1091
7 Commands for MPLS QOS	1092
<i>cos-exp mapping</i>	1092
<i>dscp-exp mapping</i>	1093
<i>exp-exp mapping</i>	1093
<i>exp-intp mapping</i>	1094
<i>exp-dp mapping</i>	1094
8 Commands For Send-label	1095
<i>show ip bgp labeled-unicast</i>	1095
<i>neighbor A.B.C.D send-label</i>	1096

01-Commands For Basic Switch Configuration

1 Commands for Basic Configuration

authentication dot1x

Command	authentication dot1x radius none no authentication dot1x radius none
Parameter	
Default	No global 802.1X authentication method is configured by default. Without this command, 802.1X port authentication will not work on any interface
Mode	Global Mode
Usage Guide	This command configures 802.1X authentication priority: verify clients via RADIUS server first. If RADIUS fails, terminals are allowed to access the network without authentication. RADIUS server must be configured in advance. The no < b0> < / b0> command clears this policy.
Example	Switch(config)#authentication dot1x radius none

authentication line

Command	authentication line {console vty web} login {local radius tacacs} no authentication line {console vty web} login						
Parameter	<table><tr><td>console</td><td>Log on the switch through the console serial port</td></tr><tr><td>vty</td><td>Log on the switch through the vty(SSH or Telnet)</td></tr><tr><td>web</td><td>Log on the switch through the web</td></tr></table>	console	Log on the switch through the console serial port	vty	Log on the switch through the vty(SSH or Telnet)	web	Log on the switch through the web
console	Log on the switch through the console serial port						
vty	Log on the switch through the vty(SSH or Telnet)						
web	Log on the switch through the web						
Default	No configuration is enabled for the console login method by default. Local authentication is enabled for the VTY and Web login method by default.						
Mode	Global Mode						
Usage Guide	This command can configure the authentication methods for Console, VTY, and Web login separately. The authentication method can be any one or combination of Local. RADIUS and TACACS. Preferences from left to right when the login method is combined configuration. If the user has passed the authentication method, the authentication method of the lower preference is ignored. As long as pass an authentication method, the user can log in. AAA function and RADIUS server should be configured before the RADIUS authentication can be used. If local authentication is configured without configuring a local user, the user will be able to log on to the switch through the console method.						

They all support the following authentication methods.
 Local: Use the local user account database for authentication.
 Tacacs: Authentication using remote Tacas server.
 Radius: Authentication using remote Radius server.

no command restores default authentication.

Example

Configure Telnet and ssh login methods to Local and RADIUS authentication methods.

Switch(config)# authentication line vty login local radius lists

banner

Command

banner {login | motd} <LINE>
no banner login | motd

Parameter

<LINE> The information displayed when the authentication is successful, length limit from 1 to 512 characters

Default

Do not show the information when the authentication is successful.

Mode

Global Mode

Usage Guide

This command is used to configure the information displayed when the login authentication of a telnet or console user is successful, the no command configures that the information is not displayed when the authentication is successful.

Example

Display “Welcome” after authentication is successful.

Switch(config)# banner motd Welcome

boot img

Command

boot img <img-file-url> {primary | secondary}

Parameter

<img-file-url> Full path to the img file

primary	First entry to the img document
secondary	Second entry to the img document

Default	The factory original configuration only specifies the first booting IMG file, it is nos.img file in the FLASH, without the second booting IMG file.
Mode	admin Mode
Usage Guide	This command is used to configure the first and second img files used by the switch next boot. The first and second img files can only use .img files stored in switch. 1. The file path comprises of three parts: device prefix used as the root directory (flash:/), sub-directory, and the file name. No space is allowed in each part or between two parts. 2. The suffix of all file names should be .img. 3. The length of the full file path should not be longer than 128 characters, while the file name can not be longer than 80 characters.
Example	Set flash:/nos.img as the second booting IMG file used in the next booting of the switch. Switch#boot img flash:/nos.img backup

boot startup-config

Command	boot startup-config {NULL <WORD > }	
Parameter	NULL	Use the factory primitive configuration as the next reboot boot configuration
	< WORD >	Startup-config filename
Default	None.	
Mode	admin Mode	
Usage Guide	This command is used configure the CFG file used in the next booting of the switch. Configure the CFG file used in the next booting can only use .cfg files stored in the switch. 1. The file path comprises of three parts: device prefix used as the root directory (flash:/), sub-directory, and the file name. No space is allowed in each part or between two parts. 2. The suffix of all file names should be .cfg. 3. The length of the full file path should not be longer than 128 characters, while the file name can not be longer than 80 characters.	
Example	Set flash:/ startup.cfg as the CFG file used in the next booting of the switch.	

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

clock set

Command	clock set <HH:MM:SS> <YYYY.MM.DD>	
Parameter	<HH:MM:SS>	Time, HH effective range 0 to 23, MM and SS 0 to 59
	<YYYY.MM.DD>	Year, month and date, and YYYY valid range is 1970 to 2038, MON is month 1 to 12, DD is date 1 to 31
Default	By default, upon first time start-up, it is defaulted to 2006.1.1 0: 0: 0.	
Mode	admin Mode	
Usage Guide	This command is used to configure switch system time and date. The switch cannot continue timing with power off, hence the current date and time must be first set at environments where exact time is required.	
Example	To set the switch current date and time to 2002.8.1 23: 0: 0. Switch#clock set 23:0:0 2002.8.1	

config

Command	config [terminal]	
Parameter	[terminal]	indicates terminal configuration
Default	None.	
Mode	admin Mode.	
Usage Guide	This command is used to switch from admin management mode to config global configuration mode.	

Example

Enter config global configuration mode from admin management mode.

Switch#config

disable

Command

disable

Parameter

none	none

Default

None.

Mode

admin Mode.

Usage Guide

This command is used for switch exit admin mode back to general user mode.

Example

Exit admin mode back to general user mode.

Switch#disable

Switch>

enable

Command

enable [<1-15>]

Parameter

[<1-15>]	User Permission Level

Default

None.

Mode

User mode/ admin mode

Usage Guide

Use enable command to enter Admin Mode from User Mode, or change the privilege level of the users.

To prevent unauthorized access of non-admin user, user authentication is required (i.e. Admin user password is required) when entering Admin Mode from User Mode.

If the correct Admin user password is entered, Admin Mode access is granted; if 3 consecutive entry of Admin user password are all wrong, it remains in the User Mode. When the user's privilege is

changed from the low level to the high level, it needs to authenticate the password of the corresponding level, or else it will not authenticate the password.

Set the Admin user password under Global Mode with “enable password” command.

Example

Enter management mode from user mode.

Switch>enable

Switch#

enable password

Command

**enable {password | [trustview [key <0|7>] [WORD]] } [level <1-15>] [0 | 7]
[LINE <1-32>] <password>
no enable password [level <1-15>]**

Parameter

[level <1-15>]	used to specify the privilege level, the default level is 15
[0 7]	If enter option 0 on password settings, the password is not encrypted; If enter option 7 on password settings, the password is encrypted
<password>	the password for the user
WORD	Key <1-16 characters>

Default

This password is empty by system default.

Mode

Global Mode

Usage Guide

Configure the password used for enter Admin Mode from the User Mode.

Configure this password to prevent unauthorized entering Admin Mode.

It is recommended to set the password at the initial switch configuration.

Also, it is recommended to exit Admin Mode with “exit” command when the administrator needs to leave the terminal for a long time.

The “no enable password” command deletes this password.

Example

Configure the command for general users to enter the admin mode by rule as test.

Switch(config)#enable password 0 test

end

Command	end
Parameter	none none
Default	None.
Mode	Except user mode / admin mode
Usage Guide	This command is used to configure the command for general users to enter the admin mode by rule as test.
Example	Quit VLAN mode and return to Admin mode. Switch(config-vlan1)#end Switch#

exec-timeout

Command	exec-timeout <minutes> [<seconds>] no exec-timeout
Parameter	<minutes> the time value shown in minute and ranges between 0~35791 [<seconds>] the time value shown in seconds and ranges between 0~59
Default	Default timeout is 10 minutes.
Mode	Global mode
Usage Guide	This command is used Configure the timeout of exiting admin mode. Timeout exit admin management mode, need to enter management code and password to enter admin management mode again. When the timeout is set to 0, the timeout timer is disabled. “no exec-timeout”command to restore default values.
Example	Set the admin mode timeout value to 5 minutes, 30 seconds.

Switch(config)#exec-timeout 5 30

exit

Command	exit
Parameter	none none
Default	None.
Mode	All Modes
Usage Guide	This command is used quit current mode and return to it's previous mode.
Example	Quit global mode to it's previous mode Switch(config)#exit Switch#

help

Command	help
Parameter	none none
Default	None.
Mode	All Modes
Usage Guide	An instant online help provided by the switch. Help command displays information about the whole help system, including complete help and partial help. The user can type in '?' any time to get online help.
Example	Get help in global mode. 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.

hostname

Command	hostname <hostname> no hostname
Parameter	<hostname> the string for the prompt, up to 64 characters are allowed
Default	The default prompt is relative with the switch.
Mode	Global Mode
Usage Guide	Use this command, set the prompt in the switch command line interface. The no operation cancels the configuration.
Example	Set the prompt to “Test”. Switch(config)#hostname Test Test(config)#

ip host

Command	ip host <WORD> <A.B.C.D > no ip host {< WORD > all}
Parameter	< WORD > the string for the prompt, up 1 to 64 characters are allowed < A.B.C.D > the corresponding IP address for the host name, takes a dot decimal format all all of the host name
Default	None.

Mode	Global Mode
Usage Guide	By using this command, you can set the mapping relationship between the host and the IP address. Set the association between host and IP address, which can be used in commands like “ping <host>”. The “no ip host” parameter of this command will delete the mapping.
Example	Set IP address of a host with the hostname of “beijing” to 200.121.1.1. <pre>Switch(config)#ip host beijing 200.121.1.1</pre>

ipv6 host

Command	<pre>ipv6 host <WORD> < X:X::X:X > no ipv6 host { < WORD > all}</pre>						
Parameter	<table> <tr> <td>< WORD ></td><td>the string for the prompt, up 1 to 64 characters are allowed</td></tr> <tr> <td>< X:X::X:X ></td><td>the corresponding IPv6 address for the host name, takes a dot decimal format</td></tr> <tr> <td>all</td><td>all of the host name</td></tr> </table>	< WORD >	the string for the prompt, up 1 to 64 characters are allowed	< X:X::X:X >	the corresponding IPv6 address for the host name, takes a dot decimal format	all	all of the host name
< WORD >	the string for the prompt, up 1 to 64 characters are allowed						
< X:X::X:X >	the corresponding IPv6 address for the host name, takes a dot decimal format						
all	all of the host name						
Default	None.						
Mode	Global Mode						
Usage Guide	By using this command, you can set the mapping relationship between the host and the IPv6 address. Set the association between host and IPv6 address, which can be used in commands like “traceroute6 <host>”. The “no ip host” parameter of this command will delete the mapping.						
Example	Set the IPv6 address of the host named beijing to 2001:1:2:3::1. <pre>Switch(config)#ipv6 host beijing 2001:1:2:3::1</pre>						

ip http server

Command	ip http {secure-ciphersuite [aes256-sha ecdhe-rsa-aes256-sha] secure-port <port-number> secure-server server } no ip http server {secure-ciphersuite secure-port secure-server server }
Parameter	<port-number> Port number <1025-65535>
Default	Enable.
Mode	Global Mode
Usage Guide	Use this command to enable Web configuration. The “no ip http server” command disables Web configuration.
Example	Enable Web Server function and enable Web configurations. Switch(config)#ip http server

login

Command	login no login
Parameter	none none
Default	No login by default.
Mode	Global Mode
Usage Guide	By using this command, users have to enter the password set by password command to enter normal user mode with console. No login cancels this restriction.
Example	Enable password. Switch(config)#login

password

Command	password [0 <LINE > 7 <WORD >] no password	
Parameter	[0 7]	if input option 0 on password setting, the password is not encrypted; if input option 7, the password is encrypted
	< LINE >	The UNENCRYPTED user password
	<WORD >	The ENCRYPTED user password
Default	This password is empty by system default.	
Mode	Global Mode	
Usage Guide	With this command,configure the password used for enter normal user mode on the console.	
	The “no password” command deletes this password.	
Example	Configure the password used to enter normal user mode as test, password is not encrypted.	
	Switch(config)#password 0 test	

privilege

Command	privilege exec level <1-15> LINE no privilege exec level <1-15> LINE	
Parameter	exec	Exec mode of the command, ‘Tab’ or ‘?’ is able to show all register modes
	<1-15>	level, its range between 1 and 15
	LINE	the command needs to be configured, it supports the command abbreviation
Default	None.	
Mode	Global Mode	
Usage Guide	Use this command to configure the permission level for the specified command.	

This function cannot change the command itself.
 LINE must be the whole command format, the command with the abbreviation format must be analyzed successfully.
 Can choose to set the level of the NO command, but it does not affect the result.
 When using a no command, the LINE must be a configured command line.
 If the command line with the parameter, the parameter must be matched with the configured command.

Example	The no command restores the original level of the command.
	Change the level of show ip route command to level 5.
	Restore the original level of the show ip route command.
	Switch(config)#privilege exec level 5 show ip route
	Switch(config)#no privilege exec level 5 show ip route

reload

Command	reload {<member-id> cancel after [HH:MM:SS days <days-id> <HH:MM:SS>]}	
Parameter	<member-id>	member ID<1-8>.
	HH:MM:SS	Delay before reload(HH:MM:SS).
	<days-id>	Days to delay before reload <1-30>.
Default	None.	
Mode	Admin Mode	
Usage Guide	The user can use this command to restart the switch continuously.	
Example	Hot restart switch.	
	Switch#reload	

service advanced-vty

Command	service advanced-vty	
	no service advanced-vty	
Parameter	none	none

Default	No service advanced-vty by system default.
Mode	Global Mode
Usage Guide	This command enables advanced VTY terminal features, including enhanced command completion and optimized remote login session control..
	no service advanced-vty command disables these advanced VTY functions.
Example	Enable advanced mode vty interface. Switch(config)# service advanced-vty

service password-encryption

Command	service password-encryption no service password-encryption
Parameter	none none
Default	No service password-encryption by system default.
Mode	Global Mode
Usage Guide	The current unencrypted passwords as well as the coming passwords configured by password, enable password, ip ftp and username command will be encrypted by executed this command. no service password-encryption cancels this function however encrypted passwords remain unchanged.
Example	Encrypt system passwords. Switch(config)#service password-encryption

set default

Command	set default vsf
Parameter	none none
Default	None.

Mode	Admin Mode
Usage Guide	This command clears all user VSF stack configurations and restores VSF parameters to factory defaults. Note: Execute the write command to save configuration after running this command, then reload the switch for the changes to take effect.
Example	Restore factory settings and restart. Switch#set default vsf Are you sure? [Y/N] = y Switch#write Switch#reload

service terminal-length

Command	service terminal-length <0-512> no service terminal-length	
Parameter	<0-512>	Columns of characters displayed on each screen of vty, ranging between 0-512
Default	None.	
Mode	Global Mode	
Usage Guide	Use this command, configure the columns of characters displayed on each screen of the terminal. The columns of characters displayed on each screen on the telnet ssh client and the Console will be following this configuration. The “no service terminal-length” command cancels the screen shifting operation.	
Example	Set the number of vty threads to 20. Switch(config)#service terminal-length 20	

sysContact

Command	sysContact <LINE> no sysContact
Parameter	<LINE> the prompt character string, range from 0 to 255 characters
Default	The default is factory setting.
Mode	Global Mode
Usage Guide	With this command,the user can set the factory contact mode bases the fact instance. The “no sysContact” command reset the switch to factory settings.
Example	Set the factory contact mode to test. Switch(config)#sysContact test

sysLocation

Command	sysLocation<LINE> no sysLocation
Parameter	<LINE> the prompt character string, range from 0 to 255 characters
Default	The default is factory setting.
Mode	Global Mode
Usage Guide	With this command,the user can set the factory address bases the fact instance. The “no sysLocation” command reset the switch to factory settings.
Example	Set the factory address to test. Switch(config)#sysLocation test

set boot password

Command	set {boot [password] sn <WORD> asset [id <WORD>]} no set {boot [password] sn asset [id]}
Parameter	<WORD> Name of asset identifier<1-32>any character
Default	None.
Mode	Global Mode
Usage Guide	Under the img mode, configure the password of entering the bootrom mode next time; under the global mode, input this command and the password according to the prompt and confirm it, then successfully to configure. Notice: the characters length of the password is from 3 to 32. The no command cancels the password.
Example	Sets the password when entering boot mode. Switch(config)#set boot password New password :***** Confirm password :***** Set password success!

setup

Command	setup
Parameter	none none
Default	None.
Mode	Admin Mode
Usage Guide	Switch provides a Setup Mode, in which the user can configure IP addresses, etc.
Example	Enter setup mode. Switch#setup

show clock

Command	show clock
Parameter	none none
Default	None.
Mode	Admin Mode.
Usage Guide	Displays the current system clock.
Example	Displays the current system clock. Switch#show clock Current time is TUE AUG 22 11: 00: 01 2002

show cpu usage

Command	show cpu usage {<cr> member <member-id>}
Parameter	<member-id> Member ID <1-8>
Default	None.
Mode	Admin and configuration mode
Usage Guide	Display current, past 5 seconds, past 30 seconds, past 5 minutes CPU usage by this command. Only the chassis switch uses slotno parameter which is used to show the CPU usage rate of the card on specified slot, if there is no parameter, the default is current card.
Example	Show the current usage rate of CPU. 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%

show cpu utilization

Command	show cpu utilization {<cr> member <member-id>}
Parameter	<member-id> Member ID <1-8>
Default	None.
Mode	Admin and configuration mode
Usage Guide	This command is used to show CPU utilization rate in the past 5 seconds, 30 seconds and 5 minutes.。
Example	Displays 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%

show cpu monitor

Command	show cpu monitor {<cr> member <member-id>}
Parameter	<member-id> Member ID <1-8>
Default	None.
Mode	Admin and configuration mode
Usage Guide	This command is used to show CPU utilization for 5 seconds, 1 minutes and 5 minutes.。 show CPU utilization per five second in the past 60 seconds , minute in the past 60 minutes and quarter in the past 96 quarters
Example	Displays CPU monitor.

Switch#show cpu monitor

CPU utilization for five seconds: 3%; one minutes: 3%; five minutes: 3%

CPU utilization per five second in the past 60 seconds:

3%	3%	3%	3%	3%	3%
3%	3%	3%	3%	3%	3%

CPU utilization per minute in the past 60 minutes:

3%	3%	3%	3%	3%	3%	3%	3%	3%	3%
3%	3%	3%	3%	3%	3%	3%	3%	3%	3%
3%	3%	3%	3%	3%	3%	3%	3%	3%	3%
3%	3%	3%	3%	3%	3%	3%	3%	3%	3%
3%	3%	3%	3%	3%	3%	3%	3%	3%	3%
3%	3%	3%	3%	3%	3%	3%	3%	3%	3%

CPU utilization per quarter in the past 96 quarters:

3%	3%	3%	3%	3%	3%	3%	3%
3%	3%	3%	3%	3%	3%	3%	3%
3%	3%	3%	3%	3%	3%	3%	3%
3%	3%	3%	3%	3%	3%	3%	3%
3%	3%	3%	3%	3%	3%	3%	3%
3%	3%	3%	3%	3%	3%	3%	3%
3%	3%	3%	3%	3%	3%	3%	3%
3%	3%	3%	3%	3%	3%	3%	3%
3%	3%	3%	3%	3%	3%	3%	3%
3%	3%	3%	3%	3%	3%	3%	3%
3%	3%	3%	3%	3%	3%	3%	3%
3%	3%	3%	3%	3%	3%	3%	3%

show memory usage

Command **show memory usage {<cr> | member <member-id>}**

Parameter	<member-id>	Member ID <1-8>

Default None.

Mode Admin and configuration mode

Usage Guide Show memory usage rate.
Only the chassis switch uses slotno parameter which is used to show the memory usage rate of card

on the specified slot, if there is no parameter, the default is current card.

Example

Show the current usage rate of the memory.

Switch#show memory usage

The memory total 128 MB, free 58914872 bytes, usage is 56.10%

show privilege

Command

show privilege

Parameter

none	none

Default

None.

Mode

Global Mode

Usage Guide

Show privilege of the current user.

Example

Show privilege of the current user.

Switch(config)#show privilege

Current privilege level is 15

show privilege mode LINE

Command

show privilege {mode} LINE

Parameter

mode	register mode of the command, 'Tab' or '?' is able to show all register modes, Example: Med-Civic, bgp-ipv4, bgp-ipv4-lu, bgp-ipv4-vrf.....
LINE	the command needs to be configured, it supports the command abbreviation

Default

None.

Mode

Admin mode/Global mode

Usage Guide	Show the level of the specified command. LINE must be the whole command format, the abbreviation format is used to the command which can be analyzed successfully. For half-baked command, false command about writing and command that abbreviation cannot be analyzed successfully, the level of them cannot be shown.
Example	Show the level of privilege command. Switch(config)#show privilege exec show ip route The command : show ip route Privilege is : 15

show tech-support

Command	show tech-support [no-more]	
Parameter	[no-more]	Display the operational information and the task status of the switch directly, do not connect the user by “more”.
Default	None.	
Mode	Admin mode/Global mode	
Usage Guide	This command is used to collect the relative information when the switch operation is malfunctioned. Display the operational information and the task status of the switch. The technique specialist use this command to diagnose whether the switch operate normally.	
Example	Displays the operational information and the task status of the switch. Switch#show tech-support	

show version

Command	show version

Parameter	none none
Default	None.
Mode	Admin mode/Global mode
Usage Guide	This command is used to show the version of the switch, it includes the hardware version and the software version information.
Example	Display the version information of the switch. Switch#show version

username

Command	username <username> [privilege <privilege>] [password [0 7]<password>] no username <username>	
Parameter	<username>	the username, its range should not exceed 32 characters
	<privilege>	the maximum privilege level of the commands that the user is able to execute, its value is limited between 1 and 15, and 1 by default
	[0 7]	If input option 0 on password setting, the password is not encrypted; if input option 7, the password is encrypted (Use 32 bits password encrypted by MD5)
	<password>	password for the user
Default	None.	
Mode	Global Mode	
Usage Guide	Configure local login username and password along with its privilege level. 16 local users at most can be configured through this command, and the maximum length of the password should be no less than 32. The user can log in user and priority after the command configures, before issuing the command authentication line console login local, it should be made sure that at one user has be configured as preference level of 15, in order to login the switch and make configuration changes in privileged mode and global mode. If there are no configured local users with preference level of 15, while only Local authentication is configured for the Console login method, the switch can be login without any authentication. When using the HTTP method to login the switch, only users with preference level of 15 can login the switch, users with preference level other than 15 will be denied.	

The no command delete user.

Example

Configure an administrator account named admin, with the preference level as 15. And configure two normal accounts with its preference level as 1. Then enable local authentication method.

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

web-auth privilege <1-15>

Command

web-auth privilege <1-15>
no web-auth privilege

Parameter

<1-15>	Appoint the level of logging in the switch by web and the range is from 1 to 15

Default

The default level is 15.

Mode

Global Mode

Usage Guide

Configure the level of logging in the switch by web.
After configured the level of logging in the switch by web, only the user with the level that is equal to or higher than it can login in the switch by web.

Example

Configure the level of logging in the switch by web as 10.

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

write

Command

write

Parameter

none	none

Default	None.
Mode	Admin Mode
Usage Guide	Save the currently configured parameters to the Flash memory. After a set of configuration with desired functions, the setting should be saved to the specified configuration file, so that the system can revert to the saved configuration automatically in the case of accidentally powered off or power failure. This is the equivalent to the copy running-config startup-config command.
Example	Save the current configuration. Switch#write

write running-config

Command	write running-config [<startup-config-file-name>]
Parameter	[<startup-config-file-name>] the full path of the cfg file
Default	None.
Mode	Admin Mode
Usage Guide	Save the current running config as .cfg file to Flash Memory. The file path comprises of two parts: device prefix used as the root directory (flash:/) and the file name. No space is allowed in each part or between two parts. The suffix of all file names should be .cfg. The length of the full file path should not be longer than 128 characters, while the file name cannot be longer than 80 characters.
Example	Save the current running config as .cfg file with name of 123. Switch#write running-config 123.cfg

2 Commands for Telnet

aaa authorization config-commands

Command	aaa authorization config-commands no aaa authorization config-commands	
Parameter	none	none
Default	By default,disable.	
Mode	Global Mode	
Usage Guide	Enable command authorization function for the login user with VTY (login with Telnet and SSH). Only enabling this command and configuring command authorization manner, it will request to authorize when executing some command. The no command disables this function.	
Example	Enable VTY command authorization function. Switch(config)#aaa authorization config-commands	

accounting exec

Command	accounting line {console vty} exec {start-stop stop-only none} method1 [method2...] no accounting line {console vty} exec	
Parameter	console	log in through serial port
	vty	log in through telnet or ssh
	start-stop	sends the accounting start or the accounting stop when the user is logging or exit the login
	stop-only	sends the accounting stop when the user exits the login only
	none	does not send the accounting start or the accounting stop
	method	the list of the accounting method, it only supports tacacs keyword; tacacs uses the remote TACACS+ server to count
Default	By default there is no accounting.	

Mode	Global Mode
Usage Guide	Configure the list of the accounting method for the login user with VTY (login with Telnet and SSH) and Console. console and vty login method are able to set the corresponding accounting method respectively, the accounting method only supports TACACS+ method currently. The no command restores the default accounting method.
Example	Configure the login accounting with the telnet method. Switch(config)#accounting line vty exec start-stop tacacs

accounting command

Command	accounting line {console vty} command <1-15> {start-stop stop-only none} method1 [method2...] no accounting line {console vty} command <1-15>	
Parameter	console	log in through serial port
	vty	log in through telnet or ssh
	command <1-15>	the level of the accounting command
	start-stop	sends the accounting start or the accounting stop when the user is logging or exit the login
	stop-only	sends the accounting stop when the user exits the login only
	none	does not send the accounting start or the accounting stop
	method	the list of the accounting method, it only supports tacacs keyword; tacacs uses the remote TACACS+ server to count
Default	By default there is no accounting method.	
Mode	Global Mode	
Usage Guide	Configure the list of the command accounting method with VTY (login with Telnet and SSH) and Console. The no command restores the default accounting method. console and vty login method are able to set the corresponding command accounting method respectively, the accounting method only supports TACACS+ method currently. Only the stop information of the accounting is recorded, whether command accounting configures start-stop method or stop-only method. The no command restores the default accounting method.	

Example

Configure command audit methods through telnet login, command level 15.

Switch(config)#authorization line vty command 15 start-stop tacacs

authentication enable

Command

authentication enable { local | radius | tacacs }
no authentication enable

Parameter

{local|radius| tacacs } the list of the authentication method, it must be among local, tacacs and radius keywords;
local:uses the local database to authenticate;
tacacs:uses the remote TACACS+ authentication server to authenticate;
radius:uses the remote RADIUS authentication server to authenticate

Default

The local authentication is enable command by default.

Mode

Global Mode

Usage Guide

Configure the list of the enable authentication method.

The enable authentication method can be any one or combination of Local,RADIUS and TACACS. When login method is configuration in combination, the preference goes from left to right.

If the users have passed the authentication method, authentication method of lower preferences will be ignored.

To be mentioned, if the user receives corresponding protocol's answer whether refuse or incept, it will not attempt the next authentication method (Exception: if the local authentication method failed, it will attempt the next authentication method); it will attempt the next authentication method if it receives nothing.

And AAA function RADIUS server should be configured before the RADIUS configuration method can be used. And TACACS server should be configured before the TACACS configuration method can be used.

The no command restores the default authentication method.

Example

Configure the enable authentication method to be tacacs and local.

Switch(config)#authentication enable tacacs local

authentication ip access-class

Command	authentication ip access-class {<1-99> <100-199> <200-299> <WORD>} in { ssh telnet web <cr>} no authentication ip access-class	
Parameter	< WORD >	the access-class name for standard ACL, the character string length is ranging between 1 and 64
Default	The binding ACL to Telnet/SSH/Web function is closed by default.	
Mode	Global Mode	
Usage Guide	Binding standard IP ACL protocol to login with Telnet/SSH/Web. The no form command will cancel the binding ACL.	
Example	Binding standard IP ACL protocol to access-class 1. Switch(config)#authentication ip access-class 1 in	

authentication ipv6 access-class

Command	authentication ipv6 access-class {<num-std> <name>} in { ssh telnet web <cr>} no authentication ipv6 access-class	
Parameter	<num-std>	the access-class number for standard numeric ACL, ranging between 500-599
	<name>	the access-class name for standard ACL, the character string length is ranging between 1 and 64
Default	The binding ACL to Telnet/SSH/Web function is closed by default.	
Mode	Global Mode	
Usage Guide	Binding standard IPv6 ACL protocol to login with Telnet/SSH/Web. The no form command will cancel the binding ACL.	
Example	Binding standard IP ACL protocol to access-class 500. Switch(config)#authentication ipv6 access-class 500 in	

authentication line login

Command	authentication line {console vty web} login {local radius tacacs} no authentication line {console vty web} login	
Parameter	console	log in through serial port
	vty	log in through telnet or ssh
	web	log in through web
	method	the list of the authentication method, it must be among local, tacacs and radius keywords; local:uses the local database to authenticate; tacacs:uses the remote TACACS+ authentication server to authenticate; radius:uses the remote RADIUS authentication server to authenticate
Default	No configuration is enabled for the console login method by default. Local authentication is enabled for the VTY and Web login method by default.	
Mode	Global Mode	
Usage Guide	Configure VTY (login with Telnet and SSH), Web and Console, so as to select the list of the authentication method for the login user. Authentication method can be any one or combination of Local, RADIUS and TACACS. When login method is configuration in combination, the preference goes from left to right. If the users have passed the authentication method, authentication method of lower preferences will be ignored. if the user receives corresponding protocol's answer whether refuse or incept, it will not attempt the next authentication method (Exception: if the local authentication method failed, it will attempt the next authentication method); it will attempt the next authentication method if itreceives nothing. And AAA function RADIUS server should be configured before the RADIUS configuration method can be used. And TACACS server should be configured before the TACACS configuration method can be used. The authentication line console login command is exclusive with the “login”command. The authentication line console login command configures the switch to use the Console login method. And the login command makes the Console login to use the passwords configured by the password command for authentication. If local authentication is configured while no local users are configured, users will be able to login the switch via the Console method. The no form command restores the default authentication method.	
Example	Configure the telnet and ssh login with the remote RADIUS authentication.	

Switch(config)#authentication line vty login radius

authentication securityip

Command	authentication securityip <ip-addr> no authentication securityip <ip-addr>	
Parameter	<ip-addr>	the trusted IP address of the client in dotted decimal format which can login the switch
Default	No trusted IP address is configured by default.	
Mode	Global Mode	
Usage Guide	To configure the trusted IP address for Telnet and HTTP login method. IP address of the client which can login the switch is not restricted before the trusted IP address is not configured. After the trusted IP address is configured, only clients with trusted IP addresses are able to login the switch. Up to 32 trusted IP addresses can be configured in the switch. The no form of this command will remove the trusted IP address configuration.	
Example	To configure 192.168.1.21 as the trusted IP address. Switch(config)#authentication securityip 192.168.1.21	

authentication securityipv6

Command	authentication securityipv6 <ipv6-addr> no authentication securityipv6 <ipv6-addr>	
Parameter	<ip-addr>	the security IPv6 address which can login the switch
Default	No security IPv6 addresses are configured by default.	
Mode	Global Mode	

Usage Guide

To configure the security IPv6 address for Telnet and HTTP login method.
IPv6 address of the client which can login the switch is not restricted before the security IPv6 address is not configured.

After the security IPv6 address is configured, only clients with security IPv6 addresses are able to login the switch.

Up to 32 security IPv6 addresses can be configured in the switch.

The no form of this command will remove the specified configuration.

Example

Configure the security IPv6 address is 2001:da8:123:1::1.

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

authorization

Command

authorization line {console | vty | web} exec {local | radius | tacacs}

no authorization line {console | vty | web} exec

Parameter

console	log in through serial port
vty	log in through telnet or ssh
web	log in through web
{local radius tacacs}	the list of the authentication method, it must be among local, tacacs and radius keywords; local:uses the local database to authenticate; tacacs:uses the remote TACACS+ authentication server to authenticate; radius:uses the remote RADIUS authentication server to authenticate

Default

There is no authorization method by default.

Mode

Global Mode

Usage Guide

Configure the list of the authorization method for the login user with VTY (login with Telnet and SSH), Web and Console.

And authorization method can be any one or combination of Local,RADIUS or TACACS.

When login method is configuration in combination, the preference goes from left to right.

If the users have passed the authorization method, authorization method of lower preferences will be ignored.

if the user receives corresponding protocol's answer whether refuse or incept, it will not attempt the next authorization method; it will attempt the next authorization method if it receives nothing.

And AAA function RADIUS server should be configured before the RADIUS configuration method can be used. And TACACS server should be configured before the TACACS configuration method can be used.

The local users adopt username command permission while authorization command is not configured, the users login the switch via RADIUS/TACACS method and works under common mode.

The no command restores the default authorization method.

Example

Configure the telnet authorization method to RADIUS.

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

authorization line vty command

Command

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

Parameter

command <1-15>	Level scope of authorization orders 1~15
local	Authorization is granted locally
radius	Authorization for remote radius
tacacs	Authorization for remote tacacs
none	Authorization mode is empty

Default

The authorization manner is not configured as default.

Mode

Global Mode

Usage Guide

Configure command authorization manner and authorization selection priority of login user with VTY (login with Telnet and SSH).

The enabling authorization method can be any one or combination of Local. RADIUS and TACACS.

When using combination authorization manners, the priority of the front authorization manner is the highest and the others are in descending order.

If the authorization with high priority passed, it is successful to configure command and the back authorization manner will be ignored.

As long as one authorization manner receives a clear response of the corresponding agreement. Whether it is received or refused, the next authorization manner will not be attempted. If the clear response is not received, try the next manner.

When using RADIUS authorization, AAA function must be enabled and configure RADIUS server. when using TACACS authorization, TACACS server must be configured.

None is the manner of escaping and it only can be the last manner.

This manner returns to passed authorization directly and it is successful to configure the command.

The no command recovers to be default manner.

Example

Configure level 1 command authorization manner of telnet login user as TACACS.

Switch(config)#authorization line vty command 1 tacacs

clear line vty <0-31>

Command

clear line vty <0-31>

Parameter

<0-31> appointed line

Default

None.

Mode

Admin Mode

Usage Guide

After inputting this command, there is need to judge for this command, “Confirm[Y/N]: “, when inputting “Y” or “y”, run to delete; when inputting “? “, do not run to delete, print the notice information only. When inputting other characters, do not run to delete.

Example

Admin users who are forced to log in through VTY (using Telnet or SSH login) are off line.

Switch#clear line vty 0

Confirm[Y/N]:y

[OK]

crypto key clear rsa

Command

crypto key clear rsa

Parameter

none none

Default

None.

Mode

Admin Mode

Usage Guide

This command is used to clear the secret key of the ssh and close the ssh service.

Example

Clear the secret key of the ssh and close the ssh service.

Switch#crypto key clear rsa

ssh host key is cleared successfully.

ssh is closed successfully.

terminal length

Command

terminal length <0-512>

terminal no length

Parameter

<0-512>

Length of characters displayed in each screen, ranging between 0-512 (0 refers to non-stop display)

Default

Default Length is 25.

Mode

Admin Mode

Usage Guide

Set length of characters displayed in each screen on terminal, so that the-More-message will be shown when displayed information exceeds the screen. Press any key to show information in next screen.

The “terminal no length” cancels the screen switching operation and display content once in all.

Example

Configure length of characters in each display to 20.

Switch#terminal length 20

telnet

Command

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

Parameter

<vrf-name>

the specific VRF name

<ip-addr>

the IP address of the remote host, shown in dotted decimal notation

<ipv6-addr>

the IPv6 address of the remote host

<hostname>

the name of the remote host, containing max 64 characters

<port>

the port number, ranging between 0 and 65535

Default	None.
Mode	Admin Mode
Usage Guide	This command is used when the switch is applied as Telnet client, for logging on remote host to configure. When a switch is applied as a Telnet client, it can only establish one TCP connection with the remote host. To connect to another remote host, the current TCP connection must be disconnected with a hotkey “CTRL+ \”. To telnet a host name, mapping relationship between the host name and the IP/IPv6 address should be previously configured. For required commands please refer to ip host and ipv6 host. In case a host corresponds to both an IPv4 and an IPv6 addresses, the IPv6 should be preferred when telneting this host name.
Example	The switch telnets to a remote host whose IP address is 20.1.1.1. <pre> 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> </pre>

telnet server enable

Command	telnet-server enable no telnet-server enable
Parameter	none none
Default	Telnet server function is enabled by default.
Mode	Global Mode
Usage Guide	Enable the Telnet server function in the switch This command is available in Console only. The administrator can use this command to enable or disable the Telnet client to login to the switch. The “no telnet server enable” command disables the Telnet function in the switch.

Example

Disable the Telnet server function in the switch.

Switch(config)# no telnet-server enable

telnet-server max-connection

Command

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

Parameter

<max-connection-number> the max connection number supported by the Telnet service, ranging from 1 to 16

default restore the default configuration

Default

The system default value of the max connection number is 5.

Mode

Global Mode

Usage Guide

Configure the max connection number supported by the Telnet service of the switch.

Example

Set the max connection number supported by the Telnet service as 10.

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

ssh-server authentication-retries

Command

ssh-server authentication-retries <authentication-retries>
no ssh-server authentication-retries

Parameter

<authentication-retries> the number of times for retrying authentication, valid range is 1 to 10

Default

The number of times for retrying SSH authentication is 3 by default.

Mode

Global Mode

Usage Guide

Configure the number of times for retrying SSH authentication.

The “no ssh-server authentication-retries” command restores the default number of times for retrying SSH authentication.

Example

Set the time for retrying SSH authentication to 5.

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

ssh-server enable

Command	ssh-server enable no ssh-server enable
Parameter	none none
Default	SSH function is disabled by default.
Mode	Global Mode
Usage Guide	Enable SSH function on the switch. In order that the SSH client can log on the switch, the users need to configure the SSH user and enable SSH function on the switch. The “no ssh-server enable” command disables SSH function.
Example	Enable SSH function on the switch. Switch(config)#ssh-server enable

ssh-server host-key create rsa

Command	ssh-server host-key create rsa [modulus < modulus >]
Parameter	< modulus > the modulus which is used to compute the host key; valid range is 768 to 2048. The default value is 1024
Default	The system uses the key generated when the ssh-server is started at the first time.
Mode	Global Mode
Usage Guide	This command is used to generate a new SSH service host rsa key.

When SSH client logs on the server, the new host key is used for authentication. After the new host key is generated and “write” command is used to save the configuration, the system uses this key for authentication all the time. Because it takes quite a long time to compute the new key and some clients are not compatible with the key generated by the modulus 2048, it is recommended to use the key which is generated by the default modulus 1024.

No command disables SSH service.

Example

Generate new host key.

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

ssh-server max-connection

Command

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

Parameter

<max-connection-number>	the max connection number supported by the SSH service, ranging from 1 to 16.
default	restore default

Default

The system default value of the max connection number is 5.

Mode

Global Mode

Usage Guide

Configure the max connection number supported by the SSH service of the switch.

Example

Set the max connection number supported by the SSH service as 10.

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

ssh-server timeout

Command

ssh-server timeout <timeout>
no ssh-server timeout

Parameter

<timeout>	timeout value; valid range is 10 to 600 seconds

Default	SSH authentication timeout is 180 seconds by default.
Mode	Global Mode
Usage Guide	Configure timeout value for SSH authentication. The “no ssh-server timeout”command restores the default timeout value for SSH authentication.
Example	Set SSH authentication timeout to 240 seconds. Switch(config)#ssh-server timeout 240

show crypto key

Command	show crypto key
Parameter	none none
Default	None.
Mode	Admin Mode
Usage Guide	Show the secret key of ssh.
Example	Show the secret key of ssh. Switch#show crypto key

show ssh-server

Command	show ssh-server
Parameter	none none
Default	None.
Mode	Admin Mode

Usage Guide Display SSH state and users which log on currently.

Example Display SSH state and users which log on currently.

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

show telnet login

Command show telnet login

Parameter none none

Default None.

Mode Admin Mode

Usage Guide Display the information of the Telnet client which currently establishes a Telnet connection with the switch.

Example Display Telnet client information.

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

show users

Command show users

Parameter none none

Default	None.															
Mode	Admin Mode															
Usage Guide	Show the user information who logs in through telnet or ssh. It includes line number, user name and user IP. Because 16 telnet users and 16 ssh users are supported at most currently, vty0-15 are used for telnet, and 16-31 are used for ssh.															
Example	Displays user information. Switch#show users <table><tr><td>Line</td><td>User</td><td>Location</td></tr><tr><td>vty 16</td><td>a</td><td>192.168.1.1</td></tr><tr><td>vty 0</td><td>admin</td><td>192.168.1.2</td></tr><tr><td>vty 17</td><td>mab</td><td>192.168.1.13</td></tr><tr><td>vty 1</td><td>test</td><td>192.168.1.40</td></tr></table>	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
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														

who

Command	who
Parameter	none none
Default	None.
Mode	All configuration modes
Usage Guide	Show the current login users with vty.
Example	Show the current login users with vty. <pre>Switch#who</pre> Telnet user a login from 192.168.1.20

3 Commands for Configuring Switch IP

interface vlan

Command	interface vlan <vlan-id> no interface vlan <vlan-id>		
Parameter	<table><tr><td><vlan-id></td><td>the VLAN ID of an existing VLAN, ranging from 1 to 4094</td></tr></table>	<vlan-id>	the VLAN ID of an existing VLAN, ranging from 1 to 4094
<vlan-id>	the VLAN ID of an existing VLAN, ranging from 1 to 4094		
Default	None.		
Mode	Global Mode		
Usage Guide	This command is used enter the VLAN interface configuration mode Users should first make sure the existence of a VLAN before configuring it. User “exit” command to quit the VLAN interface configuration mode back to the global configuration mode. the no operation of this command will delete the existing VLAN interface.		
Example	Enter the VLAN interface configuration mode of VLAN1. Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#		

ip address

Command	ip address <ip-address> <mask> [secondary] no ip address [<ip-address> <mask>] [secondary]						
Parameter	<table><tr><td><ip-address></td><td>the IP address in dot decimal format</td></tr><tr><td><mask></td><td>the subnet mask in dot decimal format</td></tr><tr><td>[secondary]</td><td>indicates the IP configured is a secondary IP address</td></tr></table>	<ip-address>	the IP address in dot decimal format	<mask>	the subnet mask in dot decimal format	[secondary]	indicates the IP configured is a secondary IP address
<ip-address>	the IP address in dot decimal format						
<mask>	the subnet mask in dot decimal format						
[secondary]	indicates the IP configured is a secondary IP address						
Default	No IP address is configured upon switch shipment.						
Mode	VLAN Interface Mode						
Usage Guide	Set the IP address and mask for the specified VLAN interface. A VLAN interface must be created first before the user can assign an IP address to the switch. The no command deletes the specified IP address setting.						

Example

Set 10.1.128.1/24 as the IP address of VLAN1 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)#
```

ipv6 address

Command

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

Parameter

<ipv6address >	the prefix of an IPV6 address
<prefix-length>	the length of the prefix of an IPV6 address, ranging from 3 to 128
[eui-64]	means that the eui64 interface id of the interface will automatically create an IPV6 address

Default

No IPv6 address is configured upon switch shipment.

Mode

VLAN Interface Mode

Usage Guide

Configure aggregatable global unicast address, site-local address and link-local address for the interface.

The prefix of an IPV6 address should not be a multicast address, or other kinds of IPV6 addresses with specific usage.

Different layer-three VLAN interfaces are forbidden to share a same address prefix. As for any global unicast address, the prefix should be limited in the range from 2001:: to 3fff::, with a length no shorter than 3. And the prefix length of a site-local address or a link-local address should not be shorter than 10.

The no command deletes the specified IPv6 address setting.

Example

Configure an IPV6 address at the layer-three interface of VLAN1: set the prefix as 2001:3f:ed8::99, the length of which is 64.

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 address 2001:3f:ed8::99/64
Switch(Config-if-Vlan1)#exit
Switch(config)#
```

ip bootp-client enable

Command	ip bootp-client enable no ip bootp-client enable
Parameter	none none
Default	BootP client function is disabled by default.
Mode	VLAN Interface Mode
Usage Guide	Enable the switch to be a BootP Client and obtain IP address and gateway address through BootP negotiation. Obtaining IP address through BootP, Manual configuration and DHCP are mutually exclusive, enabling any two methods for obtaining IP address is not allowed. To obtain IP address via BootP, a DHCP server or a BootP server is required in the network. The no command disables the BootP Client function and releases the IP address obtained in BootP.
Example	Get IP address through BootP. <pre>Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ip bootp-client enable Switch(Config-if-Vlan1)#exit Switch(config)#</pre>

ip dhcp-client enable

Command	ip dhcp-client enable no ip dhcp-client enable
Parameter	none none
Default	By default, the dhcp service is disabled.
Mode	VLAN Interface Mode

Usage Guide

Enables the switch to be a DHCP client and obtain IP address and gateway address through DHCP negotiation.

To obtain IP address via DHCP, a DHCP server is required in the network.

Obtaining IP address by DHCP, Manual configuration and BootP are mutually exclusive, enabling any 2 methods for obtaining an IP address is not allowed.

The no command disables the DHCP client function and releases the IP address obtained in DHCP.

Example

Getting 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)#
```

4 Commands for SNMP

rmon enable

Command	rmon enable no rmon enable
Parameter	none none
Default	RMON is enabled by default.
Mode	Global Mode
Usage Guide	This command is used to enable RMON remote network monitoring protocol. The no command disables RMON.
Example	Disable RMON. Switch(config)#no rmon enable

show private-mib oid

Command	show private-mib oid
Parameter	none none
Default	None.
Mode	Admin and configuration mode
Usage Guide	Show the original oid of the private mib. Check the beginning oid of the private mib by show private-mib oid command.
Example	Show the original oid of the private mib. Switch#show private-mib oid Private MIB OID:1.3.6.1.4.1.6339

show snmp

Command	show snmp
Parameter	none none
Default	None.
Mode	Admin and configuration mode
Usage Guide	Display all SNMP counter information.
Example	Display all SNMP counter information. Switch#show snmp 0 SNMP packets input 0 Bad SNMP version errors 0 Unknown 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

show snmp engineid

Command	show snmp engineid

Parameter	none none
Default	None.
Mode	Admin and configuration mode
Usage Guide	Display the engine ID commands.
Example	Display the engine ID commands. Switch#show snmp engineid SNMP engineID:3138633303f1276c

show snmp group

Command	show snmp group
Parameter	none none
Default	None.
Mode	Admin and configuration mode
Usage Guide	Display the group information .
Example	Display the group information . Switch#show snmp group Group Name:initial Security Level:noAuthnoPriv Read View:one Write View:<no writeview specified> Notify View:one

show snmp mib

Command	show snmp mib

Parameter	none none
Default	None.
Mode	Admin and configuration mode
Usage Guide	Display all MIB supported by the switch.
Example	Display all MIB supported by the switch. Switch#show snmp mib

show snmp status

Command	show snmp status
Parameter	none none
Default	None.
Mode	Admin and configuration mode
Usage Guide	Display SNMP configuration information.
Example	Display SNMP configuration information. Switch#show snmp status Trap enable RMON enable Community Information: V1/V2c Trap Host Information: V3 Trap Host Information: Security IP Information:

show snmp user

Command	show snmp user

Parameter	none none
Default	None.
Mode	Admin and configuration mode
Usage Guide	Display the user information commands.
Example	Display the user information commands. Switch#show snmp user User name: initialsha Engine ID: 1234567890 Auth Protocol:MD5 Priv Protocol:DES-CBC Row status:active

show snmp view

Command	show snmp view
Parameter	none none
Default	None.
Mode	Admin and configuration mode
Usage Guide	Display the view information.
Example	Display the view information. Switch#show snmp view View Name :readview 1. -Included active 1.3. Excluded active

snmp-server community

Command

```
snmp-server community {ro | rw} <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>}]
```

Parameter	{ro rw}	the specified access mode to MIB, ro for read-only and rw for read-write
	<string>	the configured community string <1-255> character
	<num-std>	the access-class number for standard numeric ACL, ranging between 1-99
	<name>	the access-class name for standard ACL, the character string length is ranging between 1-64
	<ipv6-num-std>	the access-class number for standard numeric IPv6 ACL, ranging between 500-599
	<ipv6-name>	the access-class name for standard IPv6 ACL, the character string length is ranging between 1-64
	<read-view-name>	the name of readable view which includes 1-32 characters
	<write-view-name>	the name of writable view which includes 1-32 characters

Default None.

Mode Global Mode

Usage Guide

Configure the community string for the switch.

The switch supports up to 4 community strings. It can realize the access-control for specifically community view by binding the community name to specifically readable view or writable view.

The no command deletes the configured community string.

Example

Add a community string 5 with write 10.

```
Switch(config)#snmp-server community rw 5 write 10
```

Delete the community string named “private”.

```
Switch(config)#no snmp-server community 5
```

snmp-server enable

Command

```
snmp-server enable
no snmp-server enable
```

Parameter	none	none

Default	None.
Mode	Global Mode
Usage Guide	Enable the SNMP proxy server function on the switch. To perform configuration management on the switch with network manage software, the SNMP proxy server function has to be enabled with this command. The “no snmp-server enable” command disables the SNMP proxy server function.
Example	Enable the SNMP proxy server function on the switch. Switch(config)#snmp-server enable

snmp-server enable traps

Command	snmp-server enable traps no snmp-server enable traps
Parameter	none none
Default	By default forbid to send Trap message.
Mode	Global Mode
Usage Guide	Enable the switch to send Trap message. When Trap message is enabled, if Down/Up in device ports or of system occurs,the device will send Trap messages to NMS that receives Trap messages. The no command disables the switch to send Trap message.
Example	Enable to send Trap messages. Switch(config)#snmp-server enable traps

snmp-server engineid

Command	snmp-server engineid <engine-string> no snmp-server engineid		
Parameter	<table><tr><td><engine-string></td><td>the engine ID shown in 1-32 digit hex characters</td></tr></table>	<engine-string>	the engine ID shown in 1-32 digit hex characters
<engine-string>	the engine ID shown in 1-32 digit hex characters		
Default	Default value is the company ID plus local MAC address.		
Mode	Global Mode		
Usage Guide	Configure the engine ID. The “no” form of this command restores to the default engine ID.		
Example	Set current engine ID to A66688999F Switch(config)#snmp-server engineid A66688999F		

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>}]																				
Parameter	<table><tr><td><group-string></td><td>group name which includes 1-32 characters</td></tr><tr><td>NoauthNopriv</td><td>Applies the non recognizing and non encrypting safety level</td></tr><tr><td>AuthNopriv</td><td>Applies the recognizing but non encrypting safety level</td></tr><tr><td>AuthPriv</td><td>Applies the recognizing and encrypting safety level</td></tr><tr><td><read-string></td><td>Name of readable view which includes 1-32 characters</td></tr><tr><td><write-string></td><td>Name of writable view which includes 1-32 characters</td></tr><tr><td><notify-string></td><td>Name of trappable view which includes 1-32 characters</td></tr><tr><td><num-std></td><td>the access-class number for standard numeric ACL, ranging between 1-99</td></tr><tr><td><name></td><td>the access-class name for standard ACL, the character string length is ranging between 1-32</td></tr><tr><td><ipv6-num-std></td><td>the access-class number for standard numeric IPv6 ACL, ranging between 500-599</td></tr></table>	<group-string>	group name which includes 1-32 characters	NoauthNopriv	Applies the non recognizing and non encrypting safety level	AuthNopriv	Applies the recognizing but non encrypting safety level	AuthPriv	Applies the recognizing and encrypting safety level	<read-string>	Name of readable view which includes 1-32 characters	<write-string>	Name of writable view which includes 1-32 characters	<notify-string>	Name of trappable view which includes 1-32 characters	<num-std>	the access-class number for standard numeric ACL, ranging between 1-99	<name>	the access-class name for standard ACL, the character string length is ranging between 1-32	<ipv6-num-std>	the access-class number for standard numeric IPv6 ACL, ranging between 500-599
<group-string>	group name which includes 1-32 characters																				
NoauthNopriv	Applies the non recognizing and non encrypting safety level																				
AuthNopriv	Applies the recognizing but non encrypting safety level																				
AuthPriv	Applies the recognizing and encrypting safety level																				
<read-string>	Name of readable view which includes 1-32 characters																				
<write-string>	Name of writable view which includes 1-32 characters																				
<notify-string>	Name of trappable view which includes 1-32 characters																				
<num-std>	the access-class number for standard numeric ACL, ranging between 1-99																				
<name>	the access-class name for standard ACL, the character string length is ranging between 1-32																				
<ipv6-num-std>	the access-class number for standard numeric IPv6 ACL, ranging between 500-599																				

	<ipv6-name> the access-class name for standard IPv6 ACL, the character string length is ranging between 1-32
Default	None.
Mode	Global Mode
Usage Guide	This command is used to configure a new group. There is a default view “v1defaultviewname” in the system. It is recommended to use this view as the view name of the notification. If the read or write view name is empty, corresponding operation will be disabled. The “no” form of this command deletes this group.
Example	Create a group CompanyGroup, with the safety level of recognizing and encrypting, the read viewname is readview, and the writing is disabled. Switch (config)#snmp-server group CompanyGroup AuthPriv read readview

snmp-server host

snmp-server host { <host-ipv4-address> <host-ipv6-address> } {v1 v2c v3 {NoauthNopriv AuthNopriv AuthPriv}}} <user-string>	
no snmp-server host { <host-ipv4-address> <host-ipv6-address> } {v1 v2c v3 {NoauthNopriv AuthNopriv AuthPriv}}} <user-string>	
<host-ipv4-address>	IP address of NMS management station which receives Trap message
<host-ipv6-address>	IPv6 address of NMS management station which receives Trap message
v1 v2c v3	the version number when sending the trap
NoauthNopriv	Applies the non recognizing and non encrypting safety level
AuthNopriv	Applies the recognizing but non encrypting safety level
AuthPriv	Applies the recognizing and encrypting safety level
<user-string>	the community character string applied when sending the Trap message at v1/v2, and will be the user name at v3

None.

Global Mode

As for the v1/v2c versions this command configures the IPv4 or IPv6 address and Trap community character string of the network manage station receiving the SNMP Trap message. And for v3

version, this command is used for receiving the network manage station IPv4 or IPv6 address and the Trap user name and safety level.

The Community character string configured in this command is the default community string of the RMON event group. If the RMON event group has no community character string configured, the community character string configured in this command will be applied when sending the Trap of RMON, and if the community character string is configured, its configuration will be applied when sending the RMON trap. This command allows to configure IPv4 or IPv6 addresses of SNMP management station that receive Trap message at the same time, but IPv4 and IPv6 addresses of v1 and v2c version are less than 8 in all.

The “no” form of this command cancels this IPv4 or IPv6 address.

Example

Configure an IP address to receive Trap.

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

snmp-server securityip

Command

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

Parameter

<ipv4-address>	NMS security IPv4 address, dotted decimal notation
<ipv6-address>	NMS security IPv6 address, colon hexadecimal

Default

None.

Mode

Global Mode

Usage Guide

Configure security IPv4 or IPv6 address allowed to access NMS management station
It is only the consistency between NMS administration station IPv4 or IPv6 address and security IPv4 or IPv6 address configured by the command, so it send SNMP packet could be processed by switch, the command only applies to SNMP. Allows configuration the IPv4 or IPv6 address of the network manage station receiving the SNMP Trap message, but the IP addresses are less than 20 in all.

The no command deletes security IPv4 or IPv6 address configured.

Example

Configure security IP address of NMS management station.

Switch(config)#snmp-server securityip 1.1.1.5

snmp-server securityip enable

Command	snmp-server securityip {enable disable}
Parameter	enable disable SNMP security ip configuration enabled or disabled
Default	Enable the security IP address authentication function.
Mode	Global Mode
Usage Guide	Enable/disable the security IP address authentication on NMS management station.
Example	Disable the security IP address authentication function. Switch(config)#snmp-server securityip disable

snmp-server trap-source

Command	snmp-server trap-source {<ipv4-address> <ipv6-address>} no snmp-server trap-source {<ipv4-address> <ipv6-address>}
Parameter	<ipv4-address> IPv4 address is used to send trap packet in dotted decimal notation <ipv6-address> IPv6 address is used to send trap packet in colon hexadecimal
Default	None.
Mode	Global Mode
Usage Guide	Set the source IPv4 or IPv6 address which is used to send trap packet. If there is no configuration, select the source address according to the interface address sent by actual trap packet, when configure the IP address, adopt the configured source address as the source address of trap packet. The no command deletes the configuration.
Example	Set the IP address which is used to send trap packet.

snmp-server user

Command `snmp-server user <use-string> <group-string> [{authPriv [auth {md5 | sha} <word>]} | {authNoPriv [{3des | aes | des} <word>]} [auth {md5 | sha} <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>}]`

Parameter	<use-string>	the user name containing 1-32 characters
	<group-string>	the name of the group the user belongs to, containing 1-32 characters
	authPriv	use DES for the packet encryption
	authNoPriv	not use DES for the packet encryption
	auth	perform packet authentication
	md5	packet authentication using HMAC MD5 algorithm
	sha	packet authentication using HMAC SHA algorithm
	3des	packet authentication using 3DES to encrypt
	aes	packet authentication using AES to encrypt
	des	packet authentication using DES to encrypt
	<word>	user password, containing 8-32 character
	<num-std>	the access-class number for standard numeric ACL, ranging between 1-99
	<name>	the access-class name for standard ACL, the character string length is ranging between 1-32
	<ipv6-num-std>	the access-class number for standard numeric IPv6 ACL, ranging between 500-599
	<ipv6-name>	the access-class name for standard IPv6 ACL, the character string length is ranging between 1-32

Default None.

Mode Global Mode

Usage Guide Add a new user to an SNMP group.
If the encryption and authentication is not selected, the default settings will be no encryption and no authentication. If the encryption is selected, the authentication must be done. When deleting a user, if correct username and incorrect group name is inputted, the user can still be deleted.

The "no" form of this command deletes this user.

Example

Add a new user tester in the UserGroup with HMAC md5 for authentication, the password is hellohello;Delete an User

Switch (config)#snmp-server user tester UserGroup authNoPriv auth md5 hellohello
Switch (config)#no snmp-server user tester

snmp-server view

Command

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

Parameter

<view-string>	view name, containing 1-32 characters
<oid-string>	OID number or corresponding node name, containing 1-255 characters
include exclude	include/exclude this OID

Default

None.

Mode

Global Mode

Usage Guide

This command is used to create or renew the view information.
The command supports not only the input using the character string of the variable OID as parameter. But also supports the input using the node name of the parameter.

the "no" form of this command deletes the view information.

Example

Create a view named readview, include iso nodes but not iso.3 nodes, and then delete them.

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

Switch(config)#no snmp-server view readview

switchport updown notification enable

Command	switchport updown notification enable no switchport updown notification enable	
Parameter	none	none
Default	Send the trap message to the port of IP/DOWN event as default.	
Mode	Port Mode	
Usage Guide	Enable/disable the function of sending the trap message to the port of UP/DOWN event. This command can control to send the trap message when the port happens the UP/DOWN event or not. As default, send the trap message to all the ports of UP/DOWN event after enabled snmp trap. The no command deletes the configuration.	
Example	Disable the function of sending the trap message to the port 1/0/1 of the UP/DOWN event. 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	

5 Commands for Switch Upgrade

copy (FTP)

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

Parameter	<source-url>	the location of the source files or directories to be copied
	<destination-url>	the destination address to which the files or directories to be copied
	ascii	ASCII standards will be adopted
	binary	File transfer will be in binary mode (default transfer method)

Default None.

Mode Admin Mode

Usage Guide This command is used to transfer files by TFTP.
When URL represents an FTP address, its form should be:
`ftp://<username>:<password>@{<ipaddress>|<ipv6address>|<hostname> }/<filename>`, amongst
`<username>` is the FTP user name, `<password>` is the FTP user password,
`<ipaddress>|<ipv6address>` is the IPv4 or IPv6 address of the FTP server/client, `<hostname>` is the
name of the host mapping with the IPv6 address, it does not support the file download and upload
with hosts mapping with IPv4 addresses, `<filename>` is the name of the FTP upload/download file.

Special keywords of the filename

keywords	explain
running-config	Running configuration files
startup-config	It means the reboot configuration files when using copy running-config startup-config command
nos.img	System files
bootrom	System startup files
stacking/nos.img	As destination address, execute system files upgrade for Slave in stacking mode
stacking/nos.rom	As destination address, execute system startup files upgrade for Slave in stacking mode

This command supports command line hints, namely if the user can enter commands in following forms: `copy <filename> ftp://` or `copy ftp:// <filename>` and press Enter, following hints will be provided by the system:

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

`ftp username>`

`ftp password>`

`ftp filename>`

Requesting for FTP server address, user name, password and file name

Example

Save images in the FLASH to the FTP server of 10.1.1.1, FTP server username is Switch, password is superuser:

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

Obtain system file nos.img from the FTP server 10.1.1.1, the username is Switch, password is superuser

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

Save the running configuration files.

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

copy (TFTP)

Command

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

Parameter

<source-url>	the location of the source files or directories to be copied
<destination-url>	the destination address to which the files or directories to be copied
ascii	ASCII standards will be adopted
binary	File transfer will be in binary mode (default transfer method)

Default

None.

Mode

Admin Mode

Usage Guide

This command is used to transfer files by TFTP.

When URL represents a TFTP address, its form should be:

tftp://{<ipaddress>|<ipv6address>|<hostname>}/<filename>, amongst <ipaddress>|

<ipv6address> is the IPv4 or IPv6 address of the TFTP server/client, <hostname> is the name of the host mapping with the IPv6 address, it does not support the file download and upload with hosts mapping with IPv4 addresses, <filename> is the name of the TFTP upload/download file.

Special keyword of the filename

keywords	explain
running-config	Running configuration files
startup-config	It means the reboot configuration files when using copy running-config startup-config command
nos.img	System files
boot.rom	System startup files

This command supports command line hints, namely if the user can enter commands in following forms: copy <filename> tftp:// or copy tftp:// <filename> and press Enter, following hints will be provided by the system:tftp server ip/ipv6 address[x.x.x.x]/[x:x::x:x]>tftp filename>
Requesting for TFTP server address, file name

Example

Save images in the FLASH to the TFTP server of 10.1.1.1

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

Obtain system file nos.img from the TFTP server 10.1.1.1

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

Save the running configuration files

Switch#copy running-config startup-config

ftp-dir

Command

ftp-dir <ftp-server-url>

Parameter

<ftp-server-url>	ftp server address

Default

None.

Mode

Admin Mode

Usage Guide

Browse the file list on the FTP server.

The form of <ftp-server-url> is :

ftp://<username>:<password>@{ <ipv4address> | <ipv6address> }, amongst <username>

is the FTP user name, <password> is the FTP user password, { <ipv4address> | <ipv6address> } is the IPv4 or IPv6 address of the FTP server.

Example

Browse the list of the files on the server with the FTP client, the username is “Switch”, the password is “superuser”.

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

ftp-server enable

Command	ftp-server enable no ftp-server enable
Parameter	none none
Default	FTP server is not started by default.
Mode	Global Mode
Usage Guide	This command is used to start the FTP server. When FTP server function is enabled, the switch can still perform ftp client functions. The “no ftp-server enable” command shuts down FTP server and prevents FTP user from logging in.
Example	Enable FTP server services. Switch(config)# ftp-server enable

ftp-server timeout

Command	ftp-server timeout <seconds>
Parameter	<seconds> the idle time threshold (in seconds) for FTP connection, the valid range is 5 to 3600
Default	The system default is 600 seconds.
Mode	Global Mode
Usage Guide	This command is used to configure FTP data connection idle time. When FTP data connection idle time exceeds this limit, the FTP management connection will be disconnected.
Example	Modify the idle threshold to 100 seconds. Switch(config)#ftp-server timeout 100

ip ftp

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

Parameter	<username>	the username of the FTP link, its range should not exceed 32 characters
	[0 7]	0 means password is not encrypted ,7 means password is encrypted
	<password>	FTP link password

Default The system uses anonymous FTP links by default.

Mode Global Mode

Usage Guide Configure the username and password for logging in to the FTP.

The no operation of this command will delete the configured username and password simultaneously.

Example Configure the username as Switch and the password as superuser.

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

show ftp

Command **show ftp**

Parameter	none	none

Default None.

Mode Admin and Global Mode

Usage Guide Display the parameter settings for the FTP server.

Example Display the parameter settings for the FTP server.

Switch#show ftp

Timeout : 600

show tftp

Command	show tftp

Parameter	none	none

Default	None.

Mode	Admin and Global Mode

Usage Guide	Display the parameter settings for the TFTP server.

Example	Display the parameter settings for the TFTP server.

Switch#show tftp

timeout : 60

Retry Times : 10

tftp-server enable

Command	tftp-server enable no tftp-server enable

Parameter	none	none

Default	Disable TFTP Server.

Mode	Global Mode

Usage Guide	This command is used to start the TFTP server.

The “no tftp-server enable” command shuts down TFTP server and prevents TFTP user from logging in.

Example

Start the TFTP server.

Switch(config)#tftp-server enable

tftp-server retransmission-number

Command

tftp-server retransmission-number <number>

Parameter

<number> the time to re-transfer, the valid range is 1 to 20

Default

Retransmit 5 times.

Mode

Global Mode

Usage Guide

Set the retransmission time for TFTP server.

Example

Modify the retransmission to 10 times.

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

tftp-server transmission-timeout

Command

tftp-server transmission-timeout <seconds>

Parameter

<seconds> the timeout value, the valid range is 5 to 3600s

Default

The system default timeout setting is 600 seconds.

Mode

Global Mode

Usage Guide

Set the transmission timeout value for TFTP server.

Example

Modify the timeout value to 60 seconds.

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

6 Commands for File System

cd

Command	cd <directory>		
Parameter	<table><tr><td><directory></td><td>the sub-directory name, a sequence of consecutive characters whose length ranges from 1 to 80</td></tr></table>	<directory>	the sub-directory name, a sequence of consecutive characters whose length ranges from 1 to 80
<directory>	the sub-directory name, a sequence of consecutive characters whose length ranges from 1 to 80		
Default	The default working directory is Flash.		
Mode	Admin Mode		
Usage Guide	Change the working directory for the storage device. After this command implemented, the current storage device will switch to the new working directory, which can be viewed by the “pwd” command.		
Example	Change the working directory of the current storage device to flash. Switch#cd flash: Switch#pwd flash:/		

copy

Command	copy <source-file-url> <dest-file-url>				
Parameter	<table><tr><td><source-file-url></td><td>The source address of the file or directory to be copied</td></tr><tr><td><dest-file-url></td><td>The destination address of the file or directory to be copied</td></tr></table>	<source-file-url>	The source address of the file or directory to be copied	<dest-file-url>	The destination address of the file or directory to be copied
<source-file-url>	The source address of the file or directory to be copied				
<dest-file-url>	The destination address of the file or directory to be copied				
Default	None.				
Mode	Admin Mode				
Usage Guide	Copy a designated file on the switch and store it as a new file. When users operate on files stored in backup master board and line cards under IMG mode, URLs of the source file and the destination file should take such a form as described in the following requirements. 1. The prefix of the source file URL should be in one of the following forms: starting with				

“flash:”

“ftp://username:pass@server-ip/file-name”

“tftp://server-ip/file-name”

2. The prefix of the destination file URL should be in one of the following forms:

starting with “flash:”

“ftp://username:pass@server-ip/file-name”

“tftp://server-ip/file-name”

when the prefix of the source file URL is ftp:// or tftp://, that of the destination file URL should not be either of them.

To use this command, the designated source file should exist, and the destination file should not be named the same as any existing directory or file, otherwise, there might be a prompt warning about a failed copy operation or an attempt to overwrite an existing file.

If the source and destination files are in different directories, with this command implemented, users can copy files from other directories into the current one.

Example

Copy the file “flash:/nos.img” and store it as “flash/ 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

Copied file flash:/nos.img to flash:/nos-6.1.11.0.img

delete

Command

delete <file-url>

Parameter

<file-url>	the full path of the file to be deleted

Default

None.

Mode

Admin Mode

Usage Guide

Delete the designate file on the storage device.

Example

Delete file flash:/nos.img.

Switch#delete flash:/nos5.img

Delete file flash:/nos5.img?[Y:N]y

Deleted file flash:/nos5.img

dir

Command	dir [WORD]
Parameter	[WORD] the name of the shown directory. There may be the following formats: directory name, slot-xx#directory name, flash:/directory name, cf:/directory name.
Default	No <WORD> means to display information of the current working directory.
Mode	Admin Mode
Usage Guide	Display the information of the designated directory on the storage device. This command does not support a recursive display of all sub-directories.
Example	Display information 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#

pwd

Command	pwd
Parameter	none none
Default	The default directory is flash.
Mode	Admin Mode
Usage Guide	Display the current working directory.
Example	Display the current working directory. Switch#pwd flash:/

rename

Command	rename <source-file-url> <new-filename >	
Parameter	<source-file-url>	the source file, in which whether specifying or not its path are both acceptable
	<new-filename >	filename without specifying its path
Default	None.	
Mode	Admin Mode	
Usage Guide	Rename a designated file on the switch. When using this command, if the new file name is not used as that of any existing directory or file, the rename operation can be done, or a prompt will indicate its failure.	
Example	Change the name of file “nos.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!	

7 Commands for Mqtt Configuration

ip mqtt client

Command	ip mqtt client no ip mqtt client	
Parameter	none	none
Default	By default, the MQTT client connection is not enabled.	
Mode	Global Mode	
Usage Guide	This command can enable the MQTT client connection.	
Example	Once the server IP and port configuration is completed, you can attempt to connect to the cloud	

platform by using this command.

Switch(config)#ip mqtt server 1 192.168.19.64

Switch(config)# ip mqtt client

ip mqtt server auto

Command	ip mqtt server auto no ip mqtt server auto	
Parameter	none	none
Default	By default, the automatic connection of the MQTT server is not enabled.	
Mode	Global Mode	
Usage Guide	Once this command is enabled, a multicast message lookup server can be automatically initiated within the local network. Once the search is successful, the server address and port will be automatically obtained. Then, by simply initiating a client connection, the server can be connected directly.	
Example	When the multicast message finds the server address, it can attempt to connect to the cloud platform by using this command. Switch(config)# ip mqtt server auto (wait for a moment) Switch(config)# ip mqtt client	

ip mqtt server session-timeout

Command	ip mqtt server session-timer <10-300> no ip mqtt server session-timer	
Parameter	timeout	The timeout duration for MQTT server session connection, measured in seconds
Default	The default connection timeout period is 30 seconds.	
Mode	Global Mode	

Usage Guide This command can configure the session connection timeout time for the MQTT server.

Example

```
Switch(config)# ip mqtt server session-timer 100
Switch(config)# no ip mqtt server session-timer
```

ip mqtt server domain

Command **ip mqtt server WORD**
no ip mqtt server domain

Parameter **WORD** MQTT server connection domain name

Default By default, it is the domain name address of the cloud server.

Mode Global Mode

Usage Guide This command can configure the MQTT server domain name. When the external network can be accessed and the ip domain-lookup function for DNS lookup is enabled, MQTT will automatically obtain the corresponding IP address through the server domain name.

Example Configure the domain name of the MQTT server to "acc.test"

```
Switch(config)# ip mqtt server acc.test
Switch(config)# no ip mqtt server domain
```

ip mqtt server

Command **ip mqtt server <1-8> A.B.C.D (protocol-port <1-65535>)**
no ip mqtt server <1-8>

Parameter	Server-id	Server session ID
	A.B.C.D	Server IP address
	Protocol-port	Server port

Default The default value of protocol-port is 1883.

Mode Global Mode

Usage Guide	This command can configure the address for connecting to the MQTT server.
Example	Once the server IP and port configuration is completed, you can attempt to connect to the cloud platform by using this command. <pre>Switch(config)# ip mqtt server 1 192.168.2.1 protocol-port 1883 Switch(config)# ip mqtt client</pre>

debug mqtt

Command	debug mqtt (info err packet all) no debug mqtt (info err packet all)
Parameter	info err packet all Enable MQTT logging mode
Default	The default is not enabled.
Mode	Admin Mode
Usage Guide	By activating different modes, the serial port will print different logs.
Example	Enable MQTT information logs <pre>Switch(Switch)# debug mqtt info Switch(Switch)# no debug mqtt info</pre>

show ip mqtt

Command	show ip mqtt
Parameter	none none
Default	none
Mode	Admin and configuration mode
Usage Guide	Display all the information of MQTT, such as the configured server address, whether the automatic discovery server is enabled, the connection status of the server, the online server address and port, and the server domain name, etc.
Example	Display the MQTT connection information

Switch(Switch)# show ip mqt

8 Commands for Netconf

debug netconf

Command	debug netconf no debug netconf
Parameter	none none
Default	Default setting is not enabled.
Mode	Admin Mode
Usage Guide	Used to activate the netconf debug function.
Example	Switch#debug netconf NETCONF debugging is on

debug netconf notification

Command	debug netconf notification (arp [ac <1 2> error <1 2 3> port <1 2> <down up>] cfm [alarm detected] config [allocate-error <1 2 3 4> am-check [error success] malloc-error write-config- error write-config-failed] configuration <1 2 3> fan [bad good inserted number removed] fdb [mac-flapping mac-removed port-down port-up] http-login [fail rejected success] interface {[ethernet <IFNAME> port-channel <IFNAME> vlan <vlan-id>] <message- type> [cleared raised] <WORD> } ip [cftnotify] lasp {1mad [switchover] 2mad [switchover] arrach conflict detach run} macOvertemp {[level status] [power-off stop-switch]} mstp {1 [discarding error forwarding learning] 2 }

ospf {neighbor [down | up]} |
 power [bad | good | macchip | macdevice | psu1 | psu2] |
 session-login [logout | rejected] |
 sfp [crx1 | ctemp | ctx1 | ctx1p | cvol | rx1 | temp | tx1 | tx1p | vol] |
 ssh-login [fail | success] |
 system {boot [other | start | up] | rebooted [days] | reload|restart [cold|warm] |skb-free} |
 telnet-login [logout | rejected | success] |
 temperature [below | lowtemp | over | status] |
 udl {notify [down | manually | open]} |
 ulpp {down-forwarding | forwarding-down | master [down | standby] | slave} |
 ulsm [open | shutdown])
 no debug netconf

Parameter	<IFNAME>	Interface name
	<vlan-id>	Vlan port number<1-4094>
	<message- type>	Notification message type
	<WORD>	Extra argument
Default	Default setting is not enabled.	
Mode	Admin Mode	
Usage Guide	Used to activate the netconf alarm debugging function.	
Example	Switch# debug netconf notification arp ac 1	

netconf enable

Command	netconf enable no netconf enable	
Parameter	none	none
Default	Default setting is not enabled.	
Mode	Global Mode	
Usage Guide	Enable or disable the netconf function. Notes: The netconf function can only be used when enabled together with ssh-server enable.	
Example	Enable the netconf function. Switch(Switch)# netconf enable	

show netconf yang

Command	show netconf yang	
Parameter	none	none
Default	None.	
Mode	Admin and Global Mode	
Usage Guide	Display the list information of the netconf yang files.	
Example	Switch#show netconf yang netconf yang file list: configuration-management.yang fan-management.yang arp-port-ntfs.yang interfaces-management.yang device-management.yang	

show netconf-database yang WORD

Command	show netconf-database yang WORD	
Parameter	WORD	Module name
Default	None.	
Mode	Admin and Global Mode	
Usage Guide		
Example	Switch#show netconf-database yang fan-management Module: fan-management Node: fans Switch#	

9 Commands for Packet Capture

packet-capture setup buffer-size

Command	packet-capture setup buffer-size <1-16>
Parameter	<1-16> Enable the message capture function and capture the file size. Unit (M)
Default	Default configuration: 16M.
Mode	Global Mode
Usage Guide	This command can be used to set the maximum size of the message capture file.
Example	Set the value of the packet capture file to 10M. Switch(config)# packet-capture setup buffer-size 10

packet-capture setup packet-num

Command	packet-capture setup packet-num <1-100000>
Parameter	<1-100000> Set the message setting to enable message capture function, and set the maximum number of captured messages. Unit: (pieces)
Default	Default configuration: 100,000 units .
Mode	Global Mode
Usage Guide	This command can enable the message capture function and set the number of captured messages.
Example	Enable message capture and set the number of captured messages to 10. Switch(config)# packet-capture setup packet-num 10

packet-capture setup timeout

Command	packet-capture setup timeout <1-60>	
Parameter	<1-60>	Enable the message capture function and set the capture time. Unit: (minutes)
Default	Default configuration: 60 minutes.	
Mode	Global Mode	
Usage Guide	This command can set the capture duration for the message capture function.	
Example	Set the message capture time to 10 minutes. Switch(config)# packet-capture setup timeout 10	

packet-capture setup file

Command	packet-capture setup file flash usb WORD	
Parameter	flash	Save the file to the flash.
	usb	Save the file to the USB drive.
	WORD	Filename
Default	Default configuration, file name is pcapng.pcapng.	
Mode	Global Mode	
Usage Guide	This command can enable the message capture function, specify the location and name of the message file. When setting the file name, you only need to enter the file name; the path and file format cannot be set.	
Example	Set the captured file to be saved in the flash with the name "arp". Switch(config)# packet-capture setup file flash arp	

no packet-capture setup

Command	no packet-capture setup file buffer-size packet-num timeout	
Parameter	file	File storage location
	Buffer-size	file size
	packet-num	Number of messages
	timeout	capture time
Default	-	
Mode	Global Mode	
Usage Guide	This command is used to remove the basic settings for packet capture functionality and restore the default values.	
Example	Remove the setting for the capture time. Restore the default value of 60 minutes.	
	Switch(config)# no packet-capture setup timeout	

packet-capture acl rule

Command	packet-capture rule WORD acl num no packet-capture rule WORD (acl num)	
Parameter	WORD	Rule Name
	num	Acl Number
Default	Default configuration not set up.	
Mode	Global Mode	
Usage Guide	This command is used to configure the rule for the hardware forwarding packet capture function. The rule is bound to the already configured access list. Multiple access lists can be bound. Conflicting access lists will follow the rules of the conflicting list for processing.	

	The No command supports deleting a specific matching access list in the rule, or deleting the entire rule. Deletion is only possible if the rule is not bound to any point.
Example	Configure a rule named "ip", with the rule definition as "access-list 1" Switch(config)# packet-capture rule ip acl 1

packet-capture cpu rule

Command	packet-capture rule WORD cpu word/all no packet-capture rule WORD						
Parameter	<table> <tr> <td>WORD</td><td>Rule Name</td></tr> <tr> <td>word</td><td>Message type</td></tr> <tr> <td>all</td><td>All message types</td></tr> </table>	WORD	Rule Name	word	Message type	all	All message types
WORD	Rule Name						
word	Message type						
all	All message types						
Default	Default configuration not set up.						
Mode	Global Mode						
Usage Guide	This command is used to configure the rule for capturing packets sent to the CPU. Bind the rule to the packet type. Only one packet type or all packet types can be set. The No command deletes the rule. It can only be deleted if it is not bound to any point.						
Example	Configure a rule named "ip" to match ARP packets. Switch(config)# packet-capture rule ip cpu arp						

packet-capture point

Command	packet-capture point WORD rule-list word in out no packet-capture point WORD
Parameter	WORD The name of Point

	word The name of Rule
	in/out Set the direction of captured packets
Default	Default configuration not set up.
Mode	Port Mode
Usage Guide	This command is used to configure the capture points, bind the capture rules, and set the direction of captured packets. The "No" command is used to delete the capture points. It can only be executed when the capture process is stopped.
Example	Configure a point named "p1" at port 1/0/1, bind the packet capture rule "r1", and set the capture direction to inbound direction. Switch(config-if-ethernet1/0/1)# packet-capture point p1 rule-list r1 in

packet-capture start

Command	packet-capture start point WORD
Parameter	WORD The name of Point
Default	By default, packet capture is not enabled.
Mode	Global Mode
Usage Guide	This command is used to start packet capture at the specified capture point. To enable packet capture, a capture point that is bound to a rule needs to be set up.
Example	Capture point p1 starts capturing packets. Switch(config)# packet-capture start point p1

packet-capture stop

Command	packet-capture stop
Parameter	-
Default	-
Mode	Global Mode
Usage Guide	This command is used to stop message capture.
Example	Stop message capture. Switch(config)# packet-capture stop

10 Commands for DNSv4/v6

clear dynamic-host

Command	clear dynamic-host {<ip-address>[<ipv6-address>]all}
Parameter	<ip-address> ip address <ipv6-address> Ipv6 address all Delete all domain name address mappings
Default	No default configuration.
Mode	Admin Mode
Usage Guide	This command is used to manually delete domain name entries in the dynamic cache. It is particularly useful when domain names have been cached for too long.
Example	Delete the domain name entry with the address 202.108.22.5. Switch#clear dynamic-host 202.108.22.5

debug dns

Command	debug dns {all packet [send recv] events relay} no debug dns {all packet [send recv] events relay}	
Parameter	all	All information
	Packet [send recv]	Dns send/receive packets
	events	Dns events
	relay	Dns relay
Default	-	
Mode	Admin Mode	
Usage Guide	Displays application debugging information when performing DNS domain name resolution.	
Example		
	Switch# debug dns all	

dns-server

Command	dns-server {<ip-address> <ipv6-address> vrf <vrf-name> [priority <value>]} no dns-server {<ip-address> <ipv6-address> vrf <vrf-name> [priority <value>]}	
Parameter	<ip-address>	ip address
	<ipv6-address>	Ipv6 address
	<value>	The value for the priority of the DNS server
	<vrf-name>	Virtual Routing and Forwarding instance name
Default	No default configuration.	
Mode	Config Mode	
Usage Guide	This command is used to configure or delete a DNS server. When dynamic domain name resolution is required, the switch sends domain name query requests to the configured DNS servers. Up to 6 DNS servers can be	

configured. The priority is an optional parameter. If the priority is configured, the DNS servers are organized in descending order of priority, and the switch first sends domain name query requests to the server with the highest priority. Therefore, you can configure a higher priority for DNS servers with faster query speeds and frequent use to facilitate queries. If the priority is not configured, the DNS servers are queried in the order of their configuration. When the switch acts as a DNS SERVER, it does not follow the above priority principle for DNS SERVER queries, but sends requests uniformly to all configured servers.

Example

Configure a DNS server 10.1.120.241 with a priority of 200.

Switch(config)#dns-server 10.1.120.241 priority 200

dns lookup

Command

dns lookup {ipv4|ipv6|vrf [ipv4|ipv6]} <hostname>

Parameter

ipv4	ip address
ipv6	Ipv6 address
hostname	The dynamic host name to be parsed can have a maximum length of 63 characters.

Default

No default configuration.

Mode

Config Mode

Usage Guide

This command queries the corresponding address based on the entered host name, supporting both IPv4 and IPv6 address queries. The resolved domain name and its corresponding address are stored in the dynamic cache. This command is solely for domain name resolution and has no other application functions. It cannot be interrupted during execution. If multiple servers and domain suffixes are configured, domain name resolution may take a long time.

Example

Query the IPv4 address of www.sina.com.

Switch(config)#dns lookup ipv4 www.sina.com

ip domain-lookup

Command	ip domain-lookup no ip domain-lookup
Parameter	None
Default	Not configured by default
Mode	Config Mode
Usage Guide	This command is used to enable or disable the dynamic DNS query function of the switch. After enabling the dynamic DNS query function, when application tools (such as ping) or the switch acts as a DNS SERVER and encounters domain name processing, it will send a domain name resolution request to the configured DNS server to obtain the corresponding IPv4/IPv6 address of the domain name. After disabling this function, when encountering domain name processing, it will no longer send domain name resolution requests, but only search in the statically configured domain names, that is, dynamic domain name resolution will no longer be performed. If there are previously resolved domain names in the dynamic domain name cache at this time, they will neither be searched nor deleted, and will be automatically deleted after the time expires.
Example	Enable the DNS function to dynamically resolve domain names. Switch(config)#ip domain-lookup

ip domain-list

Command	ip domain-list <WORD> no ip domain-list <WORD>
Parameter	WORD Domain name suffix strings can have a maximum of 63 characters.
Default	-
Mode	Config Mode
Usage Guide	This command is used to configure/delete domain name suffixes.

When an incomplete domain name (such as "sina") is entered, the switch automatically adds the domain name suffix before performing domain name resolution. A maximum of 6 domain name suffixes can be configured, and the first configured suffix will be added first.

Example

Configure the domain name suffix "com".

Switch(config)#ip domain-list com

ip dns server

Command

ip dns server
no ip dns server

Parameter

-

Default

Not configured by default.

Mode

Config Mode

Usage Guide

After enabling the DNS SERVER function, the switch can receive and process DNS requests from clients, either by looking up results locally or forwarding requests to a real DNS server.

Example

Configure the switch to enable the DNS server function.

Switch(config)#ip dns server

ip dns server queue maximum

Command

ip dns server queue maximum <1-5000>
no ip dns server queue maximum

Parameter

<1-5000> The configurable range is 1 to 5000

Default

By default, the switch allows caching information for 3000 users.

Mode

Config Mode

Usage Guide	After receiving a DNS request from a client, the switch caches the client's information. However, the number of cached client information entries cannot exceed the configured maximum value. If this limit is exceeded, the client's request will not be processed.

Example	Configure the maximum number of client information entries cached by the switch to 2000.

Switch(config)#ip dns server queue maximum 2000

ip dns server queue timeout

Command	ip dns server queue timeout <1-100> no ip dns server queue timeout

Parameter	<1-100> The configurable timeout range is 1 to 100 seconds.

Default	By default, the timeout period is 5 seconds.

Mode	Config Mode

Usage Guide	After receiving a DNS request from a client, the switch caches the client's information. However, the cached client information cannot be retained for longer than the configured maximum timeout period. After the timeout, the client's information will be cleared.

Example	Configure the maximum timeout period for caching client information on the switch to 10 seconds.

Switch(config)#ip dns server queue timeout 10

show dns name-server

Command	show dns name-server

Parameter	None

Default	-
Mode	All Mode
Usage Guide	-
Example	Displays the configured DNS server information. <pre> Switch#show dns name-server DNS NAME SERVER: Address Priority 10.1.120.231 100 10.1.180.85 80 2001::1 20 </pre>

show dns domain-list

Command	show dns domain-list
Parameter	None
Default	-
Mode	All Mode
Usage Guide	-
Example	Displays the configured DNS domain suffix information. <pre> Switch#show dns domain-list DNS DOMAIN LIST: com.cn edu.cn </pre>

show dns hosts

Command	show dns hosts

Parameter	None
Default	-
Mode	All Mode
Usage Guide	-
Example	Displays the dynamically resolved domain name information in the switch. <pre>Switch# show dns hosts Total number of dynamic host is 2 DNS HOST LIST: Hostname Address Time to live Type www.sina.com.cn 202.108.33.32 168000 dynamic www.ipv6.org 2001:6b0:1 168060 dynamic</pre>

show dns config

Command	show dns config
Parameter	None
Default	-
Mode	All Mode
Usage Guide	-
Example	Displays the globally configured DNS information in the switch. <pre>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</pre>

show dns client

Command	show dns client						
Parameter	None						
Default	-						
Mode	All Mode						
Usage Guide	-						
Example	Displays the DNS Client information maintained by the switch. Switch(config)#show dns client DNS REQUEST LIST: Total number of dns request is 2 <table><thead><tr><th>Address</th><th>Request Id</th></tr></thead><tbody><tr><td>192.168.11.141</td><td>1</td></tr><tr><td>192.168.11.138</td><td>2</td></tr></tbody></table>	Address	Request Id	192.168.11.141	1	192.168.11.138	2
Address	Request Id						
192.168.11.141	1						
192.168.11.138	2						

11 Commands for MDNS

mdns gateway enable

Command	mdns gateway enable no mdns gateway enable
Parameter	None
Default	By default, the mDNS gateway function is turned off.
Mode	Config Mode
Usage Guide	Enable the mDNS gateway function.
Example	Switch-(config)#mdns gateway enable

mdns gateway policy WORD

Command	mdns gateway policy WORD no mdns gateway policy WORD
Parameter	WORD Gateway policy name
Default	By default, no MDNS gateway policies have been configured.
Mode	Config Mode
Usage Guide	To create an MDNS gateway policy, the gateway must be enabled before configuration can be made. The policy should be configured to restrict the access of user devices to the service scope. Without configuring the policy, user devices will be unable to query any services.
Example	Switch(config)#mdns gateway enable Switch(config)#mdns gateway policy PC

mdns gateway probe interval <60-38400>

Command	mdns gateway probe interval <60-38400> no mdns gateway probe interval
Parameter	<60-38400> Fixed detection interval time
Default	Default: No configuration is made.
Mode	Vlan Mode
Usage Guide	The mDNS service enables devices to actively announce their services when they connect to the network. After an mDNS gateway device connects to the network, it will receive the service information announced by subsequent mDNS service-providing devices that connect to the network. However, for service-providing devices that already exist in the network, the service-providing devices will no longer actively announce their services, and thus the mDNS gateway cannot obtain the service information. After enabling the service timing detection function on the mDNS gateway, the mDNS gateway will periodically actively detect the service-providing devices in the network. Based on the received response messages, it will promptly update the service information list on the gateway.
Example	Switch(config)#vlan 2

```
Switch(config-vlan2)#mdns gateway probe interval 60
```

mdns gateway source ip A.B.C.D

Command	mdns gateway source ip A.B.C.D no mdns gateway source ip	
Parameter	A.B.C.D	The destination gateway uses a decimal format for the IP address.
Default	By default, no configuration is required. Use the primary IP address of the VLAN outbound interface as the source IP address for sending mDNS packets from the gateway.	
Mode	Vlan Mode	
Usage Guide	When the mDNS gateway sends mDNS probe packets or forwards/replies mDNS request packets within a certain VLAN/VSI, it needs to use the primary IP address of the VLAN interface/VSI interface as the source IP address of the mDNS probe packet, forwarding request packet or response packet. If no IP address is configured on the VLAN interface/VSI interface, the mDNS gateway cannot send mDNS probe packets. If a large number of VLAN/VSI interfaces are connected to the mDNS gateway device, and an IP address is configured for each VLAN interface/VSI interface, it will waste a lot of IP address resources. After executing this command to configure the source address of mDNS packets forwarded by the mDNS gateway, when the mDNS gateway sends mDNS probe packets or forwards/replies mDNS request packets within a certain VLAN/VSI, it will modify the source address of the mDNS packet to this address, and then send the probe packets or forward/reply mDNS request packets within the VLAN/VSI.	
Example	<pre>Switch(config)#vlan 20</pre> <pre>Switch(config-vlan20)#mdns gateway source ip 42.1.1.1</pre>	

mdns relay gateway ip

Command	mdns relay gateway ip A.B.C.D no mdns relay gateway ip

Parameter	A.B.C.D	The destination gateway uses a decimal format for the IP address.
Default	By default, no configuration is set.	
Mode	Config Mode	
Usage Guide	Only after specifying the mDNS gateway address on the mDNS relay, when the mDNS relay receives the mDNS request message sent by the mDNS user terminal device, it will modify the destination multicast address of the message to the address of the specified mDNS gateway, and then forward the mDNS request message unicast to the mDNS gateway. When the mDNS relay receives the unicast response message from the mDNS gateway, it will convert the unicast message into a multicast message and send it within the VLAN where the mDNS user terminal device is located, ensuring that the mDNS user terminal device that sent the request can receive the response message. After other mDNS user terminal devices receive the message, they can also learn the service information in the response message or refresh their own saved service information. Execute this command multiple times, and the last executed command takes effect.	
Example	Switch-(config)#mdns relay gateway ip 42.1.1.1	

mdns relay enable

Command	mdns relay enable no mdns relay enable
Parameter	None
Default	By default, no configuration is set.
Mode	Vlan Mode
Usage Guide	In enterprise networking, different devices need to be assigned to different network segments. To enable user terminal devices within a certain network segment to use mDNS application services from other network segments, support for mDNS communication across network segments is required. To solve this problem, the mDNS relay function needs to be configured on multiple network segments of the devices. The mDNS relay can learn the mDNS service information within different network segments and multicast it to the mDNS gateway for registration. When mDNS user terminal devices need to use mDNS applications, they multicast a request to the mDNS relay, which converts it into a unicast

message and forwards it to the mDNS gateway for processing. The mDNS relay function can only take effect after the address of the mDNS gateway is specified on the mDNS relay.

Example

```
Switch(config)#vlan 20
Switch(config-vlan20)#mdns relay enable
```

mdns relay probe interval

Command

mdns relay probe interval <60-38400>
no mdns relay probe interval

Parameter

<60-38400> The time interval for periodic detection ranges from 60 to 38,400 seconds.

Default

By default, no configuration is set.

Mode

Vlan Mode

Usage Guide

After enabling the timed probing function of the mDNS relay on the mDNS relay, the mDNS relay will send mDNS request packets to the VLAN where the mDNS relay function is enabled at the configured probing time intervals. After receiving the request packets, the mDNS service providing device will send mDNS response packets to the mDNS relay. After receiving the response packets, the mDNS relay will multicast the response packets to the mDNS gateway to ensure that the mDNS gateway can promptly learn the latest information of all mDNS service providing devices in the network. Repeat this command multiple times, and the last configured command will take effect.

Example

The switch configures the EXP priority 2 to be mapped to the EXP priority 6.

```
Switch(config)#vlan 20
Switch(config-vlan20)# mdns relay probe interval 66
```

mdns relay source ip

Command

mdns relay source ip A.B.C.D
no mdns relay source ip

Parameter

A.B.C.D The destination gateway uses a decimal format for the IP address.

Default	By default, no configuration is applied. When MDNS sends packets to a certain VLAN, it defaults to using the address of the outgoing interface.
Mode	Vlan Mode
Usage Guide	If the mDNS relay sends mDNS probe packets or forwards mDNS response packets within a certain VLAN, it will use the IP address of the VLAN interface as the source address of the mDNS probe packets. If no IP address is configured on the VLAN interface, the mDNS relay cannot send mDNS probe packets. If a large number of VLANs are connected to the mDNS relay device, configuring an IP address for each VLAN would significantly waste IP address resources. After configuring the source address for mDNS relay to forward mDNS packets through this command, when the mDNS relay enables the mDNS timed probing function within a certain VLAN, it will modify the source address of the mDNS probe packets to this address and then send the probe packets within the VLAN. After the mDNS relay receives the mDNS multicast packet, it will modify the source address of the packet to the specified IP address and then forward it to the mDNS gateway. The specified ip-address must be the IP address on the mDNS relay, and this address must be reachable via the routing to the mDNS gateway. Otherwise, the mDNS relay cannot receive the response packets. It is recommended to specify the source IP address as the IP address of the mDNS relay's interface connecting to the mDNS gateway.
Example	<pre>Switch(config)#vlan 20 Switch(config-vlan20)#mdns relay source ip 42.1.1.1</pre>

policy enable

Command	policy enable policy disable
Parameter	None
Default	By default, the strategy is enabled.
Mode	Policy Mode
Usage Guide	The strategy is enabled by default. This command is used to restore the default configuration. "Enable" re-enables the strategy, while "disable" makes the strategy ineffective.
Example	<pre>Switch(onfig-policy)# policy disable</pre>

```
Switch(onfig-policy)# policy enable
```

service vlan *vlan-id*

Command	service vlan <i>vlan-id</i> no service vlan <i>vlan-id</i>
Parameter	<i>vlan-id</i> Service VLAN ID. The usable range is <1 - 4094>.
Default	By default, when the policy is empty, there are no service VLANs.
Mode	Policy Mode
Usage Guide	Adding server VLANs to the policy, you can use “-” to configure consecutive VLANs, and use “,” to configure non-consecutive VLANs..
Example	Switch(config-policy)#service vlan 2

show mdns gateway policy table

Command	show mdns gateway policy table
Parameter	None
Default	By default, no configuration is set.
Mode	All Mode
Usage Guide	Display mDNS gateway policy configuration.
Example	Switch(config)#show mdns gateway policy table Policy: cc [ENABLED] User VLANs: 2 Service VLANs: 4

show mdns gateway cache

Command	show mdns gateway cache
Parameter	None
Default	By default, no configuration is set.
Mode	All Mode
Usage Guide	Display the mDNS gateway cache information.
Example	<pre>Switch(config)#show mdns gateway cache Max entries: 256, Current: 8 ----- [VALID] VLAN=9, TTL=4500, TXT: M4250-10G2XF- PoE+.169.254.100.100._telnet._tcp.local (len=0): "" [VALID] VLAN=9, TTL=120, SRV: M4250-10G2XF- PoE+.169.254.100.100._http._tcp.local -> unipoe.local:49151 (prio=0, weight=0) [VALID] VLAN=9, TTL=4500, PTR: _http._tcp.local -> M4250- 10G2XF-PoE+.169.254.100.100._http._tcp.local [VALID] VLAN=9, TTL=120, SRV: M4250-10G2XF- PoE+.169.254.100.100._telnet._tcp.local -> unipoe.local:23 (prio=0, w eight=0) [VALID] VLAN=9, TTL=4500, TXT: M4250-10G2XF- PoE+.169.254.100.100._http._tcp.local (len=6): "path=/" [VALID] VLAN=9, TTL=120, PTR: 100.100.254.169.in- addr.arpa -> unipoe.local [VALID] VLAN=9, TTL=120, A: unipoe.local -> 169.254.100.100 [VALID] VLAN=9, TTL=4500, PTR: _telnet._tcp.local -> M4250- 10G2XF-PoE+.169.254.100.100._telnet._tcp.local ----- Total records traversed: 8 (expired: 0)</pre>

show mdns relay

Command	show mdns relay
Parameter	None
Default	By default, no configuration is set.

Mode	All Mode			
Usage Guide	Display the configuration of mDNS relay.			
Example				
	Switch(config-if-vlan10)#sho mdns relay			
	mDNS relay configuration:			
	mDNS gateway IP: 42.1.1.1:5353			
	ifindex	VLAN ID	Source IP address	Probe interval (sec)
11010	10	10.1.1.1:0(Auto)	88	
11020	20	42.1.1.1:0	0	

show mdns relay statistics

Command	show mdns relay statistics
Parameter	None
Default	By default, no configuration is set.
Mode	All Mode
Usage Guide	Display the packet transmission and reception situation of mDNS.
Example	Switch(config)#show mdns relay statistics Packet statistics: Received:3 Sent:3 Dropped:0 Probe sent:4

user vlan *vlan-id*

Command	user vlan <i>vlan-id</i> no user vlan <i>vlan-id</i>
Parameter	<i>vlan-id</i> User VLAN ID, available range: <1 - 4094>
Default	By default, when the policy is empty, there are no user VLANs.
Mode	Policy Mode
Usage Guide	To add user-end VLANs to the policy, you can use “-” to configure

consecutive VLANs, and use “,” to configure non-consecutive VLANs.

Example

```
Switch(config-policy)#user vlan 2
```

02- Port Module Command Line Manual

1 Commands for Ethernet Port Configuration

bandwidth

Command	bandwidth control < <i>bandwidth</i> > { transmit receive both } no bandwidth control	
parameter	<i>bandwidth</i>	is the bandwidth limit, which is shown in kbps ranging between 1000-1000000000K
default	Disable bandwidth restrictions by default	
Mode	Port Configuration Mode	
Usage Guide	Use the bandwidth control < bandwidth >[both receive transmit] command to set the bandwidth rate. Use the no bandwidth control restore default configuration	
Example	Set the bandwidth limit of 1/0/1-8 port is 40000K. Switch(config)#interface ethernet 1/0/1-8 Switch(Config-If-Port-Range)#bandwidth control 40000 both	

clear counters interface

Command	clear counters [interface { IFNAME ethernet < <i>interface-list</i> > vlan < <i>vlan-id</i> > port-channel < <i>port-channel-number</i> > < <i>interface-name</i> > tunnel < <i>interface-name</i> >}]	
parameter	<i>interface-list</i>	stands for the Ethernet port number;
	<i>vlan-id</i>	stands for the VLAN interface number;
	<i>port-channel-number</i>	for trunk interface number;
	<i>interface-name</i>	for interface name, such as port-channel 1.

default	Port statistics default not cleared
Mode	Admin Mode
Usage Guide	If no port is specified, statistics for all ports are cleared.
Example	Clearing the statistics for Ethernet port1/0/1. Switch#clear counters interface ethernet 1/0/1

description

Command	description < <i>string</i> > no description		
parameter	<table><tr><td><i>string</i></td><td>is a character string, which should not exceeds 200 characters</td></tr></table>	<i>string</i>	is a character string, which should not exceeds 200 characters
<i>string</i>	is a character string, which should not exceeds 200 characters		
default	No port name by default		
Mode	Port Mode		
Usage Guide	This command is for helping the user manage switches, such as the user assign names according to the port application, e.g. financial as the name of 1/0/1-2 ports which is used by financial department, engineering as the name of 1/0/9 ports which belongs to the engineering department, while the name of 1/0/12 ports is assigned with Server, which is because they connected to the server. In this way the port distribution state will be brought to the table.		
Example	Specify the description of 1/0/1-2 port as financial. Switch(config)#interface ethernet 1/0/1-2 Switch(Config-If-Port-Range)#description financial		

fec

Command	fec mode (none base-r rs-fec) no fec mode				
parameter	<table><tr><td>none</td><td>Turn off the FEC mode</td></tr><tr><td>base-r</td><td>Set to the basic FEC mode (10G/25G/40G)</td></tr></table>	none	Turn off the FEC mode	base-r	Set to the basic FEC mode (10G/25G/40G)
none	Turn off the FEC mode				
base-r	Set to the basic FEC mode (10G/25G/40G)				

rs-fec	Set to rs-fec mode (25G/100G)

default	By default, different modes are enabled based on the port type. <table> <tr> <td>1G</td><td>Disabled</td></tr> <tr> <td>10G</td><td>Disabled</td></tr> <tr> <td>25G</td><td>RS-FEC</td></tr> <tr> <td>40G</td><td>Base-R FEC(Fire Code FEC)</td></tr> <tr> <td>100G</td><td>RS-FEC</td></tr> </table>	1G	Disabled	10G	Disabled	25G	RS-FEC	40G	Base-R FEC(Fire Code FEC)	100G	RS-FEC
1G	Disabled										
10G	Disabled										
25G	RS-FEC										
40G	Base-R FEC(Fire Code FEC)										
100G	RS-FEC										
Mode	Port Mode										
Usage Guide	This command is used to configure the forward error correction (FEC) mode for the port. FEC achieves automatic correction of transmission errors through redundant data, thereby enhancing the reliability of the link: - none: No error correction capability, suitable for scenarios with excellent link quality - base-r: Compatible with 10G/25G/40G rate links, following the Base-R FEC specification of IEEE 802.3 - rs-fec: Stronger error correction capability, usually used in high-speed rate, long-distance transmission scenarios such as 25G/100G etc.										
Example	Enable the base-r mode FEC on the 1/0/1-8 ports. <pre>Switch#config Switch(config)# interface ethernet 1/0/1-8 Switch(config-if-port-range)#fec mode base-r</pre>										

flow control

Command	flow control no flow control
parameter	-
default	Disable port traffic control by default
Mode	Port Mode
Usage Guide	After the flow control function is enabled, the port will notify the sending device to slow down the sending speed to prevent packet loss when traffic received exceeds the capacity of port cache. Ports support IEEE802.3X flow control; the ports work in half-duplex mode, supporting back-pressure flow control. If flow control results in serious HOL, the switch will automatically start HOL control (discarding some packets in

the COS queue that may result in HOL) to prevent drastic degradation of network performance.

Example	Enabling the flow control function in ports 1/0/1-8. Switch(config)#interface ethernet 1/0/1-8 Switch(Config-If-Port-Range)#flow control

interface ethernet

Command	interface ethernet <interface-list>
parameter	<i>interface-list</i> stands for port number.
default	-
Mode	Global Mode
Usage Guide	This command can be used to enter port configuration mode and run exit command to exit Ethernet port mode to global mode.
Example	Entering the Ethernet Port Mode for ports 1/0/1, 1/0/4-5, 1/0/8。 Switch(config)#interface ethernet 1/0/1;1/0/4-5;1/0/8 Switch(Config-If-Port-Range)#

Loopback

Command	loopback no loopback
parameter	-
default	By default, disable loop testing in the Ethernet port
Mode	Port Mode
Usage Guide	Loopback test can be used to verify the Ethernet ports are working

normally. After loopback has been enabled, the port will assume a connection established to itself, and all traffic sent from the port will be received at the very same port.

Example

Enabling loopback test in Ethernet ports 1/0/1-8.
Switch(config)#interface ethernet 1/0/1-8
Switch(Config-If-Port-Range)#loopback

Negotiation

Command

Negotiation {on | off}

parameter

-

default

By default, automatic negotiation is enabled.

Mode

Port Mode

Usage Guide

This command can be used to configure the port speed and set the working mode to auto-negotiation. This command is only applicable to 1000Base-FX interfaces. For 1000Base-TX or 100Base-TX interfaces, the negotiation command is not available. To change the negotiation mode, speed and duplex mode of a 1000Base-TX port, please use the speed-duplex command.

Example

Port 21 of Switch 1 is connected to Port 21 of Switch 2. Below, the negotiation between these two ports will be disabled.
Switch1(config)#interface ethernet1/0/21
Switch1(Config-If-Ethernet1/0/21)#negotiation off
Switch2(config)#interface ethernet1/0/21
Switch2(Config-If-Ethernet1/0/21)#negotiation off

Port-rate-statistics interval

Command

port-rate-statistics interval <interval-value>

parameter

interval-value

The interval of port-rate-statistics, unit is second, ranging from 5 to 600 with the configuration step of 5.

default

Only port-rate-statistics of 5 seconds and 5 minutes are displayed.

Mode Global Mode

Usage Guide This command can be used to set the port rate statistics interval time.

Example Count the interval of port-rate-statistics as 20 seconds.
Switch(config)#port-rate-statistics interval 20

rate-violation

Command **rate-violation [broadcast | multicast | unicast | all] <200-2000000>**
no rate-violation

parameter	broadcast	broadcast packet
	multicast	multicast packet
	unicast	unicast packet
	all	all packets
	<200-2000000>	the number of packets allowed to pass per second.

default There is no limit for the packet reception rate.

Mode Port Mode

Usage Guide This command is mainly used to detect the abnormal port flow. For example, when there are a large number of broadcast packets caused by a loopback, which affect the processing of other tasks, the port will be shut down or block to ensure the normal processing of the switch. This command needs to associate with rate-violation control command.

Example Set the rate-violation of port 1/0/8-10 (GB ports) as 10000pps, it will be shutdown after rate-violation and the port recovery time as 1200 seconds, when the packet reception rate exceeds 10000, the port will but shut down, and then, after 1200 seconds, the port will be UP again.

```
Switch(config)#interface ethernet 1/0/8-10
Switch(Config-Port-Range)#rate-violation unicast 10000
Switch(Config-Port-Range)#rate-violation control shutdown recovery 1200
```

rate-violation control

Command	rate-violation control [shutdown recovery <0-86400> block] no rate-violation control	
parameter	shutdown	A port is shutdown after rate-violation
	recovery	After a period of time the port can recover Shutdown to UP again.
	block	A port is block after rate-violation, this parameter and MSTP, EAPS(MRPP), Loopback Detection, ULPP are mutually exclusive. If other modules set STP state, this function can not be set to block mode.
	<0-86400>	Automatic recovery time
default	There is no control operation for rate-violation.	
Mode	Port Mode	
Usage Guide	This command is mainly used to the control operation after rate-violation.	
Example	After set the rate-violation of the unicast packet of port 1/8-10 (GB ports) as 10000pps, the port will be block. Switch(Config)#interface ethernet 1/0/8-10 Switch(Config-Port-Range)#rate-violation unicast 10000 Switch(Config-Port-Range)#rate-violation control block	

show interface

Command	show interface [ethernet <interface-number> port-channel <port-channel-number> vlan <vlan-id> <interface-name>] [detail] show interface ethernet status show interface ethernet counter {packet rate}	
parameter	<i>interface-number</i>	is the port number of the Ethernet,
	<i>port-channel-number</i>	is the number of the aggregation interface
	<i>vlan-id</i>	is the VLAN interface number, the value range from 1 to 4094
	<i>interface-name</i>	is the name of the interface such as port-channel1
	detail	show the detail of the port

default	Information not displayed by default
Mode	Admin and Configuration Mode.
Usage Guide	Use this command to view interface-related configuration information
Example	Show the information of VLAN 1 . <pre> Vlan1 is up, line protocol is up, dev index is 11001 Device flag 0x1003(UP BROADCAST MULTICAST) Time since last status change:0w-0d-1h-14m-57s (4497 seconds) IPv4 address is: 192.168.2.1 255.255.255.0 (Primary) VRF Bind: Not Bind Hardware is EtherSVI, address is 00-1f-ce-10-b0-1a MTU is 1500 bytes , BW is 0 Kbit Encapsulation ARPA, loopback not set 5 minute input rate 244 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 0/600, 0 drops 1012 packets input, 193127 bytes, 0 no buffer 0 input errors, 0 CRC, 0 oversize, 0 undersize 0 jabber, 0 fragments Output packets statistics: 448 packets output, 108316 bytes, 0 underruns 0 output errors, 0 collisions </pre>

shutdown

Command	shutdown
parameter	-
default	Ethernet port is open by default.
Mode	Port Mode.
Usage Guide	When Ethernet port is shut down, no data frames are sent in the port, and the port status displayed when the user types the “show interface” command is “down”.
Example	Opening ports 1/0/1-8. <pre>Switch(config)#interface ethernet1/0/1-8</pre>

Switch(Config-If-Port-Range)#no shutdown

speed-duplex

Command **speed-duplex {force1G [auto | full]| force10G-auto | force25G-auto | force40G-auto | force100G-auto}**
no speed-duplex

parameter	force1G	is the forced 1G speed
	auto	is the auto-negotiation
	full	is the full duplex
	force10G-auto	is the forced 10G at full duplex auto mode
	force25G-auto	is the forced 25G at full duplex auto mode
	force40G-auto	is the forced 40G at full duplex auto mode
	force100G-auto	is the forced 100G at full duplex auto mode

default Auto-negotiation for speed and duplex mode is set by default

Mode Port Mode

Usage Guide This command is configures the port speed and duplex mode. When configuring port speed and duplex mode, the speed and duplex mode must be the same as the setting of the remote end, i.e., if the remote device is set to auto-negotiation, then auto-negotiation should be set at the local port. If the remote end is in forced mode, the same should be set in the local end.

Example Port 1 of Switch1 is connected to port 1 of Switch2, the following will set both ports in forced 100G at full duplex auto mode.

```
Switch1(config)#interface ethernet1/0/1
Switch1(Config-If-Ethernet1/0/1)#speed-duplex force100G-auto
Switch2(config)#interface ethernet1/0/1
Switch2(Config-If-Ethernet1/0/1)#speed-duplex force100G-auto
```

storm-control

Command **storm-control { kbps | pps }**
no storm-control pps

parameter	kbps	means the unit of limit is kbits/s
	pps	means the limit unit is packets/s.

default	The default is kbps.
Mode	Global Mode
Usage Guide	Configure the kbps or pps as the limit mode in global mode, then set broadcast, multicast or unknown unicast limit value in port mode.
Example	Setting ports 1-8 allow 1000kbit broadcast packets per second. <pre>Switch(config)#storm-control kbps</pre> <pre>Switch(config-if-port-range)#storm-control broadcast 1000</pre>

storm-control

Command	storm-control {unicast broadcast multicast} {<value> action [block shutdown trap] {recovery-interval <30-86400> trigger-count <1-180> trigger-count <1-180> recovery-interval <30-86400>}} } no storm-control {unicast broadcast multicast} action [recovery-interval trigger-count trigger-count recovery-interval]	
parameter	unicast	to limit unicast traffic for unknown destination
	broadcast	to limit broadcast traffic.
	multicast	to limit multicast traffic
	value	Limit the flow rate per second, PPS range from 1 to 148810000; kbps range from 1 to 100000000.
default	No limit is set by default. So, broadcasts, multicasts and unknown destination unicasts are allowed to pass at line speed.	
Mode	Port Mode	
Usage Guide	All ports in the switch belong to a same broadcast domain if no VLAN has been set. The switch will send the above mentioned three traffics to all ports in the broadcast domain, which may result in broadcast storm and so may greatly degrade the switch performance. Enabling Broadcast Storm Control can better protect the switch from broadcast storm. If the allowed traffic is set to 1000kbps, this means allow 1000 kbit per second and suppress the rest. The switch supports two kind of speed limit, it includes kbps which is limit by bandwidth and pps which is limit by the numbers of packets. It only can select one from the two ways and cannot set the two way in the same time (by global mode) Broadcast suppression is similar to bandwidth control. There is granularity limitation for the chip; the switch support 16Kbps granularities. If the <Kbits> that user input is not the integer times of 16, the system will adjust to the integer times of 16 automatically and print the true limit value to user.	

Example

Setting ports 1-8 allow 1000kbit broadcast packets per second.
Switch(config-if-port-range)#storm-control broadcast 1000

storm-control bypass

Command

storm-control bypass {arp | bpdu | igmp | rma | rtk } <enable | disable >

parameter

arp	means the protocol packets of arp-request
bpdu	means bpdu protocol packets
igmp	means igmp protocol packets
rma	means multicast address is the saved multicast packets
rtk	means the special private packets that realtak used
enable	enable some protocol to limit filter function
disable	disable some protocol to broadcast limit filter function.

default

Disable

Mode

Global Mode.

Usage Guide

Configure broadcast limit filter function of some protocol in global mode, then configure broadcast limit in port mode. At this moment, the protocol packets flow from the port cannot be limited.

Example

Configure arp protocol filter function to make the arp-request data packets that from 1 port in cannot be limited.
Switch (config)#storm-control bypass arp enable
Switch(config-if-ethernet1/0/1)#storm-control broadcast 1000

virtual-cable-test

Command

virtual-cable-test interface ethernet <interface-list>

parameter

<i>interface-list</i>	Port ID

default

-

Mode	Admin Mode.
Usage Guide	The RJ-45 port connected with the twisted pair under test should be in accordance with the wiring sequence rules of IEEE802.3, or the wire pairs in the test result may not be the actual ones. On a 100M port, only two pairs are used: (1, 2) and (3, 6), whose results are the only effective ones. If a 1000M port is connected to a 100M port, the results of (4, 5) and (7, 8) will be of no meaning. The result may have deviations according to the type of the twisted pair, the temperature, working voltage and other conditions. When the temperature is 20 degree Celsius, and the voltage is stable without interference, and the length of the twisted pair is not longer than 100 meters, a deviation of +/-2 meters is allowed. When the port is at Link UP status, a deviation of +/-10 meters is allowed. Notice: the test procedure will block all data flow on the line for 5-10 seconds, and then restore the original status. 568A wiring sequence: (1 green white, 2 green), (3 orange white, 6 orange), (4 blue, 5 blue white), (7 brown white, 8 brown). 568B wiring sequence: (1 orange white, 2 orange), (3 green white, 6 green), (4 blue, 5 blue white), (7 brown white, 8 brown).

Example

Test the link status of the twisted pair connected to the 1000M port 1/0/1.
Switch#virtual-cable-test interface ethernet 1/0/1

```
Interface Ethernet1/0/1:
-----
Cable pairs      Cable status      Length (meters)
-----
(1, 2)           well              1
(3, 6)           well              1
(4, 5)           well              1
(7, 8)           well              1
```

switchport discard packet

Command	switchport discard packet { tag untag } no switchport discard packet { tag untag }	
parameter	tag	means it does not receive any packet including untag, tag and the deal packet
	untag	means it does not receive untag
default	The default does not have the restriction.	
Mode	Port Mode	
Usage Guide	This command is not suggested to be configured only if there is the special	

requirement.

Example

Configure the port of 1/0/8 not to receive all packets.
Switch(config)#interface ethernet 1/0/8
Switch(config-if-ethernet1/0/8)#switchport discard packet all

switchport flood-control

Command

switchport flood-control { bcast|mcast|ucast }
no switchport flood-control { bcast|mcast|ucast }

parameter

bcast	prevents that broadcast packets cannot be transmitted to the specified port
mcast	prevents that unknown multicast packets cannot be transmitted to the specified port
ucast	prevents that unknown unicast packets cannot be transmitted to the specified port

default

Switch transmits broadcast, unknown multicast and unknown unicast packets to other port in broadcast domain.

Mode

Port configuration mode.

Usage Guide

This command takes effect for 100M and 1000M ports; it is also takes effect for Access, Trunk and Hybrid ports. When this command is valid, the port will allow unicast or multicast flow to pass after port learned the corresponding unicast mac or multicast mac.

This command only control that broadcast, multicast and unknown unicast packets sent by other ports cannot be transmitted to the specified port, but it cannot control these packets from the specified port. For example, set switchport flood-control bcast command in port 1/0/1, broadcast packets cannot be transmitted from other ports to port 1/0/1, but port 1/0/1 can receive and transmit broadcast packets.

Example

Configure flood-control of bcast and mcast for port 1/0/1 or port 1/0/8-10 respectively.
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#switchport flood-control bcast
Switch(config)#interface ethernet 1/0/8-10
Switch(config-if-port-range)#switchport flood-control mcast

switchport flood-forwarding

Command	switchport flood-forwarding mcast no switchport flood-forwarding mcast	
parameter	mcast	prevents that unknown multicast packets can be transmitted to the specified port.
default	Switch transmits unknown multicast packets to other port in broadcast domain.	
Mode	Port Mode	
Usage Guide	This command takes effect for 100M and 1000M ports; it is also takes effect for Access, Trunk and Hybrid ports. The command is usually combined with ip imgp snooping, ip imgp snooping does not supports unknown multicast and broadcast, it can transfer unknown multicast flow after configure switchport flood-forwarding mcast.	
Example	Set switch 1/0/1 port broadcast flood-forwarding. switch# switch#confi switch(config)#interface ethernet 1/0/1 switch(config-if-ethernet1/0/1)# switchport flood-forwarding mcast switch(config-if-ethernet1/0/1)#exit switch(config)#	

2 Commands for Port Isolation Function

isolate-port group

Command	isolate-port group <WORD> no isolate-port group <WORD>	
parameter	<i>WORD</i>	is the name identification of the group, no longer than 32 characters
default	-	
Mode	Global Mode	
Usage Guide	Users can create different port isolation groups based on their requirements. For example, if a user wants to isolate all downlink ports in a vlan of a switch, he can implement that by creating	

a port isolation group and adding all downlink ports of the vlan into it. No more than 16 port isolation groups can a switch have. When the users need to change or redo the configuration of the port isolation group, he can delete the existing group with the no operation of this command.

Example

Create a port isolation group and name it as "test".

Switch>enable

Switch#config

Switch(config)#isolate-port group test

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>

parameter

<i>WORD</i>	is the name identification of the group, no longer than 32 characters

<i>IFNAME</i>	is the name of the interface

default

-

Mode

Global Mode or Vlan Configuration Mode

Usage Guide

Users can add Ethernet ports into a port isolation group according to their requirements, the isolation group can isolation it from each other (Global mode) in all vlan, it also can isolate it from each other (vlan mode) in some vlan or remove them from a port isolation group according to their requirements. When an Ethernet port is a member of more than one port isolate group, it will be isolated from every port of all groups it belongs to.

Example

Add Ethernet ports 1/0/1-2 and 1/0/5 into a port isolation group named as "test",

add Ethernet ports 1/0/3-4 into a port isolation group named as "1" in vlan10.

Switch(config)#isolate-port group test switchport interface ethernet 1/0/1-2; 1/0/5

Switch(config-vlan10)#isolate-port group 1 switchport interface ethernet 1/0/3-4

isolate-port apply

Command

isolate-port apply (l2 | l3 | all |)

parameter

l2	Layer 2 traffic isolation

l3	Layer 3 traffic isolation
all	All traffic isolation

default	When no parameters are configured, all traffic on the isolation path port will be blocked.
Mode	Global Mode or Vlan Configuration Mode
Usage Guide	Users can use this command to set the conditions for port isolation and selectively isolate all or part of the traffic.
Example	Configure port isolation for Layer 2 traffic. Switch#config Switch(config)#isolate-port apply l2

show isolate-port group

Command	show isolate-port group [<WORD>]
parameter	<i>WORD</i> the name identification of the group, no longer than 32 characters
default	Display the configuration of all port isolation groups.
Mode	Admin Mode and Global Mode
Usage Guide	Users can view the configuration of port isolation with this command.
Example	Display the port isolation configuration of the port isolation group named as “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 Commands for Port Loopback Detection Function

loopback-detection control

Command	loopback-detection control {shutdown block } no loopback-detection control	
parameter	shutdown	set the control method as shutdown, which means to close down the port if a port loopback is found.
	block	set the control method as block, which means to block a port by allowing bpdu and loopback detection messages only if a port loopback is found.
default	Disable the function of loopback diction control.	
Mode	Port Mode.	
Usage Guide	Enable loopback detection control on the port, which is disabled by the NO operation of this command.	
Example	Enable the function of loopback detection control under port1/2 mode. 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	

loopback-detection control-recovery timeout

Command	loopback-detection control-recovery timeout <0-3600>	
parameter	0-3600	second is recovery time for be controlled state, 0 is not recovery state.
default	The recovery is not automatic by default.	
Mode	Global Configuration Mode.	
Usage Guide	When a port detects a loopback and works in control mode, the ports always work in control mode and not recover. The port will not sent packet to detection in shutdown mode, however, the port will sent loopback-detection packet to detection whether have loopback in block or learning mode. If the recovery time is configured, the ports will recovery normal state when the overtime is time-out. The recovery time is a useful time for shutdown control mode, because the port can keep on detection loopback in the other modes, so suggest not to use this command.	

Example	Enable automatic recovery of the loopback-detection control mode after 30s. <pre>Switch(config)#loopback-detection control-recovery timeout 30</pre>

loopback-detection interval-time

Command	loopback-detection interval-time <loopback> <no-loopback> no loopback-detection interval-time	
parameter	<i>loopback</i>	the detection interval if any loopback is found, ranging from 5 to 300, in seconds.
	<i>no-loopback</i>	the detection interval if no loopback is found, ranging from 1 to 30, in seconds.
default	The default value is 5s with loopbacks existing and 3s otherwise.	
Mode	Global Mode	
Usage Guide	When there is no loopback detection, the detection interval can be relatively shorter, for too short a time would be a disaster for the whole network if there is any loopback. So, a relatively longer interval is recommended when loopbacks exist.	
Example	Set the loopback diction interval as 35, 15. <pre>Switch(config)#loopback-detection interval-time 35 15</pre>	

loopback-detection specified-vlan

Command	loopback-detection specified-vlan <vlan-list> no loopback-detection specified-vlan [<vlan-list>]	
parameter	<i>vlan-list</i>	VLAN ID
default	Disable the function of detecting the loopbacks through the port.	
Mode	Port Mode	
Usage Guide	If a port can be a TRUNK port of multiple Vlans, the detection of loopbacks can be implemented on the basis of port+Vlan, which means the objects of the detection can be the specified Vlans on a port. If the port is an ACCESS port, only one Vlan on the port is allowed to be checked despite the fact that multiple Vlans can be configured. This	

function is not supported under Port-channel.

Example

```
Enable the function of loopback detection under port 1/2 mode.
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
```

show loopback-detection

Command

show loopback-detection [interface ethernet <interface-list>]

parameter

<i>interface-list</i>	the list of ports to be displayed, for example: ethernet 1/0/1.

default

-

Mode

Admin and Configuration Mode.

Usage Guide

Display the state and result of loopback detection on ports with this command.

Example

```
Display the state of loopback detection on port 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
Ethernet1/4 Enable Shutdown No
```

5 Commands for LLDP Function

clear lldp remote-table

Command

clear lldp remote-table

parameter

-

default

Do not clear the entries.

Mode

Port Configuration Mode

Usage Guide

Clear 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
Command	lldp {enable disable}
parameter default	- Disable LLDP function.
Mode	Global Mode
Usage Guide	If LLDP function is globally enabled, it will be enabled on every port.
Example	Enable LLDP function on the switch. Switch(config)#lldp enable

lldp enable (port)

Command	lldp {enable disable}
parameter default	- Default Open
Mode	Port Configuration Mode.
Usage Guide	When LLDP is globally enabled, it will be enabled on every port, the switch on a port is used to disable this function when it is unnecessary on the port.
Example	Disable LLDP function of port on the port ethernet 1/0/5 of the switch. Switch(config)#in ethernet 1/0/5 Switch(Config-If-Ethernet1/0/5)#lldp disable

lldp management-address tlv

Command	lldp management-address tlv {ip A.B.C.D ipv6 X:X::X:X } no lldp management-address tlv	
parameter	A.B.C.D	it is the optional parameter, and it is the management address that user appoints for the port, it must be the unicast IPv4 address
	X:X::X:X	it is the optional parameter, and it is the management address that user appoints for the port, it must be the unicast IPv6 address
default	Disable	
Mode	Port Mode	
Usage Guide	User can choose the feat management IPv4 or IPv6 address according to the configuration. If user appointed the management address when enable the function, this address will be used to send the management address TLV; if user does not appoint the management address, choose the IPv4 address from the VLAN layer3 as the management address to send the management address TLV. When the address is not appointed, if there is no feat address, the management address TLV information will not be sent.	
Example	Enable the management address TLV function of ethernet 1/0/1 and appoint the address. Switch1(Config-If-Ethernet1/0/1)# lldp management-address tlv ip 192.168.24.32	

lldp mode

Command	lldp mode <send receive both disable>	
parameter	send	Configure the LLDP function as only being able to send messages.
	receive	Configure the LLDP function as only being able to receive messages.
	both	Configure the LLDP function as being able to both send and receive messages.
	disable	Configure the LLDP function as not being able to send or receive messages.
default	The operating state of the port is “both”.	

Mode	Port Configuration Mode.
Usage Guide	Choose the operating state of the lldp Agent on the port.
Example	Configure the state of port ethernet 1/0/5 of the switch as “receive”. Switch(config)#in ethernet 1/0/5 Switch(Config-If-Ethernet1/0/5)#lldp mode receive

lldp msgTxHold

Command	lldp msgTxHold <value> no lldp msgTxHold
parameter	<i>value</i> is the aging time multiplier, ranging from 2 to 10.
default	the value of the multiplier is 4 by default.
Mode	Global Mode.
Usage Guide	After configuring the multiplier, the aging time is defined as the product of the multiplier and the interval of sending messages, and its maximum value is 65535 seconds.
Example	Set the value of the aging time multiplier as 6. Switch(config)#lldp msgTxHold 6

lldp neighbors max-num

Command	lldp neighbors max-num <value> no lldp neighbors max-num
parameter	<i>value</i> is the configured number of entries, ranging from 5 to 500.
default	The maximum number of entries can be stored in Remote MIB is 100.

Mode	Port Configuration Mode.
Usage Guide	The maximum number of entries can be stored in Remote MIB.
Example	Set the Remote as 200 on port ethernet 1/0/5 of the switch. Switch(config)#in ethernet 1/0/5 Switch(Config-If-Ethernet1/0/5)#lldp neighbors max-num 200

lldp notification interval

Command	lldp notification interval <seconds> no lldp notification interval
parameter	<i>seconds</i> is the time interval, ranging from 5 to 3600 seconds.
default	The time interval is 5 seconds.
Mode	Global Mode.
Usage Guide	After configuring the notification time interval, a “trap” message will be sent at the end of this time interval whenever the Remote Table changes.
Example	Set the time interval of sending Trap messages as 20 seconds. Switch(config)#lldp notification interval 20

lldp tooManyNeighbors

Command	lldp tooManyNeighbors {discard delete}
parameter	discard discard the current message. delete Delete the message with the least TTL in the Remoter Table
default	Discard
Mode	Port Configuration Mode

Usage Guide	When the Remote MIB is full, Discard means to discard the received message; Delete means to the message with the least TTL in the Remoter Table.
Example	Set port ethernet 1/0/5 of the switch as delete. Switch(config)#in ethernet 1/0/5 Switch(Config-If-Ethernet1/0/5)#lldp tooManyNeighbors delete

lldp transmit delay

Command	lldp transmit delay <seconds> no lldp transmit delay
parameter	<i>seconds</i> is the time interval, ranging from 1 to 8192 seconds.
default	The interval is 2 seconds by default.
Mode	Global Mode
Usage Guide	When the messages are being sent continuously, a sending delay is set to prevent the Remote information from being updated repeatedly due to sending messages simultaneously.
Example	Set the delay of sending messages as 3 seconds. Switch(config)#lldp transmit delay 3

lldp transmit optional tlv

Command	lldp transmit optional tlv [portDesc] [sysName] [sysDesc] [sysCap] no lldp transmit optional tlv
parameter	portDesc the description of the port sysName the system name sysDesc The description of the system

	sysCap the capability of the system
default	The messages carry no optional TLV by default
Mode	Port Configuration Mode
Usage Guide	When configuring the optional TLV, each TLV can only appear once in a message, portDesc optional TLV represents the name of local port; sysName optional TLV represents the name of local system; sysDesc optional TLV represents the description of local system; sysCap optional TLV represents the capability of local system.
Example	Configure that port ethernet 1/0/5 of the switch carries portDesc and sysCap TLV. <pre>Switch(config)#in ethernet 1/0/5 Switch(Config-If-Ethernet1/0/5)#lldp transmit optional tlv portDesc sysCap</pre>

lldp trap

Command	lldp trap <enable disable>
parameter	-
default	The Trap function is disabled on the specified port by default
Mode	Port Configuration Mode
Usage Guide	The function of sending Trap messages is enabled on the port.
Example	Enable the Trap function on port ethernet 1/0/5 of the switch. <pre>Switch(config)#in ethernet1/0/5 Switch(Config-If-Ethernet1/0/5)#lldp trap enable</pre>

lldp tx-interval

Command	lldp tx-interval <integer> no lldp tx-interval
parameter	<i>integer</i> is the interval of sending updating messages, ranging from 5 to

32768 seconds.

default 30s
Mode Global Mode

Usage Guide After configuring the interval of sending messages, LLDP messages can only be received after a period as long as configured. The interval should be less than or equal with half of aging time, for a too long interval will cause the state of being aged and reconstruction happen too often; while a too short interval will increase the flow of the network and decrease the bandwidth of the port. The value of the aging time of messages is the product of the multiplier and the interval of sending messages. The maximum aging time is 65535 seconds.
When tx-interval is the default value and transmit delay is configured via some commands, tx-interval will become four times of the latter, instead of the default 40.

Example Set the interval of sending messages as 40 seconds.
Switch(config)#lldp tx-interval 40

lldp dot1 pvid

Command **lldp dot1 pvid**
no lldp dot1 pvid

parameter -
default Default off

Mode Port Configuration Mode

Usage Guide This command is used to enable the transmission of 802.1 PVID (Port VLAN ID) TLV on the current interface.
After enabling, the device will include the PVID information of this port in the LLDP message, allowing neighboring devices to understand the VLAN to which this port belongs.
The no form can be used to stop sending this TLV.

Example Switch(config-if-ethernet1/0/1)#lldp dot1 pvid

lldp dot1 vlan-name

Command	lldp dot1 vlan-name no lldp dot1 vlan-name
parameter	-
default	Default off
Mode	Port Configuration Mode
Usage Guide	This command is used to enable the transmission of the 802.1 VLAN Name TLV on the current interface. After enabling, the device will include the name of the VLAN to which the port belongs in the LLDP message, facilitating neighboring devices to identify the purpose of the VLAN. The no form can be used to stop sending this TLV.
Example	Switch(config-if-ethernet1/0/1)#lldp dot1 vlan-name

lldp dot3

Command	lldp dot3 [all] [link-agg] [mac-phy] [max-frame-size] no lldp dot3 all								
parameter	<table><tr><td>all</td><td>Enable the transmission of all 802.3 optional TLVs</td></tr><tr><td>link-agg</td><td>Enable the sending of link aggregation TLV</td></tr><tr><td>mac-phy</td><td>Enable the sending of MAC/PHY configuration and status TLVs</td></tr><tr><td>max-frame-size</td><td>Enable the maximum frame size TLV for transmission</td></tr></table>	all	Enable the transmission of all 802.3 optional TLVs	link-agg	Enable the sending of link aggregation TLV	mac-phy	Enable the sending of MAC/PHY configuration and status TLVs	max-frame-size	Enable the maximum frame size TLV for transmission
all	Enable the transmission of all 802.3 optional TLVs								
link-agg	Enable the sending of link aggregation TLV								
mac-phy	Enable the sending of MAC/PHY configuration and status TLVs								
max-frame-size	Enable the maximum frame size TLV for transmission								
default	By default, LLDP messages do not carry the 802.3 optional TLVs.								
Mode	Port Configuration Mode								
Usage Guide	Use this command to enable the transmission of the optional TLVs defined by the 802.3 standard on the specified interface, allowing neighboring devices to obtain the physical layer and data link layer details of this port.								

Example

Enable all 802.3 TLVs on port 1/0/1:
Switch (config)# interface ethernet 1/0/1
Switch (config-if-ethernet1/0/1)# lldp dot3 all
Enable only the MAC/PHY configuration and status TLV on port 1/0/1:
Switch (config-if-ethernet1/0/1)# lldp dot3 mac-phy
Stop the transmission of all 802.3 TLVs on port 1/0/1:
Switch (config-if-ethernet1/0/1)# no lldp dot3 all

show debugging lldp

Command**show debugging lldp****parameter**

-

default

-

Mode

Admin and Configuration Mode

Usage Guide

With show debugging lldp, all ports with lldp debug enabled will be displayed.

Example

Display all ports with lldp debug enabled.

Switch(config)#show debugging lldp

====BEGINNING OF LLDP DEBUG SETTINGS====

debug lldp packets interface Ethernet1/0/1

=====END OF DEBUG SETTINGS=====

show lldp

Command**show lldp****parameter**

-

default

Do not display the configuration information of global LLDP.

Mode	Admin Mode, Global Mode.
Usage Guide	Users can check all the configuration information of global LLDP by using “show lldp”.
Example	Check the configuration information of global LLDP after it is enabled on the switch. Switch(config)#show lldp <pre> -----LLDP GLOBAL INFORMATION----- LLDP has been enabled globally. LLDP enabled port : Ethernet1/0/1 Ethernet1/0/7 LLDP interval :30 LLDP txTTL :120 LLDP NotificationInterval :5 LLDP txDelay :2 LLDP-MED FastStart Repeat Count :4 -----END----- </pre>

show lldp neighbors brif

Command	show lldp neighbors brif
parameter	-
default	- Or display a brief description of the ports that have LLDP neighbors, while ports without neighbors will not be shown.
Mode	Admin Mode, Global Mode.
Usage Guide	By using this command, after the port receives the LLDP data packets sent by the neighbor, it can quickly view the key LLDP and LLDP-MED information of the neighbor in a concise format, facilitating the rapid troubleshooting of the network topology.
Example	Display the brief information of the ports that have LLDP neighbors. Switch(config)#show lldp neighbors brief <pre> Local Interface Chassis ID CID subtype Port ID PID subtype Time Mark System Name Ethernet1/0/1 00-03-0f-00-00-02 4 Ethernet1/0/1 Local 20 switch </pre>

show lldp interface ethernet

Command	show lldp interface ethernet <IFNAME>	
parameter	<i>IFNAME</i>	Interface name
default	Do not display the configuration information of LLDP on the port.	
Mode	Admin Mode, Global Mode.	
Usage Guide	Users can check the configuration information of LLDP on the port by using “show lldp interface ethernet XXX”.	
Example	Check the configuration information of LLDP on the port after LLDP is enabled on the switch. Switch (config-if-ethernet1/0/1)#show lldp int e 1/0/1 Port name :Ethernet1/0/1 LLDP Agent Adminstatus : Both LLDP Operation TLV : default LLDP Management Address TLV status : unenable LLDP Trap Status : disable LLDP maxRemote :100 LLDP Overflow handle : discard LLDP interface remote status : Free lldp dot3 TLV: MED Optional TLV : default MED Trap Status:Disable MED TLV Transmit Status:Disable MED Fast Transmit Status:Disable *****	

show lldp neighbors interface ethernet

Command	show lldp neighbors interface ethernet < IFNAME >	
parameter	<i>IFNAME</i>	Interface name

default	Do not display the LLDP neighbor information of the port.
Mode	Admin Mode, Global Mode.
Usage Guide	Users can check the configuration information of LLDP on the port by using “show lldp interface ethernet XXX”.

Example Check the LLDP neighbor information of the port after LLDP is enabled on the port.
Switch (config-if-ethernet1/0/1)#show lld nei int e 1/0/1

```

Port name : Ethernet1/0/1
Port Remote Counter : 1
TimeMark :92
ChassisIdSubtype :4
ChassisId :00-e0-4c-00-00-00
PortIdSubtype :Local
PortId :gi1

Lldp Port Pvid TLV :
Lldp port Pvid                : 1

*****

```

show lldp traffic

Command	show lldp traffic
parameter	-
default	Do not display the statistics of LLDP data packets.
Mode	Admin Mode, Global Mode.
Usage Guide	Users can check the statistics of LLDP data packets by using “show lldp traffic”.

Example Check the statistics of LLDP data packets 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	43
42		0	0		
	Ethernet1/0/7	0	0	0	0
42		0	0		

6 Commands for Port Channel

interface port-channel

Command	interface port-channel <port-channel-number>
parameter	<i>port-channel-number</i> Port Channel Number
default	-
Mode	Global Mode
Usage Guide	Enable port channel configuration mode
Example	Entering configuration mode for port-channel 1. Switch(config)#interface port-channel 1 Switch(Config-If-Port-Channel1)#

lacp port-priority

Command	lacp port-priority <port-priority> no lacp port-priority
parameter	<i>port-priority</i> the port priority of LACP protocol, the range from 0 to 65535.
default	The default priority is 32768 by system.

Mode	Port Mode.
Usage Guide	Use this command to modify the port priority of LACP protocol, the no command restores the default value.
Example	Set the port priority of LACP protocol. Switch(Config-If-Ethernet1/0/1)# lacp port-priority 30000

lacp system-priority

Command	lacp system-priority <system-priority> no lacp system-priority	
parameter	<i>system-priority</i>	The system priority of LACP protocol, ranging from 0 to 65535.
default	The default priority is 32768.	
Mode	Global Mode	
Usage Guide	Use this command to modify the system priority of LACP protocol, the no command restores the default value.	
Example	Set the system priority of LACP protocol. Switch(config)#lacp system-priority 30000	

lacp timeout

Command	lacp timeout {short long} no lacp timeout
parameter	-
default	Long

Mode	Port Mode
Usage Guide	Set the timeout mode of LACP protocol.
Example	Set the timeout mode as short in LACP protocol. Switch(Config-If-Ethernet1/0/1)#lacp timeout short

port-group

Command	port-group <port-group-number> no port-group <port-group-number>
parameter	<i>port-group-number</i> is the group number of a port channel from 1 ~ 127.
default	There is no port-group
Mode	Global Mode
Usage Guide	it can create 127 port group at most
Example	Creating a port group. Switch(config)# port-group 1 Delete a port group. Switch(config)#no port-group 1

port-group mode

Command	port-group <port-group-number> mode {active passive on} no port-group
parameter	<i>port-group-number</i> is the group number of port channel, from 1 ~ 128
	active enables LACP on the port and sets it in Active mode
	passive enables LACP on the port and sets it in Passive mode
	on forces the port to join a port channel without enabling LACP.

default	Switch ports do not belong to a port channel by default; LACP not enabled by default.
Mode	Port Mode
Usage Guide	Add a physical port to the port channel NO remove the specified port from the port channel
Example	Under the Port Mode of Ethernet1/0/1, add current port to “port-group 1” in “active” mode. Switch(Config-If-Ethernet1/0/1)#port-group 1 mode active

show port-group

Command	show port-group [<i><port-group-number></i>] {brief detail }														
parameter	<i>port-group-number</i>		is the group number of port channel to be displayed, from 1~128												
default	-														
Mode	All Configuration Mode														
Usage Guide	If the user does not input port-group-number, that means the information of all the existent port-group are showed; if the port channel corresponds to port-group-number parameter and is not exist, then print a error message, otherwise display the current port-channel information of the specified group number.														
Example	Display summary information for port-group 1 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. <table><thead><tr><th>ID</th><th>Mode</th><th>Partner ID</th><th>Ports</th><th>Load-balance</th></tr></thead><tbody><tr><td>1</td><td>active</td><td>0x0000,00-00-00-00-00-00</td><td>0,0,1</td><td>src-mac</td></tr></tbody></table>					ID	Mode	Partner ID	Ports	Load-balance	1	active	0x0000,00-00-00-00-00-00	0,0,1	src-mac
ID	Mode	Partner ID	Ports	Load-balance											
1	active	0x0000,00-00-00-00-00-00	0,0,1	src-mac											

7 Commands for MTU

mtu

Command	mtu [<i><mtu-value></i>] no mtu
parameter	<i>mtu-value</i> the MTU value of frames that can be received, in byte, ranging from <1500-10222>.
default	MTU function not enabled by default
Mode	Global Mode and Port Mode
Usage Guide	Set switch of both ends mtu necessarily, or mtu frame will be dropped at the switch has not be set
Example	Enable the mtu function of the switch. Switch(config)#mtu

ip mtu

Command	ip mtu <68-10000> no ip mtu
parameter	<68-10000> The range of values for MTU
default	The default MTU value is 1476.
Mode	Interface tunnel mode
Usage Guide	This command is currently only supported in the IP GRE mode.
Example	Set the MTU to 1600 in Tunnel 1. Switch(config)#interface Tunnel1 Switch(config-if-tunnel1)#tunnel source 19.1.1.2 Switch(config-if-tunnel1)#tunnel destination 19.1.1.1 Switch(config-if-tunnel1)#tunnel mode gre ip Switch(config-if-tunnel1)#ip mtu 1600

8 Commands for EFM OAM

clear ethernet-oam

Command	clear ethernet-oam [interface {ethernet } <IFNAME>]	
parameter	<i>IFNAME</i>	the name of the port needs to clear OAM statistic information
default	N/A	
Mode	Admin mode	
Usage Guide	N/A	
Example	Clear the statistic information of OAM packets and link event on all ports. Switch#clear ethernet-oam	

ethernet-oam

Command	ethernet-oam no ethernet-oam	
parameter	-	
default	Disable	
Mode	Port mode	
Usage Guide	N/A	
Example	Enable ethernet-oam of Ethernet 1/0/4 Switch(config)#interface ethernet 1/0/4 Switch(Config-If-Ethernet1/0/4)#ethernet-oam	

ethernet-oam errored-frame threshold high

Command	ethernet-oam errored-frame threshold high {<high-frames> none} no ethernet-oam errored-frame threshold high	
parameter	<i>high-frames</i>	the high detection threshold of errored frame event, ranging from 2 to 4294967295.
	none	cancel the high threshold configuration.
default	none	
Mode	Port mode	
Usage Guide	During the specific detection period, serious link event is induced if the number of errored frame is larger than or equal to the high threshold and the device notifies the peer by sending Information OAMPDU of which the value of Link Fault flag in Flags field is 1. Note that the high threshold can not be less than the low threshold	
Example	Configure the high threshold of errored frame event on Ethernet 1/0/4 to be 3000. Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame threshold high 3000	

ethernet-oam errored-frame threshold low

Command	ethernet-oam errored-frame threshold low <low-frames> no ethernet-oam errored-frame threshold low	
parameter	<i>low-frames</i>	the low detection threshold of errored frame event, ranging from 1 to 4294967295
default	1	
Mode	Port mode	
Usage Guide	During the specific detection period, errored frame event is induced if the number of errored frame is larger than or equal to the low threshold and the device notifies the peer by sending event notification OAMPDU. Note that the low threshold can not be larger than the high threshold.	

Example	Configure the low threshold of errored frame event on Ethernet 1/0/4 to 100. Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame threshold low 100	
Command	ethernet-oam errored-frame window <seconds> no ethernet-oam errored-frame window	
parameter	<i>seconds</i>	is the time for counting the specified frame number, its range from 5 to 300, unit is 200ms
default Mode	5 Port mode	
Usage Guide	Detect the errored frame number of the port after the time of specific detection period. If the number of errored frame is larger than or equal to the threshold, bring the corresponding event and notify the peer through OAMPDU.	
Example	Configure the detection period of errored frame event on port1/0/4 to be 20s. Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame window 100	

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	
parameter	<i>high-seconds</i>	the high detection threshold of errored frame period event,ranging from 2 to 4294967295.
	none	cancel the high threshold configuration.
default Mode	none Port mode	

Usage Guide	During the specific detection period, serious link event is induced if the number of errored frame is larger than or equal to the high threshold and the device notifies the peer by sending Information OAMPDU of which the value of Link Fault flag in Flags field is 1. Note that the high threshold can not be less than the low threshold.

Example	Configure the high threshold of errored frame period event on port 1/0/4 to be 3000. Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame-seconds threshold high 3000

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

parameter	<table border="0" style="width: 100%;"> <tr> <td style="width: 30%;"><i>low-seconds</i></td> <td>the low detection threshold of errored frame seconds event, ranging from 1 to 65535 seconds.</td> </tr> </table>	<i>low-seconds</i>	the low detection threshold of errored frame seconds event, ranging from 1 to 65535 seconds.
<i>low-seconds</i>	the low detection threshold of errored frame seconds event, ranging from 1 to 65535 seconds.		

default	1
Mode	Port mode

Usage Guide	During the specific detection period, errored frame period event is induced if the number of errored frame is larger than or equal to the low threshold and the device notifies the peer by event notification OAMPDU. Note that the low threshold should not be larger than the high threshold.

Example	Configure the low threshold of errored frame period event on port 1/0/4 to be 100. Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame-seconds threshold low 100

ethernet-oam errored-frame-seconds window

Command	ethernet-oam errored-frame-seconds window <seconds> no ethernet-oam errored-frame-seconds window

parameter	<table border="0" style="width: 100%;"> <tr> <td style="width: 30%;"><i>seconds</i></td> <td>is the time for counting the specified frame number, its range</td> </tr> </table>	<i>seconds</i>	is the time for counting the specified frame number, its range
<i>seconds</i>	is the time for counting the specified frame number, its range		

from 50 to 4500, unit is 200ms.

default	300
Mode	Port mode
Usage Guide	Detect errored frame seconds of the port after the time of specific detection period. If the number of errored frame seconds is larger than or equal to the threshold, corresponding event is induced and the device notified the peer through OAMPDU.
Example	Configure the detection period of errored frame seconds event on port 1/0/4 to be 120s. Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame-seconds window 600

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	
parameter	<i>high-symbols</i>	the high detection threshold of errored symbol event, ranging from 2 to 4294967295 symbols.
	none	cancel the high threshold configuration.
default	none	
Mode	Port mode	
Usage Guide	During the specific detection period, serious link event is induced if the number of errored symbols is larger than or equal to the high threshold and the device notifies the peer by sending Information OAMPDU of which the value of Link Fault flag in Flags field is 1. Note that the high threshold should not be less than the low threshold.	
Example	Set the high threshold of errored symbol event on port 1/0/4 to none. Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-symbol-period threshold high none	

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	
parameter	<i>low-symbols</i>	the low threshold of errored symbol event, ranging from 1 to 4294967295symbols.
default	1	
Mode	Port mode	
Usage Guide	During the specific detection period, errored symbol event is induced if the number of errored symbols is larger than or equal to the low threshold and the device notifies the peer by sending event notification OAMPDU. Note that the low threshold should not be larger than the high threshold.	
Example	Set the low threshold of errored symbol event on port 1/0/4 to be 5. Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-symbol-period threshold low 5	

ethernet-oam errored-symbol-period window

Command	ethernet-oam errored-symbol-period window <seconds> no ethernet-oam errored-symbol-period window	
parameter	<i>seconds</i>	is the time for counting the specified frame number, its range from 1 to 300, unit is 200ms.
default	5	
Mode	Port mode	
Usage Guide	Detect errored symbols of the port after the time of specific detection period. If the number of errored symbols is larger than or equal to the threshold, corresponding event is induced and the device notified the peer through OAMPDU.	
Example	Set the detection period of errored symbol event on port 1/0/4 to be 2s. Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-symbol-period window 10	

ethernet-oam link-monitor

Command	ethernet-oam link-monitor no ethernet-oam link-monitor
parameter	-
default	Enable
Mode	Port mode
Usage Guide	Enable OAM to monitor local link errors. Generally link monitor is enabled when enabling OAM function of the port. When OAM link monitor is disabled, although local link error is not monitored, Event information OAMPDU from the peer is still normally received and processed.
Example	Enable the link monitor of port 1/0/4. Switch(Config-If-Ethernet1/0/4)#ethernet-oam link-monitor

ethernet-oam mode

Command	ethernet-oam mode {active passive} no ethernet-oam mode				
parameter	<table><tr><td>active</td><td>active mode</td></tr><tr><td>passive</td><td>passive mode</td></tr></table>	active	active mode	passive	passive mode
active	active mode				
passive	passive mode				
default	active mode				
Mode	Port mode				
Usage Guide	At least one of the two connected OAM entities should be configured to active mode. Once OAM is enabled, the working mode of OAM cannot be changed and you need to disable OAM function if you have to change the working mode.				

Example	Set the mode of OAM function on ethernet 1/0/4 to passive mode. Switch(Config-If-Ethernet1/0/4)#ethernet-oam mode passive	
Command	ethernet-oam period <seconds> no ethernet-oam mode	
parameter	<i>seconds</i>	sending period, ranging from 1 to 2 seconds.
default	1s	
Mode	Port mode	
Usage Guide	Use this command to configure the transmission interval of Information OAMPDU which keep OAM connection normally.	
Example	Set the transmission interval of Information OAMPDU for ethernet 1/0/4 to be 2s. Switch(Config-If-Ethernet1/0/4)# ethernet-oam period 2	

ethernet-oam remote-failure

Command	ethernet-oam remote-failure no ethernet-oam remote-failure	
parameter	-	
default	Enable	
Mode	Port mode	
Usage Guide	With remote failure indication is enabled, if critical-event or link fault event is occurred locally, it will notify the peer by sending Information OAMPDU, log the fault information and send SNMP trap warning. When the remote failure indication is disabled, although local critical-	

event or link fault event is not monitored, failure indication information from the peer is still normally received and processed.

Example

Enable remote failure indication of ethernet 1/0/4.
Switch(Config-If-Ethernet1/0/4)#ethernet-oam remote-failure

ethernet-oam remote-loopback

Command

ethernet-oam remote-loopback
no ethernet-oam remote-loopback

parameter

-

default

Disable

Mode

port mode

Usage Guide

Only OAM can send remote loopback request in auto mode, the OAM work in passive mode can not send remote loopback; when remote OAM working in loopback mode, all packets except OAM PDU packets will back local port according to the same route (Notice: during OAM loopback, it can not communicate), administrator can check the link delay of loopback, shake and throughput capacity. It can do loopback configuration after create OAM link, if OAM link is broken during loopback, the loopback will be cancel automatically. The command mutex with ethernet-oam remote-loopback supported.

Example

Enable the remote OAM of port 1/0/4 to 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]

ethernet-oam remote-loopback supported

Command

ethernet-oam remote-loopback supported

no ethernet-oam remote-loopback supported

parameter	-
default	Disable
Mode	Port mode.
Usage Guide	The port that only enable loopback support function can receive OAM loopback reques and in loopback mode. So when enable remote and in OAM loopback, please ensure remote configured loopback support. The command mutex with ethernet-oam remote-loopback.
Example	Enable OAM loopback support function of ethernet 1/0/4 Switch(Config-If-Ethernet1/0/4)#ethernet-oam remote-loopback supported

ethernet-oam timeout

Command	ethernet-oam timeout <seconds> no ethernet-oam timeout
parameter	<i>seconds</i> the timeout ranging from 5 to 10 seconds.
default	5s
Mode	Port mode
Usage Guide	OAM connection will be disconnected if no OAMPDU is received after specified timeout.
Example	Set the timeout of OAM connection for ethernet 1/0/4 to be 6 seconds. Switch(Config-If-Ethernet1/0/4)#ethernet-oam timeout 6

show ethernet-oam

Command	show ethernet-oam [{local remote}] interface {ethernet } <IFNAME>]

parameter	<i>IFNAME</i> the port that OAM connection information will be shown												
default	N/A.												
Mode	Admin mode												
Usage Guide	N/A.												
Example	Show overview information of Ethernet OAM connection. Switch#show ethernet-oam Switch#show ethernet-oam Capability codes: L - Link Monitor, R - Remote Loopback U - Unidirection, V - Variable Retrieval ----- <table><tr><td>Interface</td><td>Local-Mode</td><td>Local-Capability</td><td>Remote-MAC-Addr</td><td>Remote-Mode</td><td>Remote-Capability</td></tr><tr><td>1/0/1</td><td>active</td><td>L</td><td></td><td></td><td></td></tr></table>	Interface	Local-Mode	Local-Capability	Remote-MAC-Addr	Remote-Mode	Remote-Capability	1/0/1	active	L			
Interface	Local-Mode	Local-Capability	Remote-MAC-Addr	Remote-Mode	Remote-Capability								
1/0/1	active	L											

show ethernet-oam events

Command	show ethernet-oam events {local remote} [interface {ethernet }] <IFNAME>]	
parameter	<i>IFNAME</i>	the port that the statistic information of OAM link events needs to be shown
default	N/A.	
Mode	Admin mode	
Usage Guide	N/A.	
Example	Show the statistic information of link events on Ethernet 1/0/1. <pre>Switch#show ethernet-oam events local interface 1/0/1</pre> 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

```

show ethernet-oam link-events-configuration

Command	show ethernet-oam link-events-configuration [interface {ethernet } <IFNAME>]	
parameter	<i>IFNAME</i>	the port that the statistic information of OAM link events needs to be shown
default	N/A.	
Mode	Admin mode	
Usage Guide	N/A.	

Example	Show configuration of link events on 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 -----

show ethernet-oam loopback status

Command	show ethernet-oam loopback status [interface {ethernet } <IFNAME>]	
parameter	<i>IFNAME</i>	means display the port of OAM loopback status information
default	-	
Mode	Admin mode	
Usage Guide	Displays the loopback status OAM all or specified ports of the switch	
Example	Display the OAM loopback status of all port. Switch(config)#show ethernet-oam loopback status OAM Loopback Status: Ethernet1/0/1: disable Ethernet1/0/2: disable Ethernet1/0/3: disable	

9 Commands for PORT SECURITY

clear port-security

Command	clear port-security {all configured dynamic sticky} [[address <mac-addr> interface <interface-id>] [vlan <vlan-id>]]

parameter	all	All secure MAC entries on the interfaces
	configured	The configured secure MAC
	dynamic	The dynamic secure MAC learnt by the interface
	sticky	The secure MAC of sticky
	mac-addr	The specified secure MAC address
	interface-id	The secure MAC entries of the specified interface
	vlan-id	The specified VLAN
default	-	
Mode	Admin mode	
Usage Guide	Clear secure MACs on the interface	
Example	Clear all secure MACs on the interface Switch#clear port-security all	

show port-security

Command	show port-security [interface <interface-id>] [address vlan]	
parameter	interface-id	Show port-security configuration of the interface
	address	Show the secure address of the interface
	vlan	Show the maximum number of each VLAN configured on trunk/hybrid interface.
default	-	
Mode	Any modes	
Usage Guide	Display port security configuration.	
Example	Show all secure MACs on the interfaces. Switch# show port-security address interface ethernet 1/0/1	

switchport port-security

Command	switchport port-security no switchport port-security	
parameter	-	

default	Disable
Mode	Port mode
Usage Guide	Configure port security for the interface no disable port security with commands
Example	Enable port-security on the interface. Switch(config-if- ethernet1/0/1)#switchport port-security

switchport port-security mac-address

Command	switchport port-security mac-address <i><mac-address></i> [vlan <i><vlan-id></i>]	
	no switchport port-security mac-address <i><mac-address></i> [vlan <i><vlan-id></i>]	
parameter	<i>mac-address</i>	Configure the specified MAC address as the static secure MAC.
	<i>vlan-id</i>	The specified VLAN of the MAC address, it only takes effect on trunk and hybrid interfaces.
default	No secure MAC is bound by the interface.	
Mode	Port mode	
Usage Guide	When configuring the static secure MAC, pay attention to the number of the current secure MAC whether exceed the maximum MAC limit allowed by the interface. If exceeding the maximum MAC limit, it will result in violation operation.	
Example	Configure the secure MAC address on the interface Switch (config-if- ethernet1/0/1)# switchport port-security mac-address 00-00-00-00-00-01	

switchport port-security maximum

Command	switchport port-security maximum <value> [vlan <vlan-list>] no switchport port-security maximum <value> [vlan <vlan-list>]	
parameter	<i>value</i>	Configure the maximum number of the secure MAC allowed by the interface, its range between 1 and 4096. It is determined by the maximum MAC number of the device

	<i>vlan-list</i>	Configure the maximum value for the specified VLAN, it only takes effect on trunk and hybrid interfaces.
default	After enabling port-security, if there is no other configuration, the maximum number of the secure MAC is 1 on the interface. The interface number in VLAN is no limit by default	
Mode	Port mode	
Usage Guide	Pay attention to the coupling relation about the number between the interface and VLAN, set the maximum number configured by the interface as the standard firstly.	
Example	Configure the maximum number of the secure MAC on the interface. Switch(config-if- ethernet1/0/1)# switchport port-security maximum 100	

switchport port-security violation

Command	switchport port-security violation {protect recovery restrict shutdown} no switchport port-security violation	
parameter	protect	Protect mode, it will trigger the action that do not learn the new MAC, drop the package and do not send the warning
	recovery	After triggering the violation action of the port, the mac learning function can be recovered
	restrict	Restrict mode, it will trigger the action that do not learn the new MAC, drop the package, send snmp trap and record the configuration in syslog.
	shutdown	Shutdown mode is the default mode. Under this condition, the interface is disabled directly, send snmp trap and record the configuration in syslog.
default	shutdown	
Mode	Port mode	
Usage Guide	When exceeding the maximum number of the configured MAC addresses, MAC address accessing the interface does not belongs to this interface in MAC address table or a MAC address is configured to several interfaces in same VLAN, both of them will violate the security of the MAC address.	
Example	Configure violation mode as protect for the interface. Switch(config-if-ethernet1/0/1)#switchport port-security violation protect	

10 Commands for DDM

clear transceiver threshold-violation

Command	clear transceiver threshold-violation [interface ethernet <interface-list>]	
parameter	interface-list	The interface list that the threshold violation of the transceiver monitoring needs to be cleared.
default	-	
Mode	Admin mode	
Usage Guide	Clear threshold violations monitored by transceivers	
Example	Clear the threshold violation of the transceiver monitoring on port 21, 25, 26, 28. Switch#clear transceiver threshold-violation interface ethernet 1/0/21;25-26;28	

show transceiver

Command	show transceiver [interface ethernet <interface-list>] [detail]					
parameter	interface-list		The interface list that the monitoring of the transceiver needs to be shown.			
	detail		Show the detailed monitoring of the transceiver.			
default	-					
Mode	User mode, admin mode and global mode					
Usage Guide	Displays the transceiver's detailed monitoring information.					
Example	Show the brief DDM information of all ports.					
	Switch#show transceiver					
	Interface	Temp (°C)	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

show transceiver threshold-violation

Command `show transceiver threshold-violation [interface ethernet <interface-list>]`

parameter	interface-list	The interface list that the transceiver monitoring needs to be shown.

default -

Mode Admin mode and global mode

Usage Guide Show the transceiver monitoring

Example Show the transceiver monitoring
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 (°C)	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 1/0/26 transceiver threshold-violation information:

Transceiver monitor is disabled. Monitor interval is set to 30 minutes.

The last threshold-violation doesn't exist.

transceiver-monitoring

Command	transceiver-monitoring {enable disable}
parameter	-
default	<i>Disable</i>
Mode	<i>Port mode</i>
Usage Guide	Enable/disable transceiver monitoring
Example	Enable the transceiver monitoring of ethernet1/0/1. Switch(config-if-ethernet1/0/1)#transceiver-monitoring enable

transceiver-monitoring interval

Command	transceiver-monitoring interval <minutes> no transceiver-monitoring interval	
parameter	minutes	The interval of the transceiver monitoring needs to be set. <1-550000> minutes
default	15 minutes	
Mode	Global mode	
Usage Guide	sets the interval for transceiver monitoring. No command sets the interval to the default interval of 15 minutes.	
Example	Set the interval of the transceiver monitoring as 1 minute. Switch(config)#transceiver-monitoring interval 1	

transceiver threshold

Command `transceiver threshold {default | {temperature | voltage | bias | rx-power | tx-power} {high-alarm | low-alarm | high-warn | low-warn} {<value> | default}}`

parameter	default	Restore the threshold as the default threshold set by the manufacturer. If the monitoring index is not specified, restore all thresholds, if the monitoring index is specified, restore the corresponding threshold only.
	temperature	The monitoring index—temperature
	voltage	The monitoring index—voltage
	bias	The monitoring index—bias current
	rx-power	The monitoring index—receiving power
	tx-power	The monitoring index—sending power
	high-alarm	High-alarm of the monitoring index, namely there is alarm with A+ if exceeding the threshold.
	low-alarm	Low-alarm of the monitoring index, namely there is alarm with Aif exceeding the threshold.
	high-warn	High-warn of the monitoring index, namely there is warning with W+ if exceeding the threshold.
	low-warn	Low-warn of the monitoring index, namely there is warning with W- if exceeding the threshold.

default The threshold is set by the manufacturer

Mode Port mode

Usage Guide The range of the threshold parameters is shown for each monitoring index in the following:
Temperature: -128.00~128.00 °C
Voltage: 0.00~7.00 V
Bias current: 0.00~140.00 mA
x-power: -50.00~9.00 dBm
tx-power: -50.00~9.00 dBm
The maximum length of the threshold parameter configured by the user is 20 bits.
After the user configured a parameter threshold, the threshold set by the manufacturer will be labeled with the bracket when showing the threshold, and decide whether give an alarm according to the user's configuration.

Example Configure tx-power threshold of the fiber module, the low-warn threshold is configured as -12 on ethernet1/0/1.
Switch(config-if-ethernet1/0/1)#transceiver threshold tx-power low-warn -12

11 Commands for LLDP-MED

civic location

Command	civic location { dhcp server switch endpointDev } < <i>country-code</i> > no civic location	
parameter	dhcp server	Set device type to be DHCP server
	switch	Set device type to be Switch
	endpointDev	Set device type to be LLDP-MED Endpoint
	<i>country-code</i>	Set country code which consist of 2 letters, such as DE or US, it should accord the country code of ISO 3166 standard.
default	No location with Civic Address LCI format is configured on the port.	
Mode	Port mode	
Usage Guide	Configure device type and country code of the location with Civic Address LCI format and enter Civic Address LCI address mode to configure the more detailed location.	
Example	Configure device type as switch and country code as US for the location with Civic Address LCI format on Ethernet 19. Switch(Config-If-Ethernet1/0/19)# civic location switch US Switch(Med-Civic)#	

{**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}**

parameter

description-language	language for describing location, such as 'English'
province-state	state, canton, region, province prefecture, and so on, such as 'clara'
city	city, such as 'New York'
county	county, 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/zip code, such as '10027-1234'
otherInfo	Additional location information, such as 'South Wing'
<i>address</i>	detailed address information, it cannot exceed 250 characters

default

No detailed information of the location with Civic Address LCI is configured on the port.

Mode

Civic Address LCI address mode

Usage Guide

With this command, configure the detailed information of the location with Civic Address LCI on the port, it is able to configure 10 kinds of address types at most.

Example

Configure the detailed location information in Civic Address LCI address mode.
Switch(Med-Civic)# city Beijing
Switch(Med-Civic)# street shangdi

ecs location

Command

ecs location <tel-number>
no ecs location

parameter	<i>tel-number</i>	location characters with ECS ELIN format, such as emergent telephone number, it is character string with the length between 10 and 25.
default	No location with ECS ELIN format is configured.	
Mode	Port mode	
Usage Guide	Length range of the location character string between 10 and 25 with ECS ELIN format.	
Example	Configure the location of ECS ELIN format on port 19. Switch(Config-If-Ethernet1/0/19)# ecs location 880-445-3381	

lldp med device type endpoint

Command	lldp med device type endpoint no lldp med device type endpoint	
parameter		
default	Disable	
Mode	Global mode	
Usage Guide	This command sets LLDP-MED device type to Endpoint.	
Example	Set LLDP-MED device type to Endpoint Switch(config)# lldp med device type endpoint	

lldp med fast count

Command	lldp med fast count <value> no lldp med fast count	
parameter	<i>value</i>	The number of sending the packets fast, its range from 1 to 10, unit is entries.
default	4	
Mode	Global mode	

Usage Guide	With this command, set the number for sending the packets fast.
Example	Set the number of quick packages to 5 Switch(config)#lldp med fast count 5

lldp med trap

Command	lldp med trap {enable disable}
parameter	-
default	Disable
Mode	Port mode
Usage Guide	Enable or disable LLDP-MED TRAP of the port.
Example	Enable LLDP-MED TRAP of the port 19. Switch(Config-If-Ethernet1/0/19)# lldp med trap enable

lldp transmit med tlv all

Command	lldp transmit med tlv all no lldp transmit med tlv all
parameter	-
default	Port does not enable the function for Sending LLDP-MED TLV.
Mode	Port mode
Usage Guide	After configuring this command, if the port is able to send LLDP-MED TLV, the sent LLDP packets with LLDP-MED TLV supported by all switches. However, LLDP packets sent by the port without any LLDP-MED TLV after the switch configured the corresponding no command.
Example	Port 19 enables the function for sending LLDP-MED TLV.

Switch(Config-If-Ethernet1/0/19)# lldp transmit med tlv all

lldp transmit med tlv capability

Command	lldp transmit med tlv capability no lldp transmit med tlv capability
parameter	-
default	The function is disabled for sending LLDP-MED Capability TLV.
Mode	Port mode
Usage Guide	After configuring this command, if the port is able to send LLDP-MED TLV, the sent LLDP packets with LLDP-MED Capability TLV. However, LLDP packets sent by the port without LLDP-MED Capability TLV after the switch configured the corresponding no command. Note: LLDP-MED Capability TLV is the important LLDP-MED TLV, if do not configure the port to send LLDP-MED Capability TLV firstly, other LLDP-MED TLV will not be sent.

Example	Port 19 enables the function for sending LLDP-MED Capability TLV. Switch(Config-If-Ethernet1/0/19)# lldp transmit med tlv capability

lldp transmit med tlv extendPoe

Command	lldp transmit med tlv extendPoe no lldp transmit med tlv extendPoe
parameter	-
default	The function is disabled for sending LLDP-MED Extended Power-Via-MDI TLV.
Mode	Port mode
Usage Guide	Configure specified port to send LLDP-MED extended power supply - Via-MDITLV. No command disables the function.

Example

Port 19 enables the function for sending LLDP-MED Extended Power-Via-MDI TLV.
Switch(Config-If-Ethernet1/0/19)# lldp transmit med tlv extendPoe

lldp transmit med tlv location

Command	lldp transmit med tlv location no lldp transmit med tlv location
parameter	-
default	Disable
Mode	Port Mode
Usage Guide	Configure the specified port to send LLDP-MED Location Identification TLV. After configured this command, if the port has the capability of sending LLDP-MED TLV, the LLDP packets sent from the port will include LLDP-MED Location Identification TLV. Otherwise, the LLDP packets sent from the port will not include LLDP-MED Location Identification TLV by the no command even if the port has the capability of sending LLDP-MED TLV. Notice: Before configuring this function, the capability of sending LLDP-MED Capability TLV must be configured. If the device does not support POE or the POE function of the port is disabled by the command, this TLV will not be sent.

Example

Enable the port 19 to send LLDP-MED Location Identification TLV.
Switch(Config-If-Ethernet1/0/19)#lldp transmit med tlv location

lldp transmit med tlv inventory

Command	lldp transmit med tlv inventory no lldp transmit med tlv inventory
parameter	-
default	The function is disabled for sending LLDP-MED Inventory Management TLVs
Mode	Port mode

Usage Guide	After configuring this command, if the port is able to send LLDP-MED TLV, LLDP packets with LLDP-MED Inventory Management TLVs sent by the port. However, LLDP packets without LLDP-MED Inventory Management TLVs sent by the port after the switch configured the corresponding no command. Note: LLDP-MED Capability TLV sent by the port must be configured before sending LLDP-MED Inventory Management TLVs, or else the configuration cannot be successful.

Example	Port 19 enables the function for sending LLDP-MED Inventory Management TLVs. Switch(Config-If-Ethernet1/0/19)# lldp transmit med tlv inventory

lldp transmit med tlv networkPolicy

Command	lldp transmit med tlv networkPolicy no lldp transmit med tlv networkPolicy
parameter	-
default	The function is disabled for sending LLDP-MED Network Policy TLV.
Mode	Port mode
Usage Guide	After configuring this command, if the port is able to send LLDP-MED TLV, LLDP packets with LLDP-MED Network Policy TLV sent by the port. However, LLDP packets without LLDP-MED Network Policy TLV sent by the port after the switch configured the corresponding no command. Note: LLDP-MED Capability TLV sent by the port must be configured before sending LLDP-MED Network Policy TLV, or else the configuration cannot be successful.

Example	Port 19 enables the function for sending LLDP-MED Network Policy TLV. Switch(Config-If-Ethernet1/0/19)# lldp transmit med tlv networkPolicy

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}

parameter

status	Whether the network policy is usable.
enable	Network Policy of the specified application type has been defined, enable is the default value of the network policy.
disable	Network Policy of the specified application type has been defined, disable is the default value of the network policy
tag	Configure the specified application to uses tagged or untagged VLAN method
tagged	Configure the flow of the specified application to use the tagged vlan method, here, the fields (such as VLAN ID, Layer2 priority and DSCP value) are take effect
untagged	Configure the flow without tag for the specified application, the fields (such as VLAN ID, Layer2 priority) are ignored, only DSCP value field takes effect. Untagged is the default value of VLAN method.
vid	Configure VLAN ID that the specified application belongs to
<i>vlan-id</i>	Configure the value of VLAN ID, its range from 1 to 4094
dot1p	Configure the specified application to tag the flow by using 802.1p priority, at the same time, use vlan 0 to load the flow.
cos	Configure the priority of Ethernet frame for VLAN
<i>cos-value</i>	Configure the value of Ethernet frame priority for VLAN, its range from 0 to 7, the default value is 5.
dscp	Configure DSCP of VLAN.
<i>dscp-value</i>	DSCP value input by the user, its range from 0 to 63, the default value is 46

default

No network policy is configured on the port.

Mode

Port mode

Usage Guide

User is able to configure the network policy of many kinds on a port, but their application types cannot repeat, and a kind of network policy corresponds to a LLDP-MED network policy TLV. If user configures multi-policy for a port, it will send multi-LLDP-MED network policy TLV to a LLDP packet. If user does not configure any network policy, no LLDP-MED network policy TLV is sent to LLDP packet.

Example

Configure the network policy with the application type of voice on port 19.
Switch(Config-If-Ethernet1/0/19)# network policy voice tag tagged vid 2 cos 6 dscp 23

show lldp

Command	show lldp
parameter	-
default	-
Mode	Admin mode
Usage Guide	Show the global LLDP and LLDP-MED configuration
Example	Show 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-----
```

show lldp [interface ethernet <IFNAME>]

Command	show lldp [interface IFNAME ethernet <IFNAME>]	
parameter	IFNAME	Port name
default	-	
Mode	Admin mode	
Usage Guide	Show LLDP and LLDP-MED configurations on the current port.	
Example	Show LLDP and LLDP-MED configuration of the port 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

show lldp neighbors

Command	show lldp neighbors [brief interface ethernet <IFNAME>]	
parameter	<i>IFNAME</i>	Port number; for example :1/0/1
default	-	
Mode	Admin mode	
Usage Guide	With this command, checking LLDP and LLDP-MED information of the neighbors after the port received LLDP packets sent by the neighbors.	
Example	Show the neighbor information on port 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

show lldp traffic

Command	show lldp traffic
parameter	-
default	-
Mode	Admin Mode.
Usage Guide	After the port received the LLDP packets from the neighbor, this command can be used to view the statistics of the sent and received packets of LLDP and LLDP-MED.

Example View the statistics of the sent and received packets after the LLDP function is enabled.
Switch(config)#show lldp traffic

```
PortName Ageouts FramesDiscarded FramesInErrors FramesIn FramesOut TLVsDiscarded
TLVsUnrecognized
-----
Ethernet1/0/1 0 0 0 0 7 0
```

12 Commands for bpdutunnel

bpdutunnel-protocol

Command	bpdutunnel-protocol {stp gvrp dot1x user-defined-protocol <name>} no bpdutunnel-protocol {stp gvrp dot1x user-defined-protocol <name>}	
parameter	stp	enable bpdutunnel-protocol of stp function in port.
	gvrp	enable bpdutunnel-protocol of avrp function in port.
	dot1x	enable bpdutunnel-protocol of dot1x function in port.

name	enable bpdu-tunnel-protocol of neme function in port, the protocol name range from 1 to 31 bytes, and it made up with character, data, underline and the head and tail character can not be underline

default

-

Mode

Port Mode.

Usage Guide

When finished configure bpdu-tunnel-protocol destination MAC address of some protocol, users can enable bpdu-tunnel-protocol function of protocol in port. Stp, gvrp or dot1x function mutex with bpdu-tunnel-protocol function in port, namely, if configured stp, gvrp or dot1x function in port, the bpdu-tunnel-protocol function of the protocol configured failed; if configured bpdu-tunnel-protocol function of this protocol in port, stp, gvrp or dot1x function can not configured in port.

Example

Configure bpdu-tunnel-protocol to enable stp protocol in port 1/0/1.
Switch(Config-If-Ethernet1/0/1)# bpdu-tunnel-protocol stp

bpdu-tunnel-protocol group-mac

Command

bpdu-tunnel-protocol {stp| gvrp| dot1x} {group-mac <mac> | default-group-mac}

no bpdu-tunnel-protocol {stp| gvrp| dot1x}

parameter

stp	configure bpdu-tunnel-protocol mac of stp protocol;
gvrp	configure bpdu-tunnel-protocol mac of gvrp protocol;
dot1x	configure bpdu-tunnel-protocol mac of dot1x protocol;
mac	bpdu-tunnel-protocol mac address must be multicast address and it can not be protocodl saved address, namely address between 01-80-c2-00-00-00 and 01-80-c2-00-00-30;
default-group-mac	the default mac address is 01-00-0c-cd-00-02.

default

-

Mode

Global Mode.

Usage Guide

This command must be configured before configure bpdu-tunnel-protocol in port.

Example

Configure 01-01-00-0c -00-02 bpdu-tunnel-protocol of stp protocol.
Switch(Config)# bpdu-tunnel-protocol stp group-mac 01-01-00-0c -00-02

bpdu-tunnel-protocol protocol-mac

Command	bpdu-tunnel-protocol user-defined-protocol <name> protocol-mac <mac> {group-mac <mac> default-group-mac} no bpdu-tunnel-protocol user-defined-protocol <name>	
parameter	name	it is the protocol name and the protocol name includes 1 to 32 characters, and it makes up with character, data and underline, the head and tail character can not be underline;
	group-mac <mac>	it is the address of bpdu-tunnel-protocol mac and it must be multicast address, and it is not protocol saved address, namely the address between 01-80-c2-00-00-00 and 01-80-c2-00-00-30
	protocol-mac <mac>	it is the mac address of protocol;
	default-group-mac	The default mac address is 01-00-0c-cd-00-02
default	-	
Mode	Global Mode	
Usage Guide	The command must be configured before bpdu-tunnel-protocol in port.	
Example	Configure 01-01-00-0c-00-03 to be the bpdu-tunnel-protocol of mrpp protocol. Switch(Config)# bpdu-tunnel-protocol user-defined-protocol mrpp protocol-mac 00-03-0f-00-00-02 group-mac 01-01-00-0c -00-03	

bpdu-tunnel-protocol ethernetii

Command	bpdu-tunnel-protocol user-defined-protocol <name> protocol-mac <mac> escape-type ethernetii protocol-type <type> {group-mac <mac> default-group-mac} no bpdu-tunnel-protocol user-defined-protocol <name>	
parameter	name	it is the protocol name and the protocol name includes 1 to 32 characters, and it makes up with character, data and underline, the head and tail character can not be underline;

protocol-mac <mac>	it is the mac address of protocol;
type	the value of protocol and the format is xx-xx
group-mac <mac>	it is the address of bpdu-tunnel-protocol mac and it must be multicast address, and it is not protocol saved address, namely the address between 01-80-c2-00-00-00 and 01-80-c2-00-00-30;
default-group-mac	The default mac address is 01-00-0c-cd-00-02.

default

-

Mode

Global Mode

Usage Guide

The command must be configured before bpdu-tunnel-protocol in port.

Example

Configure 01-01-00-0c-00-04 to be the bpdu-tunnel-protocol of lldp protocol.
Switch(Config)# bpdu-tunnel-protocol user-defined-protocol lldp protocol-mac
01-80-c2-00-00-0e escape-type ethernetii protocol-type 88-cc group-mac 01-01-00-0c
-00-04

bpdu-tunnel-protocol snap

Command

**bpdu-tunnel-protocol user-defined-protocol <name> protocol-mac
<mac> escape-type snap {oui <oui>| } protocol-type <type> {group-mac <mac> |
default-group-mac}
no bpdu-tunnel-protocol user-defined-protocol <name>**

parameter

name	it is the protocol name and the protocol name includes 1 to 32characters, and it makes up with character, data and underline, the head and tail character can not be underline
protocol-mac <mac>	it is the mac address of protocol
oui	the value of oui and the format is xx-xx-xx
type	the value of protocol and the format is xx-xx
group-mac <mac>	it is the address of bpdu-tunnel-protocol mac and it must be multicast address, and it is not protocol saved address, namely the address between 01-80-c2-00-00-00 and 01-80-c2-00-00-30
default-group-mac	The default mac address is 01-00-0c-cd-00-02

default

-

Mode

Global Mode

Usage Guide

The command must be configured before bpd-tunnel-protocol in port.

Example

Configure 01-01-00-0c-00-05 to be the bpd-tunnel-protocol of Apple Talk protocol.
Switch(Config)# bpd-tunnel-protocol user-defined-protocol lldp protocol-mac
00-03-c2-00-00-05 encap-type snap oui 08-00-07 protocol-type 80-9b group-mac
01-01-00-0c -00-05

bpd-tunnel-protocol llc

Command

**bpd-tunnel-protocol user-defined-protocol <name> protocol-mac
<mac> encap-type llc dsap <dsap> ssap <ssap> {group-mac <mac> |
default-group-mac}
no bpd-tunnel-protocol user-defined-protocol <name>**

parameter

name	it is the protocol name and the protocol name includes 1 to 32 characters, and it makes up with character, data and underline, the head and tail character can not be underline
protocol-mac <mac>	it is the mac address of protocol
dsap	The dsap value of protocol and it ranges from 0 to 255
ssap	The ssap value of protocol and it ranges from 0 to 255;
group-mac <mac>	it is the address of bpd-tunnel-protocol mac and it must be multicast address, and it is not protocol saved address, namely the address between 01-80-c2-00-00-00 and 01-80-c2-00-00-30
default-group-mac	The default mac address is 01-00-0c-cd-00-02

default Mode

-
Global Mode

Usage Guide

The command must be configured before bpd-tunnel-protocol in port.

Example

Configure 01-01-00-0c-00-06 to be the bpd-tunnel-protocol of NetBIOS protocol.
Switch(Config)# bpd-tunnel-protocol user-defined-protocol lldp protocol-mac
00-03-c2-00-00-06 encap-type llc dsap 240 ssap 224 group-mac 01-01-00-0c -00-06

13 Commands for EEE Energy-saving

eee enable

Command	eee enable no eee enable
parameter	-
default	-
Mode	Port Mode
Usage Guide	It supports that configure EEE energy-saving function for the appointed port. There is not the EEE energy-saving function on port as default. After configuring the port to enable EEE energy-saving function, the port will enter the energy-saving state if stop to send packets to the port, the state of port is down. When sending packets to the port, the mode will changed from power saving mode to normal mode.
Example	Enable EEE energy-saving function: Switch(config-if-ethernet1/0/1)#eee enable

14 Commands for port-split

port-split

Command	port-split split-type {4x25G} no port-split
parameter	4X25G The 100G port has been divided into 4 25G ports.
default	The port has not been split.
Mode	Port Configuration Mode.
Usage Guide	Use the "port-split" command to configure port splitting. Save the configuration and it will take effect after a reboot. Use the "no port-split" command to cancel port splitting. Save the configuration and it will take effect after a reboot. When "port-split/no port-split" is configured but the configuration has not been saved and rebooted, the configuration can be canceled by using "no port-split" or "port-split".

Example

Configure the Interface Ethernet1/0/1 port for splitting:

```
Switch(config-if-ethernet1/0/1)#port-split split-type 4x25G
```

Warning: This operation will delete interface Ethernet1/0/1 and create new ports:

```
Ethernet1/0/1:1
```

```
Ethernet1/0/1:2
```

```
Ethernet1/0/1:3
```

```
Ethernet1/0/1:4
```

This operation will take effect after write and reboot!

```
Switch(config-if-ethernet1/0/1)#
```

Configure Interface Ethernet1/0/1: 1-4. Cancel port splitting. Select any split port and configure "no port-split":

```
Switch(config-if-ethernet1/0/1:1)#no port-split
```

Warning: This operation will delete interface Ethernet1/0/1:

```
interface Ethernet1/0/1:2
```

```
interface Ethernet1/0/1:3
```

```
interface Ethernet1/0/1:4
```

and create a new port:interface Ethernet1/0/1!

This operation will take effect after write and reboot!

```
Switch(config-if-ethernet1/0/1:1)#
```

The configuration is saved and the port splitting takes effect after the system restarts:

```
Switch(config-if-ethernet1/0/1)#end
```

```
Switch#write
```

```
***** 100% ***** te current startup-config configuration [Y/N]:y
```

```
%Apr 14 12:47:03 2086 Write configuration successfully!
```

Write running-config to current startup-config successful

```
Switch#reload
```

```
Process with reboot? [Y/N] y
```

```
Switch#
```

If the port configuration has "no port-split" set and the configuration has not been saved before restarting, now if you want to cancel this configuration, you can do so by using "port-split":

```
Switch(config-if-ethernet1/0/1:1)#no port-split
```

Warning: This operation will delete interface Ethernet1/0/1:

```
interface Ethernet1/0/1:2
```

```
interface Ethernet1/0/1:3
```

```
interface Ethernet1/0/1:4
```

and create a new port:interface Ethernet1/0/1!

This operation will take effect after write and reboot!

```
Switch(config-if-ethernet1/0/1:1)#show running-config current-mode
```

```
!
```

```
Interface Ethernet1/0/1:1
```

```
no port-split
```

```
!
```

```
Switch(config-if-ethernet1/0/1:1)#port-split split-type 4x25G
```

```
Switch(config-if-ethernet1/0/1:1)#show running-config current-mode
!
Interface Ethernet1/0/1:1
!
Switch(config-if-ethernet1/0/1:1)#
```

show port-split

Command **show port-split**

parameter -

default -

Mode Admin Mode, Global Mode.

Usage Guide Display port splitting information: Original port name (Port), port splitting status (Status), port splitting type (Split-type), split port name (Split-port).

Example Display port split information.
Ethernet1/0/1 is a split port.
Ethernet1/0/2 was originally configured with port-split split-type 4x25G, but the configuration was not saved and the system was restarted.
Ethernet1/0/3 is a split port that has been configured with "no port-split", but the configuration has not been saved and the system has been restarted.
Other ports are not configured with the split function.
Switch#show port-split

```
-----
Port                Status      Split-type  Split-port
-----
Ethernet1/0/1      Enable      4x25G       Ethernet1/0/1:1 Ethernet1/0/1:2
                  Ethernet1/0/1:3 Ethernet1/0/1:4
Ethernet1/0/2      Enable-after-reboot 4x25G       Ethernet1/0/2:1 Ethernet1/0/2:2
                  Ethernet1/0/2:3 Ethernet1/0/2:4
Ethernet1/0/3      Disable-after-reboot 4x25G       Ethernet1/0/3:1 Ethernet1/0/3:2
                  Ethernet1/0/3:3 Ethernet1/0/3:4
Ethernet1/0/4      Disable      -           -
Ethernet1/0/5      Disable      -           -
Ethernet1/0/6      Disable      -           -
Ethernet1/0/7      Disable      -           -
```


03-MAC Address

1 MAC Address Table

clear collision-mac-address-table

Command	clear collision-mac-address-table WORD
Parameter	WORD Configure mac address value
Default	none
Mode	Admin Mode
Usage	If enable the function of the hash collision mac table that issued ffp (mac-address-table avoid-collision), the mac cannot be cleared.
Example	Clear the hash collision mac table. Switch#clear collision-mac-address-table

clear mac-address-table dynamic

Command	clear mac-address-table dynamic [address <mac-addr>] [vlan <vlan-id>] [interface [ethernet portchannel] <interface-name>]
Parameter	<mac-addr> MAC address will be deleted
	<vlan-id> Vlan id
	<interface-name> port name for forwarding the MAC packets
Default	None
Mode	Admin mode.
Usage	Delete all dynamic address entries which exist in MAC address table, except application, system entries. MAC address entries can be classified according to different sources, the types are as follows: DYNAMIC, STATIC, APPLICATION, SYSTEM. DYNAMIC is the dynamic MAC address entries learned by switch, it can be aged by switch automatically.
Example	Delete all dynamic MAC Switch#clear mac-address-table dynamic

mac-address-learning enable | disable

Command	mac-address-learning (enable disable) vlan <vlan-id>
Parameter	enable Enable MAC learning through port
	disable Disable MAC learning through port
	<vlan-id> VLAN ID,range:1-4094
Default	all port auto learning mac address
Mode	Global mode
Usage	After disabling the MAC address learning function of the port, the port will not be able to automatically learn the MAC address, and the user can manage it by statically adding the MAC address.
Example	Disable the MAC learning function of port 8 Switch#config Switch(config)#mac-address-learning disable vlan 5

mac-address-table aging-time

Command	mac-address-table aging-time <0 aging-time> no mac-address-table aging-time
Parameter	0 0 to disable aging.
	aging-time aging-time seconds, range from 10 to 1000000;
Default	Default aging-time is 300 seconds.
Mode	Global Mode.
Usage	If no destination address of the packets is same with the address entry in aging-time, the address entry will get aged. The user had better set the aging-time according to the network condition, it usually use the default value.
Example	Set the aging-time to 600 seconds. Switch#config Switch(config)#mac-address-table aging-time 600

mac-address-table static | dynamic | blackhole

Command	mac-address-table {static dynamic blackhole } address <mac-addr> {vfi <NAME > vlan <vlan-id>} {peer <peer-address> interface [ethernet port-channel] <interface-name>} [source destination both] no mac-address-table {static dynamic blackhole } [address <mac-addr>] {interface [ethernet port-channel] <interface-name> vfi <NAME > vlan <vlan-id>} {peer <peer-address> interface [ethernet port-channel] <interface-name>}	
Parameter	static	static entries
	blackhole	filter entries, which is for discarding frames from specific MAC address, it can filter source address, destination address or the both. When choose the filter entries, blackhole address can't based on port, and not configure to interface;
	dynamic	dynamic address entries
	<mac-addr>	MAC address to be added or deleted
	vfi <NAME >	Vfi identifier name
	<vlan-id>	vlan number
	<peer-address>	Peer neighbor address
	<interface-name>	name of the port transmitting the MAC data packet
	source	based on source address filter
	destination	based on destination address filter
	both	based on source address and destination address filter, the default is both
Default	When VLAN interface is configured and is up, the system will generate a static address mapping entry of which the inherent MAC address corresponds to the VLAN number.	
Mode	Global Mode	
Usage	In certain special applications or when the switch is unable to dynamically learn the MAC address, users can use this command to manually establish mapping relation between the MAC address and port and VLAN. no mac-address-table command is for deleting all dynamic, static, filter MAC address entries existing in the switch MAC address list, except application, system entries. MAC address entries can be classified according to the different source, the types are as follows: DYNAMIC, STATIC, APPLICATION, SYSTEM. DYNAMIC is the dynamic MAC address entries learned by switch, it can be aged by switch automatically. STATIC is the static MAC address entries (including blackhole entries) added by user. APPLICATION is the static MAC address entries added by application protocol (such as dot1x, security port...). SYSTEM is the additive static MAC address entries according to VLAN interface. When adding STATIC entries, it can cover the conflictive DYNAMIC, except APPLICATION, SYSTEM entries. After configure the static multicast MAC by this command, the multicast MAC traffic will be forwarded to the specified port of the specified VLAN.	
Example	Port 1/0/1 belongs to VLAN200, and establishes address mapping with MAC address 00-03-0f-f0-00-18.	

Switch#config
Switch(config)#mac-address-table static address 00-03-0f-f0-00-18 vlan 200 interface ethernet 1/0/1

mac-address-table static-multicast address

Command	mac-address-table static-multicast address <mac-addr> vlan <vlan-id> interface [ethernet <interface-name>] port-channel <port-channel-id> no mac-address-table static-multicast (address <mac-addr> vlan <vlan-id>) [interface (ethernet <interface-name>] port-channel <port-channel-id>)]	
Parameter	<mac-addr>	add or delete MAC address
	<interface-name>	port that transfer MAC data packets
	<port-channel-id>	aggregate port name of transfer MAC data packets
	<vlan-id>	VLAN number
Default	When VLAN interface is configured and is up, the system will generate a static address mapping entry of which the inherent MAC address corresponds to the VLAN number	
Mode	Global Mode	
Usage	In certain special applications or when the switch is unable to dynamically learn the MAC address, users can use this command to manually establish mapping relation between the MAC address and port and VLAN. After configure the static multicast MAC by this command, the multicast MAC traffic will be forwarded to the specified port of the specified VLAN.	
Example	Configure a static multicast mac 00-00-00-00-00-00, the egress is ethernet 1/0/1. <pre>Switch#config Switch(config)# mac-address-table static-multicast address 00-00-00-00-00-00 vlan 200 interface ethernet 1/0/1</pre>	

show collision-mac-address-table

Command	show collision-mac-address-table {WORD <cr>}	
Parameter	WORD	Configure mac address value
Default	None	
Mode	Global Mode.	
Usage	If enable the function of the hash collision mac table that issued ffp (mac-address-table avoid-collision), the collision mac which issued ffp use * to sign.	

Example

```
Show the hash collision mac table.
Switch#config
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

show mac-address-table**Command**

```
show mac-address-table {static [address <mac-addr> | connection | interface | vlan
<vlan-id>] |
blackhole [address <mac-addr> [vlan <vlan-id>] | vlan <vlan-id>] |
connection [direct-connection | indirect-connection] |
aging-time |
count [interface | vlan <vlan-id> interface] [IFNAME | ethernet < IFNAME> | port-
channel < IFNAME>] |
address <mac-addr> {connection [direct-connection | indirect-connection] |
interface [IFNAME | ethernet < IFNAME> | port-channel < IFNAME>] | vlan <vlan-
id> [connection | interface]} |
multicast [vlan <vlan-id>] |
vlan <vlan-id> { connection [direct-connection | indirect-connection] | interface
[IFNAME | ethernet < IFNAME> | port-channel < IFNAME>] } |
interface {[IFNAME | ethernet < IFNAME> | port-channel < IFNAME>] connection
[direct-connection | indirect-connection]} }
```

Parameter

static	static entries
blackhole	filter entries
<aging-time>	address aging time
count	entry's number
<mac-addr>	entry's MAC address
<vlan-id>	entry's VLAN number
<interface-name>	entry's interface name

Default

MAC address table is not displayed by default

Mode

Admin and Configuration Mode.

Usage

This command can display various classes of MAC address entries. Users can also use **show mac-address-table** to display all the MAC address entries.

Example

```
Display all the filter MAC address entries.
Switch#show mac-address-table blackhole
```

show mac-address-table multicast

Command	show mac-address-table multicast (<cr> [vlan <vlan-id>])				
Parameter	<vlan-id> entry's VLAN number,range:1-4094				
Default	MAC address table is not displayed by default				
Mode	Admin and Configuration Mode.				
Usage	This command can display various classes of multicast address entries.				
Example	Display all the vlan1 multicast address entries.				
	Switch#show mac-address-table multicast vlan 1				
	Vlan Address	Insert	Type	Creator	Ports

clear mac-notification statistics

Command	clear mac-notification statistics
Parameter	None
Default	None
Mode	Admin mode
Usage	When this command is used with show command, it is able to check the executive result by show command after executing this command.
Example	Switch#clear mac-notification statistics Switch#

mac-address-table notification

Command	mac-address-table notification no mac-address-table notification
Parameter	none
Default	Disable
Mode	Global Mode
Usage	This command is used with trap switch of snmp. When disabling the MAC address notification, other configuration can be shown, but the function is invalid .
Example	Enable the MAC address notification.

Switch#config
Switch(config)#mac-address-table notification
Switch(config)#

mac-address-table notification history-size

Command	mac-address-table notification history-size <0-500> no mac-address-table notification history-size
Parameter	history-size data length of sending the notification, its range from 0 to 500
Default	10
Mode	Global Mode
Usage	After the global switch is disabled, this command is also able to be configured sequentially.
Example	Change the maximum history-size to be 256. Switch#config Switch(config)#mac-address-table notification history-size 256

mac-address-table notification interval

Command	mac-address-table notification interval <0-86400> no mac-address-table notification interval
Parameter	interval interval for sending the notification, unit is second, its range from 0 to 86400.
Default	5s
Mode	Global Mode
Usage	After the global switch is disabled, this command is also able to be configured sequentially.
Example	Configure the interval as 30s for sending the MAC address notification Switch#config Switch(config)#mac-address-table notification interval 30

mac-notification

Command	mac-notification {added all moved removed} {<cr> log trap}

Parameter	no mac-notification {<cr> log trap}	
	added	added MAC address
	all	added and the removed MAC addresses
	moved	flapping MAC address
	removed	removed MAC address
	log	print to log and terminal
	trap	trap message
Default	No MAC address notification.	
Mode	Port mode	
Usage	After the global switch is disabled, this command is also able to be configured sequentially.	
Example	Send the trap notification after the MAC address is added to Ethernet 1/0/1. Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# mac-notification added	

show mac-notification summary

Command	show mac-notification summary
Parameter	none
Default	Do not show the summary.
Mode	Admin mode
Usage	With this command, check the configuration of MAC address and the sending status of MAC notification trap.
Example	Switch#show mac-notification summary MAC address notification:enabled MAC address snmp traps:disabled MAC address notification interval = 5 MAC address notification history log size = 10 MAC address added = 0 MAC address removed = 0 MAC address moved = 0 MAC address snmp traps generated = 0

snmp-server enable traps mac-notification

Command	snmp-server enable traps mac-notification no snmp-server enable traps mac-notification
Parameter	none
Default	Disable trap notification globally.
Mode	Global Mode
Usage	This command is used with MAC notification switch. When the switch is disabled, other configuration can be shown, but the function is invalid.
Example	Enable the trap notification of MAC address Switch#config Switch(config)#snmp-server enable traps mac-notification

04-Commands for VLAN Configuration

1 VLAN

vlan

Command	vlan WORD					
	no vlan					
Parameter	WORD	WORD is the VLAN ID to be created/deleted, valid range is 1 to 4094, connect with ';' and '-'.				
Default	Only VLAN1 is set by default.					
Mode	Global Mode					
Usage	VLAN1 is the default VLAN and cannot be configured or deleted by the user. The maximal VLAN number is 4094. It should be noted that dynamic VLANs learnt by GVRP cannot be deleted by this command.					
Example	Create VLAN100 and enter the configuration mode for VLAN 100.Display the status for the current VLAN;					
	Switch#config					
	Switch(config)#vlan 100					
	Switch#show vlan					
	VLAN Name	Type	Media	Ports		

	1	default	Static	ENET	Ethernet1/0/2	Ethernet1/0/3
					Ethernet1/0/4	Ethernet1/0/5
					Ethernet1/0/6	Ethernet1/0/7
					Ethernet1/0/8	Ethernet1/0/9
					Ethernet1/0/10	Ethernet1/0/11
					Ethernet1/0/12	Ethernet1/0/13
					Ethernet1/0/14	Ethernet1/0/15
					Ethernet1/0/16	Ethernet1/0/17
					Ethernet1/0/18	Ethernet1/0/19
					Ethernet1/0/20	Ethernet1/0/21
					Ethernet1/0/22	Ethernet1/0/23
					Ethernet1/0/24	Ethernet1/0/25
					Ethernet1/0/26	Ethernet1/0/27
					Ethernet1/0/28	
	100	VLAN0100	Static	ENET		
	Switch#					

name (vlan)

Command	name NAME no name																																																																								
Parameter	NAME specified name string.																																																																								
Default	The default VLAN name is vlanXXX, where xxx is VID.																																																																								
Mode	VLAN Configuration Mode.																																																																								
Usage	The switch can specify names for different VLANs, making it easier for users to identify and manage VLANs.																																																																								
Example	Specify the name of VLAN100 as 100 Switch#config Switch(config)# vlan 100 Switch(config-vlan100)#name 100 Switch# show vlan <table><tr><th>VLAN Name</th><th>Type</th><th>Media</th><th>Ports</th></tr><tr><td colspan="4">-----</td></tr><tr><td>1</td><td>default</td><td>Static</td><td>ENET</td></tr><tr><td></td><td></td><td></td><td>Ethernet1/0/2 Ethernet1/0/3</td></tr><tr><td></td><td></td><td></td><td>Ethernet1/0/4 Ethernet1/0/5</td></tr><tr><td></td><td></td><td></td><td>Ethernet1/0/6 Ethernet1/0/7</td></tr><tr><td></td><td></td><td></td><td>Ethernet1/0/8 Ethernet1/0/9</td></tr><tr><td></td><td></td><td></td><td>Ethernet1/0/10 Ethernet1/0/11</td></tr><tr><td></td><td></td><td></td><td>Ethernet1/0/12 Ethernet1/0/13</td></tr><tr><td></td><td></td><td></td><td>Ethernet1/0/14 Ethernet1/0/15</td></tr><tr><td></td><td></td><td></td><td>Ethernet1/0/16 Ethernet1/0/17</td></tr><tr><td></td><td></td><td></td><td>Ethernet1/0/18 Ethernet1/0/19</td></tr><tr><td></td><td></td><td></td><td>Ethernet1/0/20 Ethernet1/0/21</td></tr><tr><td></td><td></td><td></td><td>Ethernet1/0/22 Ethernet1/0/23</td></tr><tr><td></td><td></td><td></td><td>Ethernet1/0/24 Ethernet1/0/25</td></tr><tr><td></td><td></td><td></td><td>Ethernet1/0/26 Ethernet1/0/27</td></tr><tr><td></td><td></td><td></td><td>Ethernet1/0/28</td></tr><tr><td>100</td><td>100</td><td>Static</td><td>ENET</td></tr></table> Switch#	VLAN Name	Type	Media	Ports	-----				1	default	Static	ENET				Ethernet1/0/2 Ethernet1/0/3				Ethernet1/0/4 Ethernet1/0/5				Ethernet1/0/6 Ethernet1/0/7				Ethernet1/0/8 Ethernet1/0/9				Ethernet1/0/10 Ethernet1/0/11				Ethernet1/0/12 Ethernet1/0/13				Ethernet1/0/14 Ethernet1/0/15				Ethernet1/0/16 Ethernet1/0/17				Ethernet1/0/18 Ethernet1/0/19				Ethernet1/0/20 Ethernet1/0/21				Ethernet1/0/22 Ethernet1/0/23				Ethernet1/0/24 Ethernet1/0/25				Ethernet1/0/26 Ethernet1/0/27				Ethernet1/0/28	100	100	Static	ENET
VLAN Name	Type	Media	Ports																																																																						

1	default	Static	ENET																																																																						
			Ethernet1/0/2 Ethernet1/0/3																																																																						
			Ethernet1/0/4 Ethernet1/0/5																																																																						
			Ethernet1/0/6 Ethernet1/0/7																																																																						
			Ethernet1/0/8 Ethernet1/0/9																																																																						
			Ethernet1/0/10 Ethernet1/0/11																																																																						
			Ethernet1/0/12 Ethernet1/0/13																																																																						
			Ethernet1/0/14 Ethernet1/0/15																																																																						
			Ethernet1/0/16 Ethernet1/0/17																																																																						
			Ethernet1/0/18 Ethernet1/0/19																																																																						
			Ethernet1/0/20 Ethernet1/0/21																																																																						
			Ethernet1/0/22 Ethernet1/0/23																																																																						
			Ethernet1/0/24 Ethernet1/0/25																																																																						
			Ethernet1/0/26 Ethernet1/0/27																																																																						
			Ethernet1/0/28																																																																						
100	100	Static	ENET																																																																						

switchport interface

Command	switchport interface [ethernet portchannel] [<interface-name interface-list>] no switchport interface [ethernet portchannel] [<interface-name interface-list>]
Parameter	ethernet Ethernet port to be added
	portchannel link-aggregation port to be added

	interface-name	port name, such as e1/0/1. If this option is selected, ethernet or portchannel should not be.			
	interface-list	port list to be added or deleted, “;” and “-” are supported, for example: ethernet1/0/1;3;4-7;8.			
Default	A newly created VLAN contains no port by default.				
Mode	VLAN Mode				
Usage	Access ports are normal ports and can join a VLAN, but a port can only join one VLAN for a time.				
Example	Assign Ethernet port 1, 3, 4-7 of VLAN100. Switch#config Switch(config)#vlan 100 Switch(config-vlan100)#switchport interface ethernet 1/0/1;3;4-7 Set the port Ethernet1/0/1 access vlan 100 successfully Set the port Ethernet1/0/3 access vlan 100 successfully Set the port Ethernet1/0/4 access vlan 100 successfully Set the port Ethernet1/0/5 access vlan 100 successfully Set the port Ethernet1/0/6 access vlan 100 successfully Set the port Ethernet1/0/7 access vlan 100 successfully Switch#show vlan				
	VLAN Name	Type	Media	Ports	

	1	default	Static	ENET	Ethernet1/0/2 Ethernet1/0/8 Ethernet1/0/9 Ethernet1/0/10 Ethernet1/0/11 Ethernet1/0/12 Ethernet1/0/13 Ethernet1/0/14 Ethernet1/0/15 Ethernet1/0/16 Ethernet1/0/17 Ethernet1/0/18 Ethernet1/0/19 Ethernet1/0/20 Ethernet1/0/21 Ethernet1/0/22 Ethernet1/0/23 Ethernet1/0/24 Ethernet1/0/25 Ethernet1/0/26 Ethernet1/0/27 Ethernet1/0/28
	100	VLAN0100	Static	ENET	Ethernet1/0/1 Ethernet1/0/3 Ethernet1/0/4 Ethernet1/0/5 Ethernet1/0/6 Ethernet1/0/7
	Switch#				

switchport forbidden vlan

Command	switchport forbidden vlan (WORD all add WORD except WORD remove WORD)

Parameter	WORD	add the vlanList as forbidden vlan and cover the previous configuration
	all	set all VLANs as forbidden vlan
	add WORD	add vlanList to the current forbidden vlanList
	except WORD	set all VLANs as forbidden vlan except vlanList
	Remove WORD	remove vlan specified by vlanList from current forbidden vlanList
Default	Forbidden vlanList is empty	
Mode	Port mode	
Usage	Tag the corresponding position for forbidden vlanList and clear allow vlanList flags in ports. A port leaves these VLANs if it joins them statically, and it sends message to GVRP module to enable corresponding registered machine of the port to enter forbidden mode. show running-config display current setting	
Example	Port quits the corresponding VLAN and the corresponding registered machine of GVRP to enter forbidden mode. <pre> Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#switchport mode hybrid Switch(config-if-ethernet1/0/1)#switchport forbidden vlan all Set the port Ethernet1/0/1 mode Hybrid successfully Switch#show running-config ! no service password-encryption ! hostname Switch sysLocation Default sysContact Default ! username admin privilege 15 password 0 admin ! authentication line console login local ! ! ! ! snmp-server enable ! ! ! ! ! ! ! ! ! </pre>	

```

!
vlan 1;100
!
Interface Ethernet1/0/1
    switchport mode hybrid
    switchport forbidden vlan 1-4094
!
Interface Ethernet1/0/2
!
Interface Ethernet1/0/3
    switchport mode trunk
    switchport trunk native vlan 100
!
Interface Ethernet1/0/4
!
Interface Ethernet1/0/5
!
Interface Ethernet1/0/6
!
Interface Ethernet1/0/7
!
Interface Ethernet1/0/8
!
Interface Ethernet1/0/9
Switch#

```

switchport mode

Command	switchport mode (access hybrid trunk)						
Parameter	<table> <tr> <td>access</td><td>Access port.</td></tr> <tr> <td>hybrid</td><td>Hybrid port.</td></tr> <tr> <td>trunk</td><td>Trunk port.</td></tr> </table>	access	Access port.	hybrid	Hybrid port.	trunk	Trunk port.
access	Access port.						
hybrid	Hybrid port.						
trunk	Trunk port.						
Default	The port is in Access mode by default.						
Mode	Port Mode.						
Usage	Ports in trunk mode is called Trunk ports. Trunk ports can allow traffic of multiple VLANs to pass through. VLAN in different switches can be interconnected with the Trunk ports. Ports under access mode are called Access ports. An access port can be assigned to one and only one VLAN at a time. Hybrid ports can allow traffic of multiple VLANs to pass through, receive and send the packets of multiple VLANs, used to connect switch, or user's computer. When Hybrid ports and Trunk ports receive the data, the deal way is same, but the deal way is different in sending the data. Because Hybrid						

ports can allow the packets of multiple VLANs to send with no tag, however, Trunk ports can only allow the packets of the default VLAN to send with no tag. The attribute of ports can not directly convert between Hybrid and Trunk, it must configure to be access at first, then configure to be Hybrid or Trunk. When the Trunk or Hybrid attribute is cancelled, the port attribute restores the default (access) attribute and belongs to vlan1.

show switchport interface display setting

Example

```
Set port 1 to hybrid mode.
Switch#config
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# switchport mode hybrid
Set the port Ethernet1/0/1 mode Hybrid successfully
Switch(config-if-ethernet1/0/1)#show switchport interface ethernet 1/0/1

Ethernet1/0/1
Type :Universal
Mode :Hybrid
Port VID :1
Switch(config-if-ethernet1/0/1)#
```

switchport hybrid native vlan

Command

switchport hybrid native vlan <vlan-id>
no switchport hybrid native vlan

Parameter

<vlan-id> VLAN ID (e.g. 100), PVID of Hybrid port.

Default

The default PVID of Hybrid port is 1.

Mode

Port Mode.

Usage

When an untagged frame enters a Hybrid port, it will be added a tag of the native PVID which is set by this command, and is forwarded to the native VLAN.

show switchport interface display setting。

Example

```
Set the native vlan to 100 for a Hybrid port.
Switch#config
Switch(config) # interface ethernet 1/0/2
Switch(config-if-ethernet1/0/2)#switchport mode hybrid
Switch(config-if-ethernet1/0/2)#switchport hybrid native vlan 100
Switch# show switchport interface ethernet 1/0/2

Ethernet1/0/2
Type :Universal
Mode :Hybrid
Port VID :100
Switch#
```

switchport hybrid allowed vlan

Command	switchport hybrid allowed vlan (WORD all add WORD except WORD remove WORD) (tag untag)	
	no switchport hybrid allowed vlan	
Parameter	WORD	Set vlan List to allowed vlan, and the late configuration will cover the previous configuration;
	all	Set all VLANs to allowed vlan;
	add WORD	Add vlanList to the existent allowed vlanList;
	except WORD	Set all VLANs to allowed vlan except the configured vlanList;
	Remove WORD	Delete the specific VLAN of vlanList from the existent allow vlanList;
	tag	Join the specific VLAN with tag mode;
	untag	Join the specific VLAN with untag mode.
Default	Deny all VLAN traffic to pass.	
Mode	Port Mode.	
Usage	The user can use this command to set the VLANs whose traffic allowed to pass through the Hybrid port, traffic of VLANs not included are prohibited. The difference between tag and untag mode by setting allowed vlan: set VLAN to untag mode, the frame sent via hybrid port without VLAN tag; set VLAN to tag mode, the frame sent via hybrid port with corresponding VLAN tag. The same VLAN can not be allowed with tag and untag mode by a Hybrid port at the same time. If configure the tag (or untag) allowed VLAN to untag (or tag) allowed VLAN, the last configuration will cover the previous. show switchport interface display setting。	
Example	<pre> Set hybrid port allowed vlan 1,100 with tag mode Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#switchport mode hybrid Set the port Ethernet1/0/1 mode Hybrid successfully Switch(config-if-ethernet1/0/1)#switchport hybrid allowed vlan 1;100 tag set the Hybrid port Ethernet1/0/1 tag allowed vlan successfully Switch#show switchport interface ethernet 1/0/1 Ethernet1/0/1 Type :Universal Mode :Hybrid Port VID :1 Hybrid tag allowed Vlan: 1;100 Switch# </pre>	

switchport access vlan

Command	switchport access vlan <valn-id> no switchport access vlan
Parameter	< valn-id > VLAN ID (e.g. 100),valid range is 1 to 4094.
Default	All ports belong to VLAN1 by default.
Mode	Port Mode.
Usage	Only ports in Access mode can join specified VLANs, and an Access port can only join one VLAN at a time. The “no switchport access vlan” command deletes the current port from the specified VLAN, and the port will be partitioned to VLAN1. show switchport interface display setting
Example	Add some Access port to VLAN100. <pre>Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#switchport mode access Set the port Ethernet1/0/1 mode Access successfully Switch(config-if-ethernet1/0/1)# switchport access vlan 100 Set the port Ethernet1/0/1 access vlan 100 successfully Switch#show switchport interface ethernet 1/0/1</pre> Ethernet1/0/1 Type :Universal Mode :Access Port VID :100 Switch#

switchport trunk allowed vlan

Command	switchport trunk allowed vlan (WORD all add WORD except WORD remove WORD) (tag untag) no switchport trunk allowed vlan										
Parameter	<table><tr><td>WORD</td><td>specified VIDs ,the range from 1 to 4094;</td></tr><tr><td>all</td><td>all VIDs</td></tr><tr><td>add WORD</td><td>add assigned VIDs behind allow vlan;</td></tr><tr><td>except WORD</td><td>all VID add to allow vlan except assigned VIDs;</td></tr><tr><td>Remove WORD</td><td>delete assigned allow vlan from allow vlan list.</td></tr></table>	WORD	specified VIDs ,the range from 1 to 4094;	all	all VIDs	add WORD	add assigned VIDs behind allow vlan;	except WORD	all VID add to allow vlan except assigned VIDs;	Remove WORD	delete assigned allow vlan from allow vlan list.
WORD	specified VIDs ,the range from 1 to 4094;										
all	all VIDs										
add WORD	add assigned VIDs behind allow vlan;										
except WORD	all VID add to allow vlan except assigned VIDs;										
Remove WORD	delete assigned allow vlan from allow vlan list.										
Default	Trunk port allows all VLAN traffic by default.										
Mode	Port Mode.										

Usage	The user can use this command to set the VLAN traffic allowed to passthrough the Trunk port; traffic of VLANs not included are prohibited. show switchport interface display setting.
Example	Set Trunk port to allow traffic of VLAN1, 3-5 Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# switchport trunk allowed vlan 1;3-5 set the trunk port Ethernet1/0/1 allowed vlan successfully. Switch#show switchport interface ethernet 1/0/1 Ethernet1/0/1 Type :Universal Mode :Trunk Port VID :1 Trunk allowed Vlan: 1;3-5 Switch#

switchport trunk native vlan

Command	switchport trunk native vlan <vlan-id> no switchport trunk allowed vlan
Parameter	<vlan-id> PVID for Trunk port.
Default	The default PVID of Trunk port is 1.
Mode	Port Mode.
Usage	PVID concept is defined in 802.1Q. PVID in Trunk port is used to tag untagged frames. When an untagged frame enters a Trunk port, the port will tag the untagged frame with the native PVID set with this commands for VLAN forwarding. show switchport interface display setting
Example	Set the native VLAN for a Trunk port to 100. Switch#config Switch(config)#interface ethernet 1/0/3 Switch(config-if-ethernet1/0/3)# switchport trunk native vlan 100 Set the port Ethernet1/0/3 native vlan 100 successfully Switch#show switchport interface ethernet 1/0/3 Ethernet1/0/3 Type :Universal Mode :Trunk Port VID :100 Trunk allowed Vlan: 1-4094 Switch#

switchport mode trunk allow-null

Command	switchport mode trunk allow-null
Parameter	none
Default	access mode.
Mode	Port mode
Usage	Configure the port as trunk, enable it to leave all VLANs and clear allow-list. show switchport interface display setting
Example	Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# switchport mode trunk allow-null Set the port Ethernet1/0/1 mode Trunk successfully Switch#show switchport interface ethernet 1/0/1 Ethernet1/0/1 Type :Universal Mode :Trunk Port VID :1 switchport mode trunk allow-null Switch#

vlan ingress enable

Command	vlan ingress enable no vlan ingress enable
Parameter	none
Default	Enable VLAN ingress filtering function.
Mode	Port Mode.
Usage	After VLAN ingress filtering is enabled on the port, when the system receives data it will check source port first, and forwards the data to the destination port if it is the VLAN member port, or else drop the data. show running-config display setting
Example	Disable VLAN ingress rules on the port. Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# no vlan ingress enable Switch# show running-config ! no service password-encryption

```

!
hostname Switch
sysLocation Default
sysContact Default
!
username admin privilege 15 password 0 admin
!
authentication line console login local
!
!
!
!
snmp-server enable
!
!
!
!
!
!
!
!
!
!
vlan 1
!
Interface Ethernet1/0/1
    no vlan ingress enable
!
Interface Ethernet1/0/2
Switch#

```

vlan-translation enable

Command	vlan-translation enable no vlan-translation enable
Parameter	none
Default	VLAN translation has not been enabled on the port by default.
Mode	Port Mode.
Usage	vlan-translation and dot1q-tunnel are mutually exclusive, it is recommended to enable vlan-translation on trunk port and manually disable port filtering.
Example	show vlan-translation display setting Enable VLAN translation function on port1. Switch#config

```

Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# vlan-translation enable
Switch# show vlan-translation
Interface Ethernet1/0/1:
    vlan-translation is enable, miss drop is not set
Switch#

```

vlan-translation

Command	vlan-translation <old-valn-id> to <new-vlan-id> {in out} no vlan-translation <old-valn-id> {in out}
Parameter	old-valn-id original VLAN ID
	new-vlan-id translated VLAN ID
	in ingress translation
	out outgress translation.
Default	There is no VLAN translation relation.
Mode	Port Mode.
Usage	The command is for configuring the translation relation of the VLAN translation function. The data packets will be matched according to the configured translation relations, and its VLAN ID will be changed to the one in the configured item once matched, while forward the packets of the original VLAN if not match. This command cannot be used with dot1q-tunnel enable at the same time. show vlan-translation display setting
Example	Move the VLAN100 data entered from the port1 to VLAN2 after ingress translation. 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# show vlan-translation Interface Ethernet1/0/1: vlan-translation is enable, miss drop is not set vlan-translation 100 to 2 in Switch#

vlan-translation miss drop

Command	vlan-translation miss drop {in out both} no vlan-translation miss drop {in out both}
Parameter	in entrance

	out	export
	both	two-way
Default	Not miss drop when translation failed.	
Mode	Port Mode.	
Usage	During translate the mapping relation between original VID and present VID, if not configure related translation, the default is not packets miss. After using the command, it will miss data packets when translation failed.	
	show vlan-translation display setting	
Example	set port 1 translation failed and miss packets in entrance. 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 miss drop in Switch# show vlan-translation Interface Ethernet1/0/1: vlan-translation is enable, miss drop is set in Switch#	

dot1q-tunnel enable

Command	dot1q-tunnel enable no dot1q-tunnel enable
Parameter	none
Default	Dot1q-tunnel function disabled on the port by default.
Mode	Port Mode.
Usage	After enabling dot1q-tunnel on the port, data packets without VLAN tag (referred to as tag) will be packed with a tag when entering through the port; those with tag will be packed with an external tag. The TPID in the tag is the global configuration TPID. it default value is 0x8100, and the VLAN ID is the VLAN ID the port belongs to. Data packets with double tags will be forwarded according to MAC address and external tag, till the external tag is removed when transmitted outside from the access port. Since the length of the data packet may be over sized when packed with external tag, it is recommended to use this command associating the Jumbo function. Normally this command is used on access ports. This command can not be used when vlan-translation enabled. show dot1q-tunnel display setting
Example	Join port1 into VLAN3, enable dot1q-tunnel function. Switch#config 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# show dot1q-tunnel
Interface Ethernet1/0/1:
    dot1q-tunnel is enable

Switch#

```

dot1q-tunnel selective enable

Command	dot1q-tunnel selective enable no dot1q-tunnel selective enable
Parameter	none
Default	Do not enable selective QinQ.
Mode	Port mode
Usage	Enable selective QinQ command should associates with hybrid mode, and it should not be used with dot1q-tunnel enable synchronously. show running-config display setting
Example	Enable dot1q-tunnel selective enable of port1. Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# dot1q-tunnel selective enable Switch# show running-config ! no service password-encryption ! hostname Switch sysLocation Default sysContact Default ! username admin privilege 15 password 0 admin ! authentication line console login local ! ! ! ! snmp-server enable ! !

```

!
!
!
!
!
!
!
vlan 1;3
!
Interface Ethernet1/0/1
    dot1q-tunnel selective enable
!
Interface Ethernet1/0/2
!
Interface Ethernet1/0/3
!
Switch#

```

dot1q-tunnel selective s-vlan

Command	dot1q-tunnel selective s-vlan <s-vlan> c-vlan <c-vid-list> no dot1q-tunnel selective s-vlan <s-vlan> c-vlan <c-vid-list>
Parameter	<s-vlan> SP VLAN ID
	<c-vid-list> range of user's VLAN ID.
Default	There is no mapping relation.
Mode	Port mode
Usage	This command is used to configure the mapping relation for selective QinQ. If packets match the mapping relation, they will be tagged with SP vlan tag as the outer VLAN tag. show running-config display setting
Example	Packets of VLAN 3 through VLAN 5 are tagged with the tag of VLAN 1 as the outer VLAN tag on Ethernet1/0/1. Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# dot1q-tunnel selective s-vlan 1 c-vlan 3-5 Switch(config-if-Ethernet1/0/1)# dot1q-tunnel selective enable Switch# show running-config ! no service password-encryption ! hostname Switch sysLocation Default sysContact Default !

```

username admin privilege 15 password 0 admin
!
authentication line console login local
!
!
!
!
snmp-server enable
!
!
!
!
!
!
!
!
!
!
vlan 1;3
!
Interface Ethernet1/0/1
    dot1q-tunnel selective s-vlan 1 c-vlan 3-5
    dot1q-tunnel selective enable
!
Interface Ethernet1/0/2
!
Interface Ethernet1/0/3
!
Interface Ethernet1/0/4
!
Interface Ethernet1/0/5
!
Interface Ethernet1/0/6
Switch#

```

garp timer join

Command	garp timer join <200-500>
Parameter	<200-500> millisecond
Default	200 ms
Mode	Global mode
Usage	Check whether the value satisfy the range. If so, modify the value of garp timer to the specified value, otherwise return a configuration error.

Example	show garp timer display setting
	Set the value of garp join timer as 210ms. Switch#config Switch(config)# garp timer join 210 Switch#show garp timer GARP join timer value is : 210 (ms) GARP leave timer value is : 600 (ms) GARP leaveall timer value is : 10000 (ms) Switch#

garp timer leave

Command	garp timer leave <500-1200>
Parameter	<500-1200> millisecond
Default	600ms
Mode	Global mode
Usage	Check whether the value satisfy the range. If so, modify the value of garp timer to the specified value, otherwise return a configuration error.
Example	show garp timer display setting
	Set the value of garp leave timer as 700ms. Switch#config Switch(config)#garp time leave 700 Switch#show garp timer GARP join timer value is : 210 (ms) GARP leave timer value is : 700 (ms) GARP leaveall timer value is : 10000 (ms) Switch#

garp timer leaveall

Command	garp timer leaveall <5000-60000>
Parameter	<500-60000> millisecond
Default	10000ms
Mode	Global mode
Usage	Check whether the value satisfy the range. If so, modify the value of garp leaveAll timer to the specified value, otherwise return a configuration error.

Example	show garp timer display setting
	Set the value of garp leaveAll as 20000ms. Switch#config Switch(config)#garp time leaveall 20000 Switch(config)#show garp timer GARP join timer value is : 210 (ms) GARP leave timer value is : 700 (ms) GARP leaveall timer value is : 20000 (ms)
	Switch#

no garp timer

Command	no garp timer (join leave leaveall)
Parameter	join join timer
	leave leave timer
	leaveall leaveAll timer
Default	200 600 10000 milliseconds for join leave leaveall timer respectively.
Mode	Global mode
Usage	Check whether the default value satisfy the range. If so, modify the value of garp join leave leaveAll timer to the default value, otherwise return a configuration error.
Example	show garp timer join display setting
	Restore garp timer join to the default value. Switch#config Switch(config)# no garp timer join Switch(config)# show garp timer join GARP join timer value is : 200 (ms)
	Switch#

gvrp(Global)

Command	gvrp no gvrp
Parameter	none
Default	Disabled.
Mode	Global mode
Usage	Enable GVRP function globally and only in this way GVRP module can work normally.

Example

	show running-config display setting
	Enable GVRP function globally.
	Switch#config
	Switch(config)#gvrp
	Switch(config)#show running-config
	!
	no service password-encryption
	!
	hostname Switch
	sysLocation Default
	sysContact Default
	!
	username admin privilege 15 password 0 admin
	!
	authentication line console login local
	!
	!
	!
	!
	snmp-server enable
	!
	!
	!
	!
	!
	!
	!
	!
	vlan 1
	!
	gvrp
	!
	Interface Ethernet1/0/1
	Switch#

gvrp(Port)

Command	gvrp no gvrp
Parameter	none
Default	Disabled
Mode	Port mode

Usage	GVRP function can only be enabled on trunk and hybrid ports, and enabling GVRP will return an error on access port. After GVRP enabled on port, this port will be added to GVRP (i.e. adding corresponding state machine to GVRP of the port). show gvrp port-member display setting
Example	Enable GVRP of port. Switch#config Switch(config)# interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#switchport mode hybrid Set the port Ethernet1/0/1 mode Hybrid successfully Switch(config-if-ethernet1/0/1)#gvrp Switch#show gvrp port-member Ports which were enabled gvrp included: Ethernet1/0/1 Switch#

private-vlan

Command	private-vlan {primary isolated community} no private-vlan						
Parameter	<table> <tr> <td>primary</td><td>set current VLAN to Primary VLAN</td></tr> <tr> <td>isolated</td><td>set current VLAN to Isolated VLAN</td></tr> <tr> <td>community</td><td>set current VLAN to Community VLAN</td></tr> </table>	primary	set current VLAN to Primary VLAN	isolated	set current VLAN to Isolated VLAN	community	set current VLAN to Community VLAN
primary	set current VLAN to Primary VLAN						
isolated	set current VLAN to Isolated VLAN						
community	set current VLAN to Community VLAN						
Default	Private VLAN is not configured by default.						
Mode	VLAN mode						
Usage	There are three Private VLANs: Primary VLAN, Isolated VLAN and Community VLAN. Ports in Primary there are three Private VLANs: Primary VLAN, Isolated VLAN and Community VLAN can communicate with ports of Isolated VLAN and Community VLAN related to this Primary VLAN; Ports in Isolated VLAN are isolated between each other and only communicate with ports in Primary VLAN they related to; ports in Community VLAN can communicate both with each other and with Primary VLAN ports they related to; there is no communication between ports in Community VLAN and port in Isolated VLAN. Only VLANs containing empty Ethernet ports can be set to Private VLAN, and only the Private VLANs configured with associated private relationships can set the Access Ethernet ports their member ports. Normal VLAN will clear its Ethernet ports when set to Private VLAN. It is to be noted Private VLAN messages will not be transmitted by GVRP. show vlan private-vlan display setting						
Example	Set VLAN100, 200, 300 to private vlans, with respectively primary, Isolated, Community types. Switch#config Switch(config)#vlan 100;200;300						

```
Switch(config)#vlan 100
Switch(config-vlan100)#private-vlan primary
Note:This will remove all the access ports from vlan 100
Switch(config-vlan100)#vlan 200
Switch(config-vlan200)#private-vlan isolated
Note:This will remove all the access ports from vlan 200
Switch(config-vlan200)#vlan 300
Switch(config-vlan300)#private-vlan community
Note:This will remove all the access ports from vlan 300
Switch# show vlan private-vlan
```

VLAN Name	Type	Asso VLAN Ports
100 VLAN0100	Primary	
200 VLAN0200	Isolate	
300 VLAN0300	Community	

```
Switch#
```

private-vlan association

Command	private-vlan association <secondary-vlan-list> no private-vlan association													
Parameter	<secondary-vlan-list>	Sets Secondary VLAN list which is associated to Primary VLAN. There are two types of Secondary VLAN: Isolated VLAN and Community VLAN. Users can set multiple Secondary VLANs by ','.												
Default	There is no Private VLAN association by default.													
Mode	VLAN Mode.													
Usage	This command can only used for Private VLAN. The ports in Secondary VLANs which are associated to Primary VLAN can communicate to the ports in Primary VLAN. Before setting Private VLAN association, three types of Private VLANs should have no member ports; the Private VLAN with Private VLAN association can't be deleted. When users delete Private VLAN association, all the member ports in the Private VLANs whose association is deleted are removed from the Private VLANs.													
Example	show vlan private-vlan display setting Associate Isolated VLAN200 and Community VLAN300 to Primary VLAN100. <pre>Switch#config Switch(config)# vlan 100 Switch(config-vlan100)#private-vlan association 200;300 Set vlan 100 associated vlan successfully Switch(config-vlan100)#show vlan private-vlan</pre> <table> <thead> <tr> <th>VLAN Name</th> <th>Type</th> <th>Asso VLAN Ports</th> </tr> </thead> <tbody> <tr> <td>100 VLAN0100</td> <td>Primary</td> <td></td> </tr> <tr> <td>200 VLAN0200</td> <td>Isolate</td> <td></td> </tr> <tr> <td>300 VLAN0300</td> <td>Community</td> <td></td> </tr> </tbody> </table>		VLAN Name	Type	Asso VLAN Ports	100 VLAN0100	Primary		200 VLAN0200	Isolate		300 VLAN0300	Community	
VLAN Name	Type	Asso VLAN Ports												
100 VLAN0100	Primary													
200 VLAN0200	Isolate													
300 VLAN0300	Community													

100	VLAN0100	Primary	200	300
200	VLAN0200	Isolate	100	
300	VLAN0300	Community	100	
Switch#				

show dot1q-tunnel

Command	Show dot1q-tunnel
Parameter	none
Default	None.
Mode	Admin and Configuration Mode.
Usage	This command is used for displaying the information of the ports at dot1q-tunnel state.
Example	Display current dot1q-tunnel state. Switch#show dot1q-tunnel Interface Ethernet1/0/1: dot1q-tunnel is enable Switch#

show garp timer

Command	Show garp timer [join leave leaveall]
Parameter	join join timer leave leave timer leaveall leaveAll timer
Default	200 600 10000 milliseconds for join leave leaveAll timer respectively.
Mode	Admin mode
Usage	Show the corresponding value of the timer specified in the command.
Example	Show the value of all garp timers currently. Switch# show garp timer GARP join timer value is : 200 (ms) GARP leave timer value is : 600 (ms) GARP leaveall timer value is : 10000 (ms) Switch#

show gvrp fsm information

Command	show gvrp fsm information interface (ethernet port-channel IFNAME)		
Parameter	ethernet	physical port	
	port-channel	aggregate port	
	IFNAME	port name	
Default	MT for registered machine and VO for request state machine.		
Mode	Admin mode		
Usage	Show the corresponding state of all registered machines and request state machines.		
Example	Show 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 Acitve member, LO:leaving Observer		
	IN:In, LV:Leaving, MT:Empty		
	INR:In Registration fixed, LVR:Leaveing Registration fixed, MTR:Empty Registration fixed		
	INF:In, registration forbidden, LVF:Leaveing, registration forbidden, MTF:Empty, registration forbidden		
	Ethernet1/0/1 gvrp fsm information:		
	Index	VLANID	Applicant Registrar
	----	-----	-----
	1	1	Qa MT
	Switch#		

show gvrp leaveAll fsm information

Command	show gvrp leaveAll fsm information interface (ethernet port-channel IFNAME)	
Parameter	ethernet	physical port
	port-channel	aggregate port
	IFNAME	port name
Default	Passive	

Mode	Admin mode								
Usage	Check the state of leaveAll state machine								
Example	Show the state of leaveAll state machine on port. Switch# show gvrp fsm information interface ethernet 1/0/1 <table> <tr> <td>Interface</td><td>LeaveAll fsm</td></tr> <tr> <td>-----</td><td>-----</td></tr> <tr> <td>Ethernet1/0/1</td><td>Passive</td></tr> <tr> <td>Switch#</td><td></td></tr> </table>	Interface	LeaveAll fsm	-----	-----	Ethernet1/0/1	Passive	Switch#	
Interface	LeaveAll fsm								
-----	-----								
Ethernet1/0/1	Passive								
Switch#									

show gvrp leavetimer running information

Command	show gvrp leavetimer running information [vlan <1-4094> interface (ethernet port-channel IFNAME)]										
Parameter	<1-4094>	Vlan tag									
	ethernet	physical port									
	port-channel	aggregate port									
	IFNAME	port name									
Default	leavetimer is disabled.										
Mode	Admin mode										
Usage	Show running state and expiration time of each leave timer.										
Example	Show running state and expiration time of each leave timer on current port. Switch# show gvrp leavetimer running information interface ethernet 1/0/1 <table> <tr> <td>VLANID</td><td>running state</td><td>expired time</td></tr> <tr> <td>-----</td><td>-----</td><td>-----</td></tr> <tr> <td>Switch#</td><td></td><td></td></tr> </table>		VLANID	running state	expired time	-----	-----	-----	Switch#		
VLANID	running state	expired time									
-----	-----	-----									
Switch#											

show gvrp port-member

Command	show gvrp [active port-member]	
Parameter	active	port is in active state
Default	GVRP is disabled on port.	
Mode	Admin mode	
Usage	Show all ports (enable GVRP) saved in GVRP.	
Example	Show all ports with GVRP enabled. Switch#show gvrp port-member Ports which were enabled gvrp included: Ethernet1/0/1 Switch#	

show gvrp port registerd vlan

Command	show gvrp port [dynamic static] registerd vlan interface (Ethernet port-channel IFNAME)	
Parameter	dynamic	dynamic registration
	static	static registration
	Ethernet	physical port
	port-channel	aggregate port
	port IFNAME	port name
Default	No dynamic or static registration VLANs on port.	
Mode	Admin mode	
Usage	Show the corresponding VLANs of the registered machines by dynamic or static registration.	
Example	Show all dynamic or static registration VLANs on current port. Switch#show gvrp port registerd vlan interface ethernet 1/0/1 Current port dynamic registerd vlan included: Current port static registerd vlan included: Switch#	

show gvrp timer running information

Command	show gvrp timer (join leaveall) running information interface (ethernet port-channel IFNAME)	
Parameter	join	join timer
	leaveall	leaveAll timer
	Ethernet	physical port
	port-channel	aggregate port
	port IFNAME	port name
Default	Join timer is disabled and leaveAll timer is enabled	
Mode	Admin mode	
Usage	Check running state of join leaveAll timer on port.	
Example	Show running state and expiration time of each timer. Switch#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 Switch#	

show gvrp vlan registerd port

Command	show gvrp vlan <1-4094> registerd port
Parameter	<1-4094> Vlan tag
Default	No ports with specified VLAN registered.
Mode	admin mode
Usage	none
Example	Show all ports with current VLAN 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) Switch#

show vlan

Command	show vlan [brief summary] [id <vlan-id>] [name <vlan-name>] [internal usage [id <vlan-id> name <vlan-name>]]
Parameter	brief brief information; summary VLAN statistics <vlan-id> for VLAN ID of the VLAN to display status information, the valid range is 1 to 4094; <vlan-name> is the VLAN name for the VLAN to display status information, valid length is 1 to 11 characters.
Default	none
Mode	Admin Mode and Configuration Mode.
Usage	If no <vlan-id> or <vlan-name> is specified, then information for all VLANs in the switch will be displayed.
Example	Display the status for the current VLAN; display statistics for the current VLAN. Switch#show vlan VLAN Name Type Media Ports ----- 1 default Static ENET Ethernet1/0/2 Ethernet1/0/3 Ethernet1/0/4 Ethernet1/0/5 Ethernet1/0/6 Ethernet1/0/7 Ethernet1/0/8 Ethernet1/0/9 Ethernet1/0/10 Ethernet1/0/11 Ethernet1/0/12 Ethernet1/0/13 Ethernet1/0/14 Ethernet1/0/15 Ethernet1/0/16 Ethernet1/0/17

Ethernet1/0/18	Ethernet1/0/19
Ethernet1/0/20	Ethernet1/0/21
Ethernet1/0/22	Ethernet1/0/23
Ethernet1/0/24	Ethernet1/0/25
Ethernet1/0/26	Ethernet1/0/27
Ethernet1/0/28	

```
Switch#show vlan summary
The max. Vlan entries: 4094
```

```
Existing Vlan:
Universal Vlan:
1
Private Vlan:
100 200 300
```

```
Total Existing Vlan:4
Switch#
```

displayed information	Explanation
VLAN	VLAN ID
Name	VLAN name
Type	VLAN type, statically configured or dynamically learned.
Media	VLAN interface type: Ethernet
Ports	Access port within a VLAN

show vlan-translation

Command	show vlan-translation
Parameter	None
Default	none
Mode	Admin and Configuration Mode.
Usage	Display the information of all the ports at VLAN-translation state.
Example	Display current VLAN translation state information. Switch#show vlan-translation vlan-translation n-to-1 2-4 to 100

vlan-translation n-to-1

Command	vlan-translation n-to-1 <WORD> to <new-vlan-id>

Parameter	no vlan-translation n-to-1 <WORD>	
	<WORD>	original VLAN ID, its range from 1 to 4094, connect them with ‘;’ and ‘-’. If there are two VLANs with different range are translated into different VLAN ID in the same port, two VLAN ranges should not be superposed.
Default	<new-vlan-id>	translated VLAN ID,its range from 1 to 4094.
	Disable	
Mode	Global Mode	
Usage	Multi-to-One VLAN translation is used to network edge to map multiple VLANs to one VLAN of backbone network. When data traffic returns from backbone network to network edge, it will restore VLAN of network edge to implement Multi-to-One VLAN translation and save VLAN resource of backbone network. Note: When using this function, the device must establish the original and the translated VLAN firstly, and enabling the downlink port of this function and the uplink port for connecting backbone network, which must be join in the original and the translated VLAN with tagged mode. This function should not be used with dot1q-tunnel and VLAN translation at the same time Note: Multi-to-One VLAN translation should be enabled after MAC learning. show vlan-translation display setting。	
Example	translate the data traffic from VLAN with the range between 1 to 5 into VLAN 100, and translate the data traffic (belongs to VLAN with the range between 1 to 5) out from VLAN100 into the corresponding VLAN ID Switch#config Switch(config)#vlan 1;5;100 Switch(config)#vlan 2-4 Switch(config)#vlan-translation n-to-1 2-4 to 100	

dynamic-vlan mac-vlan prefer

Command	dynamic-vlan mac-vlan prefer
Parameter	None
Default	MAC-based VLAN is preferred by default.
Mode	Global Mode.
Usage	Configure the preference of dynamic-vlan on switch. The default priority sequence is MAC-based VLAN. IP-subnet-based VLAN. Protocol-based VLAN, namely the preferred order when several dynamic VLAN is available. After the IP-subnet-based VLAN is set to be preferred and the user wish to restore to preferring the MAC-based VLAN, please use this command. show dynamic-vlan prefer display setting。
Example	Set the MAC-based VLAN preferred. Switch#config Switch(config)#dynamic-vlan mac-vlan prefer Switch#show dynamic-vlan prefer

Mac Vlan/Voice Vlan
IP Subnet Vlan
Protocol Vlan

dynamic-vlan subnet-vlan prefer

Command	dynamic-vlan subnet-vlan prefer
Parameter	None
Default	MAC-based VLAN is preferred by default.
Mode	Global Mode.
Usage	Configure the preference of dynamic-vlan on switch. The default priority sequence is MAC-based VLAN. IP-subnet-based VLAN. Protocol-based VLAN, namely the preferred order when several dynamic VLAN is available. This command is used to set to preferring the IP-subnet-based VLAN. show dynamic-vlan prefer display setting.
Example	Set the IP-subnet-based VLAN preferred. Switch#config Switch(config)#dynamic-vlan subnet-vlan prefer Switch(config)#show dynamic-vlan prefer IP Subnet Vlan Mac Vlan/Voice Vlan Protocol Vlan

mac-vlan vlan

Command	mac-vlan vlan <vlan-id> no mac-vlan vlan <vlan-id>																													
Parameter	<vlan-id> <vlan-id> is the number of the specified VLAN.																													
Default	No MAC VLAN is configured by default.																													
Mode	Global Mode.																													
Usage	Set specified VLAN for MAC VLAN. show mac-vlan display setting.																													
Example	Set VLAN100 to MAC VLAN. Switch#config Switch(config)#mac-vlan vlan 100 Switch#show vlan <table><tr><th colspan="2">VLAN Name</th><th>Type</th><th>Media</th><th colspan="2">Ports</th></tr><tr><td colspan="6">-----</td></tr><tr><td>1</td><td>default</td><td>Static</td><td>ENET</td><td>Ethernet1/0/1</td><td>Ethernet1/0/2</td></tr><tr><td></td><td></td><td></td><td></td><td>Ethernet1/0/3</td><td>Ethernet1/0/4</td></tr></table>						VLAN Name		Type	Media	Ports		-----						1	default	Static	ENET	Ethernet1/0/1	Ethernet1/0/2					Ethernet1/0/3	Ethernet1/0/4
VLAN Name		Type	Media	Ports																										

1	default	Static	ENET	Ethernet1/0/1	Ethernet1/0/2																									
				Ethernet1/0/3	Ethernet1/0/4																									

	Ethernet1/0/5	Ethernet1/0/6
	Ethernet1/0/7	Ethernet1/0/8
	Ethernet1/0/9	Ethernet1/0/10
	Ethernet1/0/11	Ethernet1/0/12
	Ethernet1/0/13	Ethernet1/0/14
	Ethernet1/0/15	Ethernet1/0/16
	Ethernet1/0/17	Ethernet1/0/18
	Ethernet1/0/19	Ethernet1/0/20
	Ethernet1/0/21	Ethernet1/0/22
	Ethernet1/0/23	Ethernet1/0/24
	Ethernet1/0/25	Ethernet1/0/26
	Ethernet1/0/27	Ethernet1/0/28
100	VLAN0100	UserDynam ENET

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}			
Parameter	<mac-addrss>/<mac-mask>mac-address/mac-mask format:XX-XX-XX-XX-XX-XX <vlan-id>vlan-id is the ID of the VLAN with a valid range of 1~4094 <priority-id>priority-id is the level of priority and is used in the VLAN tag with a valid range of 0~7			
Default	No MAC address joins the VLAN by default.			
Mode	Global Mode			
Usage	With this command user can add specified MAC address to specified VLAN. If there is a non VLAN label data packet enters from the switch port from the specified MAC address, it will be assigned with specified VLAN ID so sent enter specified VLAN. Their belonging VLAN are the same no matter which port did they enter through. The command does not have any interfere on the VLAN label data packet.			
Example	show mac-vlan display setting			
	Add network device of MAC address as 00-03-0f-11-22-33 to VLAN 100.			
	Switch#config			
	Switch(config)#mac-vlan vlan 100			
	Switch(config)#mac-vlan mac 00-03-0f-11-22-33 ff-ff-ff-ff-ff-ff vlan 100 priority 0			
	Switch#show mac-vlan			
	Mac-Address	Mac-Mask	VLAN_ID	Priority
	-----	-----	-----	-----
	00-03-0f-11-22-33	ff-ff-ff-ff-ff-ff	100	0

protocol-vlan

Command	protocol-vlan mode (ethernetII snap) etype <etype-id> vlan <vlan-id> [priority <priority-id>] protocol-vlan mode llc dsap <dsap-id> ssap <ssap-id> vlan <vlan-id> no protocol-vlan (mode ((ethernetII snap) etype <etype-id>) all} no protocol-vlan mode llc dsap <dsap-id> ssap <ssap-id>																				
Parameter	<etype-id>	etype-id is the type of the packet protocol, with a valid range of 1536~65535;																			
	<vlan-id>	vlan-id is the ID of VLAN, the valid range is 1~4094。																			
	<priority-id>	priority-id is the priority, the range is 0~7																			
	<dsap-id>/<ssap-id>	dsap-id is Dsap ID, ssap-id is Ssap ID, the range is 0-255																			
Default	No protocol joined the VLAN by default																				
Mode	Global Mode																				
Usage	The command adds specified protocol into specified VLAN. If there is any non VLAN label packet from specified protocol enters through the switch port, it will be assigned with specified VLAN ID and enter the specified VLAN. No matter which port the packets go through, their belonging VLAN is the same. The command will not interfere with VLAN labeled data packets. It is recommended to configure ARP protocol together with the IP protocol or else some application may be affected. show protocol -vlan display setting。																				
Example	Assign the IP protocol data packet encapsulated by the EthernetII to VLAN200 Switch#config Switch(config)#protocol-vlan mode ethernetII etype 1536 vlan 200 Switch#show protocol-vlan <table><tr><td>Protocol_Type</td><td>VLAN_ID</td><td>Priority</td></tr><tr><td>-----</td><td>-----</td><td>-----</td></tr><tr><td>mode ethernetii etype 0x600</td><td>200</td><td>0</td></tr><tr><td>mode ethernetii etype 0x60e</td><td>1</td><td>7</td></tr><tr><td>mode snap etype 0x613</td><td>1</td><td>1</td></tr><tr><td>mode llc dsap 0x1 ssap 0x1</td><td>1</td><td>0</td></tr></table>			Protocol_Type	VLAN_ID	Priority	-----	-----	-----	mode ethernetii etype 0x600	200	0	mode ethernetii etype 0x60e	1	7	mode snap etype 0x613	1	1	mode llc dsap 0x1 ssap 0x1	1	0
Protocol_Type	VLAN_ID	Priority																			
-----	-----	-----																			
mode ethernetii etype 0x600	200	0																			
mode ethernetii etype 0x60e	1	7																			
mode snap etype 0x613	1	1																			
mode llc dsap 0x1 ssap 0x1	1	0																			

show dynamic-vlan prefer

Command	show dynamic-vlan prefer
Parameter	None
Default	Mac Vlan/Voice Vlan
Mode	Admin Mode and Configuration Mode.
Usage	Display the dynamic VLAN preference.
Example	Display current dynamic VLAN preference.

```
Switch#show dynamic-vlan prefer
Mac Vlan/Voice Vlan
IP Subnet Vlan
Protocol Vlan
```

show mac-vlan interface

Command	show mac-vlan interface
Parameter	None
Default	None
Mode	Admin Mode and other configuration Mode.
Usage	Display the ports of enabling MAC-based VLAN, the character in the bracket indicate the ports mode, A means Access port, T means Trunk port, H means Hybrid port.
Example	Display the ports of enabling MAC-based VLAN currently. Switch#show mac-vlan Ports ----- Ethernet1/0/1(A) Ethernet1/0/2(A) Ethernet1/0/3(A) Ethernet1/0/4(A) Ethernet1/0/5(A) Ethernet1/0/6(A) Ethernet1/0/7(A) Ethernet1/0/8(A) Ethernet1/0/9(A) Ethernet1/0/10(A) Ethernet1/0/11(A) Ethernet1/0/12(A) Ethernet1/0/13(A) Ethernet1/0/14(A) Ethernet1/0/15(A) Ethernet1/0/16(A) Ethernet1/0/17(A) Ethernet1/0/18(A) Ethernet1/0/19(A) Ethernet1/0/20(A) Ethernet1/0/21(A) Ethernet1/0/22(A) Ethernet1/0/23(A) Ethernet1/0/24(A) Ethernet1/0/25(A) Ethernet1/0/26(A) Ethernet1/0/27(A) Ethernet1/0/28(A)

show protocol-vlan

Command	show protocol-vlan
Parameter	None
Default	None
Mode	Admin Mode and Configuration Mode
Usage	Display the configuration of Protocol-based VLAN on the switch.

Example	Display the configuration of the current Protocol-based VLAN.		
	Switch#show protocol-vlan		
	Protocol_Type	VLAN_ID	Priority
	-----	-----	
	mode ethernetii etype 0x600	200	0
	mode ethernetii etype 0x60e	1	7
	mode snap etype 0x613	1	1
	mode llc dsap 0x1 ssap 0x1	1	0

show subnet-vlan

Command	show subnet-vlan
Parameter	None
Default	None
Mode	Admin Mode and other Configuration Mode.
Usage	Display the configuration of the IP-subnet-based VLAN on the switch.
Example	Display the configuration of the current IP-subnet-based VLAN.
	Switch#show subnet-vlan
	IP-Address Mask VLAN_ID Priority
	----- ----- ----- -----
	192.168.5.2 255.255.255.0 100 0

show subnet-vlan interface

Command	show subnet-vlan interface
Parameter	None
Default	None
Mode	Admin Mode and other Configuration Mode.
Usage	Display the port of enabling IP-subnet-based VLAN, the character in the bracket indicate the ports mode, A means Access port, T means Trunk port, H means Hybrid port.
Example	Display the port of enabling IP-subnet-based VLAN currently.
	Switch#show subnet-vlan interface
	Ports

	Ethernet1/0/1(A) Ethernet1/0/2(A)
	Ethernet1/0/3(A) Ethernet1/0/4(A)
	Ethernet1/0/5(A) Ethernet1/0/6(A)
	Ethernet1/0/7(A) Ethernet1/0/8(A)
	Ethernet1/0/9(A) Ethernet1/0/10(A)

Ethernet1/0/11(A)	Ethernet1/0/12(A)
Ethernet1/0/13(A)	Ethernet1/0/14(A)
Ethernet1/0/15(A)	Ethernet1/0/16(A)
Ethernet1/0/17(A)	Ethernet1/0/18(A)
Ethernet1/0/19(A)	Ethernet1/0/20(A)
Ethernet1/0/21(A)	Ethernet1/0/22(A)
Ethernet1/0/23(A)	Ethernet1/0/24(A)
Ethernet1/0/25(A)	Ethernet1/0/26(A)
Ethernet1/0/27(A)	Ethernet1/0/28(A)

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}			
Parameter	<ipv4-addrss>	ipv4-address is the IPv4 address shown in dotted decimal notation; the valid range of each section is 0~255;		
	<subnet-mask>	subnet-mask is the subnet mask code shown in dotted decimal notation; the valid range of each section is 0~255;		
	<vlan-id>	vlan-id is the VLAN ID with a valid range of 1~4094		
	<priority-id>	priority-id is the priority applied in the VLAN tag with a valid range of 0~7;		
Default	No IP subnet joined the VLAN by default.			
Mode	Global Mode.			
Usage	This command is used for adding specified IP subnet to specified VLAN. When packet without VLAN label and from the specified IP subnet enters through the switch port, it will be matched with specified VLAN id and enters specified VLAN. These packets will always come to the same VLAN no matter through which port did they enter. This command will not interfere with VLAN labeled data packets.			
	show subnet-vlan display setting.			
Example	Add the network equipment with IP subnet of 192.168.1.1/24 to VLAN 300			
	Switch#config			
	Switch(config)#vlan 300			
	Switch(config-vlan300)#exit			
	Switch(config)#subnet-vlan ip-address 192.168.1.1 mask 255.255.255.0 vlan 300 priority 0			
	Switch(config)#show subnet-vlan			
	IP-Address	Mask	VLAN_ID	Priority
-----	-----	-----	-----	
192.168.1.1	255.255.255.0	300	0	

switchport mac-vlan enable

Command	switchport mac-vlan enable no switchport mac-vlan enable
Parameter	none
Default	The MAC-base VLAN function is enabled on the port by default.
Mode	Port Mode.
Usage	After adding a MAC address to specified VLAN, the MAC-based VLAN function will be globally enabled. This command can disable the MAC-based VLAN function on specified port to meet special user applications. show mac-vlan interface display setting。
Example	Disable the MAC-based VLAN function on port1. Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#no switchport mac-vlan enable Switch(config-if-ethernet1/0/1)#show mac-vlan interface Ports ----- Ethernet1/0/2(A) Ethernet1/0/3(A) Ethernet1/0/4(A) Ethernet1/0/5(A) Ethernet1/0/6(A) Ethernet1/0/7(A) Ethernet1/0/8(A) Ethernet1/0/9(A) Ethernet1/0/10(A) Ethernet1/0/11(A) Ethernet1/0/12(A) Ethernet1/0/13(A) Ethernet1/0/14(A) Ethernet1/0/15(A) Ethernet1/0/16(A) Ethernet1/0/17(A) Ethernet1/0/18(A) Ethernet1/0/19(A) Ethernet1/0/20(A) Ethernet1/0/21(A) Ethernet1/0/22(A) Ethernet1/0/23(A) Ethernet1/0/24(A) Ethernet1/0/25(A) Ethernet1/0/26(A) Ethernet1/0/27(A) Ethernet1/0/28(A)

switchport subnet-vlan enable

Command	switchport subnet-vlan enable no switchport subnet-vlan enable
Parameter	none
Default	The IP-subnet-based VLAN is enabled on the port by default.
Mode	Port Mode.
Usage	After adding the IP subnet to specified VLAN, the IP-subnet-based VLAN function will

be globally enabled. This command can disable the IP-subnet-based VLAN function on specified port to meet special user applications.

show subnet-vlan interface display setting.

Example

Disable the IP-subnet-based VLAN function on port2.

Switch#config

Switch(config)# interface ethernet 1/0/2

Switch(config-if-ethernet1/0/2)#no switchport subnet-vlan enable

Switch(config-if-ethernet1/0/2)#show subnet-vlan interface

Ports

```

-----
Ethernet1/0/1(A)    Ethernet1/0/3(A)
Ethernet1/0/4(A)    Ethernet1/0/5(A)
Ethernet1/0/6(A)    Ethernet1/0/7(A)
Ethernet1/0/8(A)    Ethernet1/0/9(A)
Ethernet1/0/10(A)   Ethernet1/0/11(A)
Ethernet1/0/12(A)   Ethernet1/0/13(A)
Ethernet1/0/14(A)   Ethernet1/0/15(A)
Ethernet1/0/16(A)   Ethernet1/0/17(A)
Ethernet1/0/18(A)   Ethernet1/0/19(A)
Ethernet1/0/20(A)   Ethernet1/0/21(A)
Ethernet1/0/22(A)   Ethernet1/0/23(A)
Ethernet1/0/24(A)   Ethernet1/0/25(A)
Ethernet1/0/26(A)   Ethernet1/0/27(A)
Ethernet1/0/28(A)

```

show voice-vlan

Command

show voice-vlan

Parameter

None

Default

None

Mode

Admin Mode and other Configuration Mode.

Usage

Display Voice VLAN Configuration.

Example

Display the Current Voice VLAN Configuration.

Switch#show subnet-vlan

IP-Address	Mask	VLAN_ID	Priority
-----	-----	-----	-----
192.168.5.2	255.255.255.0	100	0

switchport voice-vlan enable

Command	switchport voice-vlan enable no switchport voice-vlan enable
Parameter	none
Default	Voice VLAN is enabled by default.
Mode	Port Mode.
Usage	When voice equipment is added to the Voice VLAN, the Voice VLAN is enabled globally by default. This command disables Voice VLAN on specified port to meet specified application of the user. show voice-vlan display setting.
Example	Disable the Voice VLAN function on port2. <pre>Switch#config Switch(config)# interface ethernet 1/0/2 Switch(config-if-ethernet1/0/2)# no switchport voice-vlan enable Switch(config-if-ethernet1/0/2)# show voice-vlan Voice VLAN ID:100 Ports ----- Ethernet1/0/1(A) Ethernet1/0/3(A) Ethernet1/0/4(A) Ethernet1/0/5(A) Ethernet1/0/6(A) Ethernet1/0/7(A) Ethernet1/0/8(A) Ethernet1/0/9(A) Ethernet1/0/10(A) Ethernet1/0/11(A) Ethernet1/0/12(A) Ethernet1/0/13(A) Ethernet1/0/14(A) Ethernet1/0/15(A) Ethernet1/0/16(A) Ethernet1/0/17(A) Ethernet1/0/18(A) Ethernet1/0/19(A) Ethernet1/0/20(A) Ethernet1/0/21(A) Ethernet1/0/22(A) Ethernet1/0/23(A) Ethernet1/0/24(A) Ethernet1/0/25(A) Ethernet1/0/26(A) Ethernet1/0/27(A) Ethernet1/0/28(A) Voice name Mac-Address Mask Priority ----- </pre>

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}
Parameter	<mac-address> Mac-address is the voice equipment MAC address, shown

	in "xx-xx-xx-xx-xx-xx" format;		
<mac-mask>	mac-mask is the last eight digit of the mask code of the MAC address, the valid values are: 0xff, 0xfe, 0xfc, 0xf8, 0xf0, 0xe0, 0xc0,0x80, 0x0;		
<priority-id>	priority-id is the priority of the voice traffic, the valid range is 0–7;		
<voice-name>	the voice-name is the name of the voice equipment, which is to facilitate the equipment management;		
This command will add a specified voice equipment into the Voice VLAN, if a non VLAN labeled data packet from the specified voice equipment enters through the switch port, then no matter through which port the packet enters, it will belongs to Voice VLAN. The command will not interfere with the packets of VLAN labels.			
Global Mode.			
This command will add a specified voice equipment into the Voice VLAN, if a non VLAN labeled data packet from the specified voice equipment enters through the switch port, then no matter through which port the packet enters, it will belongs to Voice VLAN. The command will not interfere with the packets of VLAN labels.			
show voice-vlan display setting.			
Add the 256 sets of voice equipments of the R&D department with MAC address ranging from 00-03-0f-11-22-00 to 00-03-0f-11-22-ff to the Voice VLAN.			
Switch#config			
Switch(config)#vlan 100			
Switch(config-vlan100)#exit			
Switch(config)#voice-vlan vlan 100			
Switch(config)#voice-vlan mac 00-03-0f-11-22-00 mask 0 priority 5 name R&D			
Switch(config)#show voice-vlan			
Voice VLAN ID:100			
Ports			

Ethernet1/0/1(A)	Ethernet1/0/3(A)		
Ethernet1/0/4(A)	Ethernet1/0/5(A)		
Ethernet1/0/6(A)	Ethernet1/0/7(A)		
Ethernet1/0/8(A)	Ethernet1/0/9(A)		
Ethernet1/0/10(A)	Ethernet1/0/11(A)		
Ethernet1/0/12(A)	Ethernet1/0/13(A)		
Ethernet1/0/14(A)	Ethernet1/0/15(A)		
Ethernet1/0/16(A)	Ethernet1/0/17(A)		
Ethernet1/0/18(A)	Ethernet1/0/19(A)		
Ethernet1/0/20(A)	Ethernet1/0/21(A)		
Ethernet1/0/22(A)	Ethernet1/0/23(A)		
Ethernet1/0/24(A)	Ethernet1/0/25(A)		
Ethernet1/0/26(A)	Ethernet1/0/27(A)		
Ethernet1/0/28(A)			
Voice name	Mac-Address	Mask	Priority
-----	-----	-----	-----
R&D	00-03-0f-11-22-00	00-00-00-00-00-00	5

voice-vlan vlan

Command	voice-vlan vlan <vlan-id> no voice-vlan			
Parameter	<vlan-id>	Vlan id is the number of the specified VLAN.		
Default	No Voice VLAN is configured by default.			
Mode	Global Mode.			
Usage	Set specified VLAN for Voice VLAN, There can be only one Voice VLAN at the same time. The voice VLAN can not be applied concurrently with MAC-based VLAN. show voice-vlan display setting.			
Example	Set VLAN100 to Voice VLAN. Switch#config Switch(config)#vlan 100 Switch(config-vlan100)#exit Switch(config)#voice-vlan vlan 100 Switch(config)#show voice-vlan Voice VLAN ID:100 Ports ----- Ethernet1/0/1(A) Ethernet1/0/3(A) Ethernet1/0/4(A) Ethernet1/0/5(A) Ethernet1/0/6(A) Ethernet1/0/7(A) Ethernet1/0/8(A) Ethernet1/0/9(A) Ethernet1/0/10(A) Ethernet1/0/11(A) Ethernet1/0/12(A) Ethernet1/0/13(A) Ethernet1/0/14(A) Ethernet1/0/15(A) Ethernet1/0/16(A) Ethernet1/0/17(A) Ethernet1/0/18(A) Ethernet1/0/19(A) Ethernet1/0/20(A) Ethernet1/0/21(A) Ethernet1/0/22(A) Ethernet1/0/23(A) Ethernet1/0/24(A) Ethernet1/0/25(A) Ethernet1/0/26(A) Ethernet1/0/27(A) Ethernet1/0/28(A) Voice name Mac-Address Mask Priority ----- ----- ----- -----			

05-Commands for Anti-ring Protocol

1 Commands for MSTP

abort

Command	abort
parameter	-
default	-
Mode	MSTP Region Mode

Usage Guide This command is to quit MSTP region mode without saving the current configuration. The previous MSTP region configuration is valid.

Example Quit MSTP region mode without saving the current configuration.
Switch(Config-Mstp-Region)#abort
Switch(config)#

exit

Command	exit
parameter	-
default	-
Mode	MSTP Region Mode

Usage Guide This command is to quit MSTP region mode with saving the current configuration.

Example Quit MSTP region mode with saving the current configuration.
Switch(Config-Mstp-Region)#exit
Switch(config)#

instance vlan

Command **instance** <instance-id> **vlan** <vlan-list>
no instance <instance-id> [**vlan** <vlan-list>]

parameter	<i>instance-id</i>	sets the instance number. The valid range is from 0 to 64
	<i>vlan-list</i>	sets consecutive or non-consecutive VLAN numbers. “-” refers to consecutive numbers, and “,” refers to non-consecutive numbers

default	Before creating any Instances, there is only the instance 0, and VLAN 1~4094 all belong to the instance 0.
Mode	MSTP Region Mode
Usage Guide	This command sets the mappings between VLANs and instances. Only if all the mapping relationships and other attributes are same, the switches are considered in the same MSTP region. Before setting any instances, all the VLANs belong to the instance 0. MSTP can support maximum 64 MSTIs (except for CISTs). CIST can be treated as MSTI 0. All the other instances are considered as instance 1 to 64.
Example	Map VLAN1-10 and VLAN 100-110 to Instance 1. Switch(config)#spanning-tree mst configuration Switch(Config-Mstp-Region)#instance 1 vlan 1-10;100-110

Name

Command	name <name> no name
parameter	name is the MSTP region name. The length of the name should be less than 32 characters
default	Default MSTP region name is the MAC address of this bridge.
Mode	MSTP Region Mode
Usage Guide	This command is to set MSTP region name. The bridges with same MSTP region name and same other attributes are considered in the same MSTP region.
Example	Set MSTP region name to mstp-test. Switch(config)#spanning-tree mst configuration Switch(Config-Mstp-Region)#name mstp-test

revision-level

Command	revision-level <level> no revision-level

parameter	<i>level</i> is revision level. The valid range is from 0 to 65535
default	The default revision level is 0.
Mode	MSTP Region Mode
Usage Guide	This command is to set revision level for MSTP configuration. The bridges with same MSTP revision level and same other attributes are considered in the same MSTP region.
Example	Set revision level to 2000. Switch(config)#spanning-tree mst configuration Switch(Config-Mstp-Region)# revision-level 2000

spanning-tree

Command	spanning-tree no spanning-tree
parameter	-
default	MSTP is not enable by d default.
Mode	Global Mode and Port Mode
Usage Guide	If the MSTP is enabled in global mode, the MSTP is enabled in all the ports except for the ports which are set to disable the MSTP explicitly
Example	Enable the MSTP in global mode, and disable the MSTP in the interface1/0/2. Switch(config)#spanning-tree Switch(config)#interface ethernet 1/0/2 Switch(Config-If-Ethernet1/0/2)#no spanning-tree

spanning-tree tc-guard

Command	spanning-tree tc-guard no spanning-tree tc-guard

parameter	
default	tc-guard is not enable by default.
Mode	Port Mode
Usage Guide	This command suppresses frequent TC (Topology Change) packets received on the port to prevent excessive MAC address table flushing and CPU overload. Run the no form to disable this function.
Example	Enable the tc-guard in the interface1/0/2 <pre>Switch(config)#interface ethernet 1/0/2 Switch(Config-If-Ethernet1/0/2)# spanning-tree tc-guard</pre>

spanning-tree bpdu

Command	spanning-tree bpdu vlan <vlan-id> no spanning-tree bpdu vlan
parameter	<vlan-id> Vlan id<1-4094>
default	bpdu is not enable by default.
Mode	Port Mode
Usage Guide	This command filters BPDUs of the specified VLAN on the port to avoid STP topology interference. Use no < b0> < / b0> to cancel the filter.
Example	Enable the bpdu in the interface1/0/2 ,the vlan is 10. <pre>Switch(config)#interface ethernet 1/0/2 Switch(Config-If-Ethernet1/0/2)# spanning-tree bpdu vlan 10</pre>

spanning-tree cost

Command	spanning-tree cost <cost> no spanning-tree cost
parameter	<i>cost</i> sets path cost. The valid range is from 1 to 200,000,000.
default	By default, the port cost is relevant to the port bandwidth.

For the aggregation ports, the default costs are as below:	Default Path Cost	Suggested Range
10Mbps	2000000	2000000-20000000
100Mbps	200000	200000-2000000
1GMbps	20000	20000-200000

For the aggregation ports, the default costs are as below:

Port Type	Allowed Number Of Aggregation Ports	Default Port Cost
10Mbps	N	2000000/N
100Mbps	N	200000/N
1GMbps	N	20000/N

Mode

Port Mode

Usage Guide

By setting the port cost, users can control the cost from the current port to the root bridge in order to control the elections of port and the designated port of the instance.

Example

On the port1/0/2, set the port cost is 3000000.
Switch(Config-If-Ethernet1/0/2)#spanning-tree cost 3000000

spanning-tree digest-snooping

Command

spanning-tree digest-snooping
no spanning-tree digest-snooping

Parameter

-

default

Don't use the authentication string of partner port.

Mode

Port Mode

Usage Guide

According to MSTP protocol, the region authentication string is generated by MD5 algorithm with public authentication key, instance ID, VLAN ID. Some manufactory don't use the public authentication key, this causes the incompatibility. After the command is executed the port can use the authentication string of partner port, realize compatibility with these manufactories equipment.

Because the authentication string is related to instance ID and VLAN ID, the command may cause recognizing the equipment that with different instance and VLAN relation as in the same region. Before the command is executed, make sure that instance and VLAN relation is accord for all the equipment. If there are more than one equipment connected, all the connected ports should execute this command.

Example

```
Configure the authentication string of partner port.  
Switch(config)#interface ethernet 1/0/2  
Switch(Config-If-Ethernet1/0/2)#spanning-tree digest-snooping  
Switch(Config-If-Ethernet1/0/2)#
```

spanning-tree format

Command **spanning-tree format {standard | privacy | auto}**
no spanning-tree format

parameter	standard	The packet format provided by IEEE
	privacy	Privacy packet format, which is compatible with CISCO equipments.
	auto	Auto identified packet format, which is determined by checking the format of the received packets.

default Auto Packet Format.

Mode Port Mode

Usage Guide

As the CISCO has adopted the packet format different with the one provided by IEEE, while many companies also adopted the CISCO format to be CISCO compatible, we have to provide support to both formats. The standard format is originally the one provided by IEEE, and the privacy packet format is CISCO compatible. In case we are not sure about which the packet format is on partner, the AUTO configuration will be preferred so to identify the format by the packets they sent. The AUTO packet format is set by default in the concern of better compatibility with previous products and the leading companies. The packet format will be privacy format before receiving the partner packet when configured to AUTO.

When the format is not AUTO and the received packet format from the partner does not match the configured format, we set the state of the port which receives the unmatched packet to DISCARDING to prevent both sides consider themselves the root which leads to circuits.

When the AUTO format is set, and over one equipment which is not compatible with each other are connected on the port (e.g. a equipment running through a HUB or Transparent Transmission BPDU is connected with several equipments running MSTP), the format alter counts will be recorded and the port will be disabled at certain count threshold. The port can only be re-enabled by the administrator.

Example

Configure port message format as the message format of IEEE.
Switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)#spanning-tree format standard
Switch(Config-If-Ethernet1/0/2)#

spanning-tree forward-time

Command	spanning-tree forward-time <time> no spanning-tree forward-time	
parameter	time	is forward delay time in seconds. The valid range is from 4 to 30
default	The forward delay time is 15 seconds by default	
Mode	Global Mode	
Usage Guide	When the network topology changes, the status of the port is changed from blocking to forwarding. This delay is called the forward delay. The forward delay is co working with hello time and max age. The parameters should meet the following conditions. Otherwise, the MSTP may work incorrectly. $2 * (\text{Bridge\_Forward\_Delay} - 1.0 \text{ seconds}) \geq \text{Bridge\_Max\_Age}$ $\text{Bridge\_Max\_Age} \geq 2 * (\text{Bridge\_Hello\_Time} + 1.0 \text{ seconds})$	

Example

In global mode, set MSTP forward delay time to 20 seconds.
Switch(config)#spanning-tree forward-time 20

spanning-tree hello-time

Command	spanning-tree hello-time <time> no spanning-tree hello-time	
parameter	time	is Hello time in seconds. The valid range is from 1 to 10
default	Hello Time is 2 seconds by default	
Mode	Global Mode	

Usage Guide

This command is used to set the interval bpd switch sending, command "no spanning-tree hello-time" restore default configuration. Hello time is the interval that the switch sends BPDUs. Hello time is co working with forward delay and max age. The parameters should meet the following conditions. Otherwise, the MSTP may work incorrectly.

$$2 * (\text{Bridge\_Forward\_Delay} - 1.0 \text{ seconds}) \geq \text{Bridge\_Max\_Age}$$
$$\text{Bridge\_Max\_Age} \geq 2 * (\text{Bridge\_Hello\_Time} + 1.0 \text{ seconds})$$

Example

Set MSTP hello time to 5 seconds in global mode.

```
Switch(config)#spanning-tree hello-time 5
```

spanning-tree link-type p2p

Command

spanning-tree link-type p2p {auto | force-true | force-false}

no spanning-tree link-type

parameter

auto	sets auto-negotiation
force-true	forces the link as point-to-point type
force-false	forces the link as non point-to-point type.

default

The link type is auto by default; The MSTP detects the link type automatically.

Mode

Port Mode

Usage Guide

For configuring port link types, command "no spanning-tree link-type" restore default configuration. When the port is full-duplex, MSTP sets the port link type as point-to-point;

When the port is half-duplex, MSTP sets the port link type as shared.

Example

Force the port 1/0/7-8 as point-to-point type.

```
Switch(config)#interface ethernet 1/0/7-8
```

```
Switch(Config-Port-Range)#spanning-tree link-type p2p force-true
```

spanning-tree maxage

Command

spanning-tree maxage <time>

no spanning-tree maxage

parameter

time	is max aging time in seconds. The valid range is from 6 to 40.

default

The max age is 20 seconds by default.

Mode	Global Mode
Usage Guide	this command is used to configure bpdu maximum aging time, command "no spanning-tree maxage" restore default configuration. The lifetime of BPDU is called max age time. The max age is co working with hello time and forward delay. The parameters should meet the following conditions. Otherwise, the MSTP may work incorrectly. $2 * (\text{Bridge\_Forward\_Delay} - 1.0 \text{ seconds}) \geq \text{Bridge\_Max\_Age}$ $\text{Bridge\_Max\_Age} \geq 2 * (\text{Bridge\_Hello\_Time} + 1.0 \text{ seconds})$
Example	In global mode, set max age time to 25 seconds. <pre>Switch(config)#spanning-tree maxage 25</pre>

spanning-tree max-hop

Command	spanning-tree max-hop <hop-count> no spanning-tree max-hop	
parameter	hop-count	sets maximum hops. The valid range is from 1 to 40
default	The max hop is 20 by default.	
Mode	Global Mode	
Usage Guide	This command is used to set BPDU maximum number of hops, and the command "no spanning-tree max-hop" is used to restore the default configuration. The MSTP uses max-age to count BPDU lifetime. In addition, MSTP also uses max-hop to count BPDU lifetime. The max-hop is degressive in the network. The BPDU has the max value when it initiates from MSTI root bridge. Once the BPDU is received, the value of the max-hop is reduced by 1. When a port receives the BPDU with max-hop as 0, it drops this BPDU and sets itself as designated port to send the BPDU.	
Example	Set max hop to 32. <pre>Switch(config)#spanning-tree max-hop 32</pre>	

spanning-tree mcheck

Command	spanning-tree mcheck
parameter	-
default	The port is in the MSTP mode by default

Mode Port Mode

Usage Guide

If a network which is attached to the current port is running IEEE 802.1D STP, the port converts itself to run in STP mode. The command is used to force the port to run in the MSTP mode. But once the port receives STP messages, it changes to work in the STP mode again.

This command can only be used when the switch is running in IEEE802.1s MSTP mode. If the switch is running in IEEE802.1D STP mode, this command is invalid.

Example

Force the port 1/0/2 to run in the MSTP mode.
Switch(Config-If-Ethernet1/0/2)#spanning-tree mcheck

spanning-tree mode

Command **spanning-tree mode {mstp | stp | rstp}**
no spanning-tree mode

parameter	mstp	sets the switch in IEEE802.1s MSTP mode
	stp	sets the switch in IEEE802.1D STP mode
	rstp	sets the switch in IEEE802.1w RSTP mode

default The switch is in the MSTP mode by default

Mode Global Mode

Usage Guide

This command is used to configure the spanning tree mode and the command "**no spanning-tree mode**" is used to restore the default mode. When the switch is in IEEE802.1D STP mode, it only sends standard IEEE802.1D BPDU and TCN BPDU. It drops any MSTP BPDUs.

Example

Set the switch in the STP mode.
Switch(config)#spanning-tree mode stp

spanning-tree mst configuration

Command **spanning-tree mst configuration**
no spanning-tree mst configuration

parameter -
default -

Mode Global Mode

Usage Guide Whether the switch is in the MSTP region mode or not, users can enter the MSTP mode, configure the attributes, and save the configuration. When the switch is running in the MSTP mode, the system will generate the MST configuration identifier according to the MSTP configuration. Only if the switches with the same MST configuration identifier are considered as in the same MSTP region.

Example Enter MSTP region mode.
Switch(config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#

panning-tree mst cost

Command **spanning-tree mst <instance-id> cost <cost>**
no spanning-tree mst <instance-id> cost

parameter	<i>instance-id</i>	sets the instance ID. The valid range is 0-64
	<i>cost</i>	sets path cost, different cost formats have different ranges. For the default dot1t mode the valid range is 1-200,000,000, and for dot1d is 1-65535.

default By default, the port cost is relevant to the port bandwidth.

Port Type	Default Path Cost	Suggested Range
10Mbps	2000000	2000000-20000000
100Mbps	200000	200000-2000000
1GMbps	20000	20000-200000

For the aggregation ports, the default costs are as below:

Port Type	Allowed Number Of Aggregation Ports	Default Port Cost
10Mbps	N	2000000/N
100Mbps	N	200000/N

1GMbps	N	20000/N	
Port Speed	Port Type	Port Cost	
		802.1D-2008	802.1T
0		65535	200000000
10Mbps	Half- duplex	100	2,000,000
	Full- duplex	99	1,999,999
	aggregation	95	1,000,000
	link with	95	666,666
	2 ports	95	500,000
	aggregation		
	link with		
	3 ports		
	aggregation		
	link with		
	4 ports		
100Mbps	Half- duplex	19	200,000
	Full- duplex	18	199,999
	aggregation	15	100,000
	link with	15	66,666
	2 ports	15	50,000
	aggregation		
	link with		
	3 ports		
	aggregation		
	link with		
	4 ports		
1000Mbps	Full- duplex	4	20,000
	aggregation	3	10,000
	link with	3	6,666
	2 ports	3	5,000
	aggregation		
	link with		
	3 ports		
	aggregation		
	link with		
	4 ports		

Mode

Port Mode

Usage Guide

By setting the port cost, users can control the cost from the current port to the root bridge in order to control the elections of root port and the designated port of the instance.

Example

On the port1/0/2, set the MSTP port cost in the instance 2 to 3000000.
Switch(Config-If-Ethernet1/0/2)#spanning-tree mst 2 cost 3000000

spanning-tree cost-format

Command	spanning-tree cost-format {dot1d dot1t}
	-
default	count path-cost with dot1t format.
Mode	Global mode.
Usage Guide	There are two formats about cost value: they are dot1d marked on IEEE802.1d-2008 and dot1t marked on IEEE802.1t, but path-cost ranges of them are different, dot1d range from 1 to 65535, and dot1t range from 1 to 200,000,000.

Example

Set the cost format in global mode.
Switch(config)#spanning-tree cost-format dot1d

spanning-tree mst loopguard

Command	spanning-tree [mst <instance-id>] loopguard no spanning-tree [mst <instance-id>] loopguard	
parameter	instance-id	MSTP instance ID <0-64>.
default	Disable loopguard function	
Mode	Port Mode	
Usage Guide	The command can avoid root port or alternate port to be changed as designated port due to invalid unilateralism link. When the receiving timer is time, the configured port with loopguard is set as block state.	

Example

Configure port 1/0/2 as loopguard mode 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)#

spanning-tree mst port-priority

Command **spanning-tree mst <instance-id> port-priority <port-priority>**
no spanning-tree mst <instance-id> port-priority

parameter	<i>instance-id</i>	sets the instance ID. The valid range is from 0 to 64
	<i>port-priority</i>	sets port priority. The valid range is from 0 to 240. The value should be the multiples of 16, such as 0, 16, 32...240.

default The default port priority is 128

Mode Port Mode

Usage Guide By setting the port priority, users can control the port ID of the instance in order to control the root port and designated port of the instance. The lower the value of the port priority is, the higher the priority is.

Example Set the port priority as 32 on the port 1/0/2 for the instance 1.
Switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)#spanning-tree mst 1 port-priority 32

spanning-tree mst priority

Command **spanning-tree mst <instance-id> priority <bridge-priority>**
no spanning-tree mst <instance-id> priority

parameter	<i>instance-id</i>	sets instance ID. The valid range is from 0 to 64;
	<i>port-priority</i>	sets the switch priority. The valid range is from 0 to 61440. The value should be the multiples of 4096, such as 0, 4096, 8192...61440

default The default bridge priority is 32768

Mode Global Mode

Usage Guide By setting the bridge priority, users can change the bridge ID for the specified instance. And the bridge ID can influence the elections of root bridge and designated port for the specified instance.

Example

Set the priority for Instance 2 to 4096.
Switch(config)#spanning-tree mst 2 priority 4096

spanning-tree mst rootguard

Command **spanning-tree [mst <instance-id>] rootguard**
no spanning-tree [mst <instance-id>] rootguard

parameter	instance-id	MSTP instance ID, Instance value <0-64>

default Disable rootguard function

Mode Port Mode

Usage Guide The command is used in Port Mode, if the port is configured to be a rootguard port, it is forbidden to be a MSTP root port. If superior BPDU packet is received from a rootguard port, MSTP did not recalculate spanning-tree, and just set the status of the port to be root_inconsistent (blocked). If no superior BPDU packet is received from a blocked rootguard port, the port status will restore to be forwarding. The rootguard function can maintain a relative stable spanning-tree topology when a new switch is added to the network.

Example

Enable rootguard function for port 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)#

spanning-tree portfast

Command **spanning-tree portfast [bpduguard | bpdufilter] [recovery <30-3600>]**
no spanning-tree portfast

parameter	bpdufilter	configure the border port mode as BPDU filter
	bpduguard	configure the border port mode as BPDU guard
	recovery	configure the border port can be recovered automatically after implement bpduguard violation operation
	<30-3600>	the recovery time, do not recover it by default

default All the ports are non-boundary ports by default when enabling MSTP

Mode Port Mode

Usage Guide

Set the current port as boundary port, and BPDU filter. BPDU guard as specified mode or default mode; the command “no spanning-tree portfast” sets the current port as non-boundary port.

When a port is set to be a boundary port, the port converts its status from discarding to forwarding without bearing forward delay. Once the boundary port receives the BPDU, the port becomes a non-boundary port.

Example

Configure the border port mode as BPDU guard, the recovery time as 60s.

```
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)#
```

spanning-tree port-priority

Command	spanning-tree port-priority <port-priority> no spanning-tree port-priority

parameter	port-priority	sets port priority. The valid range is from 0 to 240. The value should be the multiples of 16, such as 0, 16, 32, 48...240

default	The default port priority is 128

Mode	Port Mode

Usage Guide	By setting the port priority to designated port. The lower the value of the port priority is, the higher the priority is.

Example

Set the port priority as 20 on the port 1.

```
Switch(Config-If-Ethernet1/0/1)#spanning-tree port-priority 20
```

spanning-tree priority

Command	spanning-tree priority <bridge-priority> no spanning-tree priority

parameter	bridge-priority	is the priority of the bridging switch. Its value should be round times of 4096 between 0 and 61440, such as 0, 4096, 8192... 61440.

default	Default priority is 32768
Mode	Global Mode
Usage Guide	The bridge ID can be altered by changing the priority of the switch. Further, the priority information can also be used for voting of the root bridge and the specified ports. The bridge priority value of the switch is smaller, however the priority is higher.
Example	Configure the priority is 4096. Switch(config)#spanning-tree priority 4096

spanning-tree rootguard

Command	spanning-tree rootguard no spanning-tree rootguard
parameter default	- Port is non-root port
Mode	Port Mode
Usage Guide	The command is used in Port Mode, if the port is configured to be a rootguard port, it is forbidden to be a MSTP root port. If superior BPDU packet is received from a rootguard port, MSTP did not recalculate spanning-tree, and just set the status of the port to be root_inconsistent (blocked). If no superior BPDU packet is received from a blocked rootguard port, the port status will restore to be forwarding. The rootguard function can maintain a relative stable spanning-tree topology when a new switch is added to the network.
Example	Set the port 1 is root port. Switch(Config-If-Ethernet1/0/1)#spanning-tree rootguard

spanning-tree tcflush (Global mode)

Command	spanning-tree tcflush {enable disable protect} no spanning-tree tcflush

parameter	enable	<i>The spanning-tree flush once the topology changes.</i>
	disable	<i>The spanning tree don't flush when the topology changes.</i>
	protect	<i>the spanning-tree flush not more than one time every ten seconds.</i>
default	<i>Enable</i>	
Mode	<i>Global mode</i>	
Usage Guide	Configure the spanning-tree flush mode once the topology changes. “no spanning-tree tcflush” restores to default setting. According to MSTP, when topology changes, the port that send change message clears MAC/ARP table (FLUSH). In fact it is not needed for some network environment to do FLUSH with every topology change. At the same time, as a method to avoid network assault, we allow the network administrator to configure FLUSH mode by the command.	
Example	Configure the spanning-tree flush mode once the topology changes is not flush to TC. <pre>Switch(config)#spanning-tree tcflush disable Switch(config)#</pre>	

spanning-tree tcflush (Port mode)

Command	spanning-tree tcflush {enable disable protect} no spanning-tree tcflush	
parameter	enable	The spanning-tree flush once the topology changes
	disable	The spanning tree don't flush when the topology changes
	protect	the spanning-tree flush not more than one time every ten seconds
default	Default enable mode	

Mode	Port Mode
Usage Guide	Configure the spanning-tree flush mode for port once the topology changes. “no spanning-tree tcfush” restores to default setting. According to MSTP, when topology changes, the port that send change message clears MAC/ARP table (FLUSH). In fact it is not needed for some network environment to do FLUSH with every topology change. At the same time, as a method to avoid network assault, we allow the network administrator to configure FLUSH mode by the command.
Example	Configure the spanning-tree flush mode once the topology change is not flush to TC. Switch(config)#spanning-tree tcfush disable

spanning-tree transmit-hold-count

Command	spanning-tree transmit-hold-count <tx-hold-count-value> no spanning-tree transmit-hold-count	
parameter	<i>tx-hold-count-value</i>	ranging from 1 to 255, the default value is 10
default	10	
Mode	Global Mode	
Usage Guide	Set the max number for sending BPDU within the Hello Time interval to control BPDU flow. The variable is used to whole MST bridge.	
Example	Set the max transmit-hold-count as 20. Switch(config)#spanning-tree transmit-hold-count 20	

show mst-pending

Command	show mst-pending	
parameter	-	
default	-	
Mode	Admin Mode	
Usage Guide	In the MSTP region mode, display the configuration of the current MSTP region such as MSTP name, revision, VLAN and instance mapping.	

Example

```
Display the configuration of the current MSTP region.
Switch(config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#show mst-pending
Name switch
Revision 0
Instance Vlans Mapped
-----
00 1-29, 31-39, 41-4093
03 30
04 40
05 4094
-----
Switch(Config-Mstp-Region)#
```

show spanning-tree

Command `show spanning-tree [mst [<instance-id>]] [interface <interface-list>] [detail]`

parameter

<i>instance-id</i>	sets interface list
<i>interface-list</i>	sets the instance ID. The valid range is from 0 to 64
detail	sets the detailed spanning-tree information

default

-

Mode

Admin and Configuration Mode

Usage Guide

This command can display the MSTP information of the instances in the current bridge.

Example

```
Display the bridge MSTP.
Switch#sh spanning-tree
***** Process 0
*****

-- MSTP Bridge Config Info --

Standard      : IEEE 802.1s
Bridge MAC    : 00:1f:ce:10:b0:1b
Bridge Times  : Max Age 20, Hello Time 2, Forward Delay 15
Force Version: 3

##### Instance 0 #####
Self Bridge Id : 32768.00:1f:ce:10:b0:1b
Root Id        : this switch
Ext.RootPathCost : 0
Region Root Id : this switch
Int.RootPathCost : 0
```

Root Port ID : 0
 Current port list in Instance 0:
 Ethernet1/0/12 Ethernet1/0/20 (Total 2)

PortName	ID	ExtRPC	IntRPC	State	Role	DsgBridge
DsgPort						
Ethernet1/0/12	128.012	0	0 FWD	DSGN	32768.001fce10b01b	128.012
Ethernet1/0/20	128.020	0	0 FWD	DSGN	32768.001fce10b01b	128.020

Display information

describe

MSTP Bridge Config Info

Standard

STP version

Bridge MAC

Bridge MAC address

Bridge Times

Max Age, Hello Time and Forward Delay of the bridge

Force Version

Version of STP

Instance 0

Self Bridge Id

The priority and the MAC address of the current bridge for the current instance

Root Id

The priority and the MAC address of the root bridge for 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 region root of the current instance

Root Port ID

Root port of the current instance on the current bridge

Current port list in Instance 0

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 region root of the current instance

State Role

Port status of current instance

DsgBridge

Upward designated bridge of the current port in the current instance

DsgPort

Upward designated port of the current port in the current instance

show spanning-tree mst config

Command	show spanning-tree mst config

parameter	-

default	-

Mode	Admin Mode

Usage Guide	In the Admin mode, this command can show the parameters of the MSTP configuration such as MSTP name, revision, VLAN and instance mapping.

Example	Display the configuration of the MSTP on the switch. Switch#show spanning-tree mst config

Name	
Revision	0
Instance	Vlans Mapped

00	1-4094

spanning-tree process

Command	spanning-tree process <process-id> no spanning-tree process <process-id>

parameter	process-id the range is 1-31

default	-

Mode	Global Mode

Usage Guide	Create the new mstp process. Multiple mstp processes can be configured on one device and each process is standalone. The process 0 exists only as default.

Example	Create the new mstp process 1. Switch(config)#spanning-tree process 1

spanning-tree tc-notify process0

Command	spanning-tree tc-notify process0

no spanning-tree tc-notify process0

parameter	-
default	-
Mode	mstp process mode

Usage Guide

When there is a change in mstp process N, the device will receive the tc packet, at the same time, the process N will notify tc to the instance in mstp process 0 on the shared link. It makes the process 0 refresh the table entry for ensuring the traffic not to break off.

Example

Configure to notify TC of process 1 to process 0.
Switch(Config-Mstp-Process-1)#spanning-tree tc-notify process0

spanning-tree binding-process

Command

spanning-tree binding-process <process-id>
no spanning-tree binding-process <process-id>

parameter	process-id	the range is 1-31.

default

All the ports belong to process 0

Mode

Port Mode

Usage Guide

Configure the port to join the appointed mstp process N. The port will enter into process N from the process 0. This command is mutually exclusive to the shared port configuration command (link-share).

Example

Add the Ethernet1/0/2 into process 1.
Switch(Config-If-Ethernet1/0/2)#spanning-tree binding-process 1

spanning-tree binding-process link-share

Command

spanning-tree binding-process < process-id > link-share
no spanning-tree binding-process < process-id > link-share

parameter	process-id	the range is 1-31

default

The port is only in the mstp calculating of process 0

Mode Port Mode

Usage Guide Configure the port belong to the shared port of process N. Except for process 0, the configured port can be in the mstp calculating of multiple processes, but the port status can be only configured by process 0. This command can be configured for more than once.

Example Configure the Ethernet1/0/2 as the shared port of process 1 and 0.
Switch(Config-If-Ethernet1/0/2)#spanning-tree binding-process 1 link-share

2 ERPS Configuration

ethernet tcn-propagation erps to {erps | stp}

Command **ethernet tcn-propagation erps to {erps | stp}**
no ethernet tcn-propagation erps to

parameter	erps	topology changing sends the R-APS event packets to notify the connection ring of this device
	stp	topology changing sends the stp packets to notify the stp topology connected to this device

default ERPS ring topology changing only takes effect in this ring but does not send the notification packets

Mode Global Mode

Usage Guide Configure the topology changing transmission notification method supported by this device as the appointed method. The ERPS ring instance detects the changing, it will send the notification packets. If configured erps method, it will send the R-APS event packets to other ERPS rings; if configured stp method, it will send the stp packets outward.

Example Configure to send R-APS event notification to the interconnection ring after the topology changing.
Switch(config)#ethernet tcn-propagation erps to erps
Configure to send STP notification to the interconnection ring after the topology changing.
Switch(config)#ethernet tcn-propagation erps to stp
Delete the topology changing transmission notification method.
Switch(config)#no ethernet tcn-propagation erps to

erps-ring <ring-name>

Command	erps-ring < ring-name > no erps-ring < ring-name >	
parameter	ring-name	the ERPS ring name created. The maximum character number is 64 and it is made up with letters, numbers and the underlines. The first and last character cannot be the underline
default	Do not configure any ERPS ring.	
Mode	Global Mode	
Usage Guide	Create a ERPS ring and enter ERPS ring configuration mode. enter ERPS ring configuration mode if the ERPS ring already exists. no command delete ERPS ring.	
Example	Create the ERPS ring of ring1 Switch(config)#erps-ring 1 Switch(config-erps-ring)# Delete the EPRS ring of ring1 Switch(config)#no erps-ring 1	

version {v1 | v2}

Command	version {v1 v2} no version	
parameter	v1	means to support v1 which is released in 2008-06 and the amendment (2009-04)
	v2	means to support v2 which is released in 2010-03 and the amendment (2010-06)
default Mode	V2 ERPS Ring Configuration Mode	
Usage Guide	This command is used to configure the supporting version of the ERPS loop, no the command is restored to the default state of the v2. If configured ERPS ring to support v1, this ring will not support multi-instance. ERPS ring instance does not support the management commands of MS, FS, etc. and the non-revertive switch is not effective. It only support revertive switch. If configured ERPS ring to support v1, the instance of this ring will deal with the ERPS	

packets according to the v1 format. Package the R-APS packets and resolve the fields according to v1 format. The fields defined by v2 will not be dealt.

Example

```
Configure the ERPS ring of ring1 to support v1
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#version v1
Delete v1 supported by the ERPS ring of ring1
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#no version
```

open-ring

Command

open-ring
no open-ring

parameter default

-
Default Configuration ERPS Subrings

Mode

ERPS Ring Configuration Mode

Usage Guide

If the ERPS ring instance has been configured on the ring, there will be the message of **“Cann't config open-ring on ERPS ring whitch has ERPS instance, please delete ERPS instance firstly!”** Otherwise, enter into the next step. Configure this ERPS ring type as sub ring.

Example

```
Configure the ERPS ring of ring1 as sub ring of open type.
Switch(config)#erps-ring 1
Switch(config-erps-ring)#open-ring
Delete the configuration of the sub ring of open type.
Switch(config)#erps-ring 1
Switch(config-erps-ring)#no open-ring
```

raps-virtual-channel {with | without}

Command

raps-virtual-channel {with | without}

parameter

with	the R-APS virtual channel is existed in this ERPS ring
without	the R-APS virtual channel is not existed in this ERPS ring

default

The R-APS virtual channel is not existed in ERPS ring

Mode	ERPS Ring Configuration Mode
Usage Guide	Configure if there is the R-APS virtual channel in ERPS ring according to the configuration. Inputting: Success or error. If there is not R-APS virtual channel on the ERPS ring, the R-APS channel of all the instances of ERPS ring will be unblocked forever and it only blocks the data channel; otherwise, the R-APS channel and the data channel will be blocked at the same time.
Example	Configure that there is R-APS virtual channel in the ERPS sub ring of ring1. <pre>Switch(config)#erps-ring ring1 Switch(config-erps-ring)#raps-virtual-channel with</pre>

erps-ring <ring-name> port0 [port1-none]

Command	erps-ring <ring-name> port0 [port1] no erps-ring <ring-name> port0	
parameter	ring-name	ERPS ring name, the maximum string is 64, and it is made up with letters, numbers and underlines; the first and last characters cannot be underlines
	port1-none	there is only the port0 on this ERPS ring node, no port1 and it is the interconnection node
default	Do not configure port0 on ERPS ring	
Mode	Port Mode	
Usage Guide	this command is used to configure the port as the port of the specified ERPS ring. If this ERPS ring is not open-ring type, the port1-none cannot be configured. Check if the ERPS ring configuration is integral; if it is integral, check if the ERPS instance configuration is integral; if it is integral, activate the instance as active and run the protocol.	
Example	Configure e 1/0/1 as the port0 of ERPS ring1 <pre>Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#erps-ring ring1 port0</pre> Delete the e 1/0/1 as port0 of ERPS ring1 <pre>Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#no erps-ring ring1 port0</pre>	

erps-ring <ring-name> port1

Command	erps-ring <ring-name> port1 no erps-ring <ring-name> port1	
parameter	ring-name	ERPS ring name, the maximum string is 64, and it is made up with letters, numbers and underlines; the first and last characters cannot be underlines
default	Do not configure port1 on ERPS ring	
Mode	Port Mode	
Usage Guide	This command is used to configure the port as the port of the specified ERPS ring. Check if the ERPS ring configuration is integral; if it is integral, check if the ERPS instances configuration is integral; if it is integral, activate the instance as active and run the protocol.	

Example

```

Configure e 1/0/1 as the port1 of ERPS ring1
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#erps-ring ring1 port1
Delete the e 1/0/1 as the port1 of ERPS ring1
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#no erps-ring ring1 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>

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	
parameter	{port0 port1}	parameter selection. Port0 means the fault detection type of port0. Port1 means the fault detection type of port1
	{cc physical-link-or-cc}	parameter selection. cc means that the ERPS ring port detection is cc report fault. physical-link-or-cc means that the ERPS ring port detection is cc report fault and physical link fault.

<domain-name>	the cfm domain name of ERPS ring port detection <1-43> character
< ma-name >	the service name that cfm belongs to of ERPS ring port detection. string <1-45> character
< ma-num >	Service number value <0-65535>
< vlan-id >	Service primary vlan value <1-4094>
<mep-id>	the local mep id that cfm monitored of ERPS ring port detection, Local mepid configuration <1-4094>
<rmep-id>	the remote mep id that cfm monitored of ERPS ring port detection, Remote mepid configuration <1-4094>

default ERPS ring port only detects the physical link fault as default

Mode ERPS Ring Configuration Mode

Usage Guide Configure the fault detection type of ERPS ring ports. If it is detected as cc type, the maintenance domain, maintenance set that cc belongs to and the monitoring link (it is conditioned with (mep-id, rmep-id)) should be appointed. The premise of this configuration is that the corresponding ring port has been joined into ERPS ring. The no command deletes the fault detection type of ERPS ring ports. Configure the fault detection type of ERPS ring ports as the appointed type. If the type is cc, save the configured md, ma, mep and rmep information to use for matching after receiving the cfm fault notification.

Example Configure the detection type of ERPS ring1 port0as cc.
Switch(config)#erps-ring 1
Switch(config-erps-ring)#port0 failure-defect cc domain domain1 service service1 mep 1
rmep 2
Delete this configuration.
Switch(config)#erps-ring 1
Switch(config-erps-ring)#no port0 failure-defect

erps-instance <instance-id>

Command **erps-instance <instance-id>**
no erps-instance <instance-id>

parameter **instance-id** id of ERPS ring, the range is 1 to 48

default	Do not configure any ERPS ring instance
Mode	ERPS Ring Configuration Mode
Usage Guide	Create the ERPS ring instance and enter into the ERPS ring instance configuration Mode. If the ERPS ring supports v1, there will be the message of “Doesn't support multiple ERPS instance capability on the ring running version 1!” when configured more than one ERPS instance.

Example	Configure the ERPS ring instance 1 on ERPS ring1. Switch(config)#erps-ring 1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)# Delete the ERPS ring instance 1 on ERPS ring1. Switch(config)#erps-ring 1 Switch(config-erps-ring)#no erps-instance 1

description

Command	description <instance-name> no description <instance-name>

parameter	<table> <tr> <td>instance-name</td><td>ERPS instance name, the maximum string is 64, and it is made up with letters, numbers and underlines; the first and last characters cannot be underlines. The no command deletes the ERPS instance name.</td></tr> </table>	instance-name	ERPS instance name, the maximum string is 64, and it is made up with letters, numbers and underlines; the first and last characters cannot be underlines. The no command deletes the ERPS instance name.
instance-name	ERPS instance name, the maximum string is 64, and it is made up with letters, numbers and underlines; the first and last characters cannot be underlines. The no command deletes the ERPS instance name.		

default	Do not configure the ERPS instance name as default

Mode	ERPS Instance Configuration Mode

Usage Guide	Configure the description string for the ERPS instance.

Example	Configure the ERPS instance1 name on ring1 as instance1. Switch(config)#erps-ring ring1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)# description instance1 Delete this name of instance1. Switch(config)#erps-ring ring1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)# no description

ring-id <ring-id>

Command	ring-id <ring-id> no ring-id <ring-id>		
parameter	<table><tr><td>ring-id</td><td>ERPS ring id and the range is 1 to 64</td></tr></table>	ring-id	ERPS ring id and the range is 1 to 64
ring-id	ERPS ring id and the range is 1 to 64		
default	The MAC address is 01-19-A7-00-00-01 as default		
Mode	ERPS Instance Configuration Mode.		
Usage Guide	Configure the last byte of R-APS packets destination MAC address sent by ERPS ring node to carry ring-id. If ERPS ring supports v1, ring-id only can be configured as 1. The no command configures it not to carry the ring-id, it means that the MAC is 01-19-A7-00-00-01.		

Example	Configure the last byte of R-APS packets destination MAC address sent by ERPS ring1 instance2 to carry the ring-id 2. <pre>Switch(config)#erps-ring 1 Switch(config-erps-ring)#erps-instance 2 Switch(config-erps-ring-inst-2)#ring-id 2</pre> Configure the last byte of R-APS packets destination MAC address sent by ERPS ring1 instance2 not to carry the ring-id, it means the destination MAC is 01-19-A7-00-00-01. <pre>Switch(config)#erps-ring 1 Switch(config-erps-ring)#erps-instance 2 Switch(config-erps-ring-inst-2)#no ring-id</pre>

rpl {port0 | port1} {owner | neighbour}

Command	rpl {port0 port1} {owner neighbour} no rpl {port0 port1}				
parameter	<table><tr><td>{port0 port1}</td><td>ERPS ring member ports</td></tr><tr><td>{owner neighbour}</td><td>Owner: RPL owner Neighbour: RPL owner</td></tr></table>	{port0 port1}	ERPS ring member ports	{owner neighbour}	Owner: RPL owner Neighbour: RPL owner
{port0 port1}	ERPS ring member ports				
{owner neighbour}	Owner: RPL owner Neighbour: RPL owner				
default	None, it is the ordinary transmission node type.				
Mode	ERPS Instance Configuration Mode				
Usage Guide	Configure the member port of ERPS ring instance as RPL owner or RPL neighbour, the RPL node roles of different instances on the same ERPS ring cannot be configured on the same member port. The no command configures the member port of ERPS ring instance as				

the ordinary transmission port member.

Example

Configure the port0 of ERPS ring1 instance1 as RPL owner node.
Switch(config)#erps-ring 1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)#rpl port0 owner

non-revertive

Command

non-revertive
no non-revertive

**parameter
default**

-
ERPS ring instance supports the revertive as default

Mode

ERPS Instance Configuration Mode

Usage Guide

Configure the ERPS ring instance as non-revertive. If this ERPS ring supports v1, this command is null and cannot be configured. The no command configures the ERPS ring instance as revertive. If this ERPS ring supports v1, this command is null. This command can be configured only on the RPL owner node of the sub ring.

Example

Configure the ERPS ring1 instance1 to support the non-revertive.
Switch(config)#erps-ring 1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)#non-revertive

guard-timer <guard-times>

Command

guard-timer <guard-times>
no guard-timer

parameter

guard-times	the interval is 10ms and the range is 10ms to 2s

default

500ms

Mode

ERPS Instance Configuration Mode

Usage Guide

Configure the Guard timer. The guard timer is used for the Ethernet node to avoid the error handling and the close loop according to the outdated R-APS packets. In the starting time of the timer, any R-APS packets received (the R-APS packets that the

Request/State="1110" are except) will be dropped. The no command configures the guard timer as the default value.

Example

Configure the guard timer of ERPS ring1 instance1 as 1s.

```
Switch(config)#erps-ring 1
```

```
Switch(config-erps-ring)#erps-instance 1
```

```
Switch(config-erps-ring-inst-1)guard-timer 100
```

holdoff-timer <holdoff-times>

Command

holdoff -timer <holdoff-times>

no holdoff -timer

parameter

holdoff-times

the interval is 1s and the range is 0 to 10s

default

0s

Mode

ERPS Instance Configuration Mode

Usage Guide

This command is used to configure the delay timer, and the default configuration is restored in the form of No

Example

Configure the Holdoff timer of ERPS ring1 instance1 as 5s.

```
Switch(config)#erps-ring ring1
```

```
Switch(config-erps-ring)#erps-instance 1
```

```
Switch(config-erps-ring-inst-1)#holdoff -timer 5
```

wtr-timer <wtr-times>

Command

wtr-timer <wtr-times>

no wtr-timer

parameter

wtr-times

the interval is 1min and the range is from 1 to 12min

default

5min

Mode

ERPS Instance Configuration Mode

Usage Guide

Configure the WTR timer. WTR timer is used to avoid the frequent protection switching of RPL owner node because of the periodic (intermittent) default. When RPL owner port received the default recovery packets, after some time, and then check if the default still existed on the other nodes and prevent blocking RPL owner port immediately to cause the chokepoint shocking. The no command configures the WTR timer as the default.

Example

Configure the WTR timer of ERPS ring1 instance1 as 10min.

```
Switch(config)#erps-ring 1
```

```
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)#wtr-timer 10
```

protected-instance

Command	protected-instance <instance-list> no protected-instance <instance-list>	
parameter	instance-list	the MSTP instance list protected by ERPS ring instance, such as i, j-k. The number of the instances in the list is not limited.
default	ERPS ring instance does not protect any MSTP instance	
Mode	ERPS Instance Configuration Mode	
Usage Guide	Configure the protection instance of ERPS ring instance. ERPS ring instance can protect all the MSTP instances. The same instance cannot be quoted by multiple ERPS ring instances under the same topology. Under the same ERPS ring instance, run this command more than once to protect instance, the result will be accumulated. The no command deletes the protection instance of ERPS ring instance.	

Example	Configure the protection instance of ERPS ring1 instance1 as instance 2. Switch(config)#erps-ring ring1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)#protected-instance 2

raps-mel <level-value>

Command	raps-mel <level-value> no raps-mel	
parameter	level-value	the level value of APS packets, range is from 0 to 7
default	Level is 7	
Mode	ERPS Instance Configuration Mode	
Usage Guide	Configure the level of R-APS channel of ERPS ring instance as the appointed level. If configured successfully, the mel field of the R-APS packet sent by this ERPS ring instance will be added as the appointed level and only the R-APS packets with the level that is	

larger than or same as the appointed level can be allowed passing by, or notify the error. The no command configures the level as the default of 7. The MEL field in the protocol packets is used to detect if the current packet can pass by.

Example

```
Configure the level of R-APS channel of ERPS ring1 instance1 as 5.
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)raps-mel 5
```

control-vlan <vlan-id>

Command

control-vlan <vlan-id>
no control-vlan

parameter

parameter	description
vlan-id	vlan id of R-APS packets, range is from 2 to 4094

default

Do not configure any control vlan

Mode

ERPS Instance Configuration Mode

Usage Guide

Configure the control vlan of R-APS packets of R-APS channel. In the ERPS ring instance, this vlan is only used to transmit ERPS protocol packets but not to forward the user business packets. It improves the ERPS protocol security. User makes sure the configuration uniqueness. This vlan is as the vlan tag when sending R-APS packets. The protection VLAN configuration of all the nodes in the instance must be identical. The no command deletes the control vlan.

Example

```
Configure the control vlan of ERPS ring1 instance1 as vlan10.
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)control-vlan 10
```

forced-switch {port0 | port1}

Command

forced-switch {port0 | port1}

parameter

parameter	description
port0	means to run the forced switch configuration on port0 of the ring node

	<table> <tr> <td>port1</td><td>means to run the forced switch configuration on port1 of the ring node</td></tr> </table>	port1	means to run the forced switch configuration on port1 of the ring node
port1	means to run the forced switch configuration on port1 of the ring node		
default	No forced switch in ERPS ring instance		
Mode	ERPS Instance Configuration Mode		
Usage Guide	Run the forced switch on the port of ERPS ring node. Two or more forced switch are allowed existing at the same time in one ERPS ring instance. But only one forced switch command can be existed on one ring node. User should avoid using multiple forced switch in ERPS ring instance to cause the ERPS ring instance splitting. If the forced switch is on the current highest priority, block the data channel and R-APS channel of this ERPS ring instance on the appointed member port (port0 or port1), and unblock the other member port of this ring node; If this instance configuration is not integral, it is on the status of unactive, there will be the message of “The request is rejected because the ERP instance in unactive state!” otherwise, enter into the next step;		

Example

Run the forced switch configuration on the port0 of ERPS ring1 instance1.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)#force-switch port0
```

manual-switch {port0 | port1}

Command **manual-switch {port0 | port1}**

parameter	port0	means to run the manual switch configuration on port0 of the ring node
	port1	means to run the manual switch configuration on port1 of the ring node

default No manual switch in ERPS ring instance

Mode ERPS Instance Configuration Mode

Usage Guide

Run the manual switch on the port of ERPS ring node. Only one manual switch is allowed existing in one ERPS ring instance, and the premise is that there is no SF fault or FS command in ERPS ring instance.

If this instance configuration is not integral, it is on the status of unactive, there will be the

message of “The request is rejected because the ERP instance in unactive state!” otherwise,
enter into the next step;

Example

Run the manual switch configuration on the port0 of ERPS ring1 instance1.
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)#manual-switch port0

clear command

Command

clear command

parameter

-

default

No clear command in ERPS ring instance.

Mode

ERPS Instance Configuration Mode

Usage Guide

Run the clear command to the member port of ERPS ring node, it can clear the management command of the local activity: forced switch command and manual switch command; it can be also used to trigger the link switch under the revertive mode before WTR or WTB is time out; and trigger the link to switch from the standby link RPL back to the intrinsic link under the non-revertive mode after the fault recovery.

If the forced or manual switch command has existed on the node of this ring instance, clear

the switch command and keep the block status of the data channel and R-APS channel of the

blocked member ports. And send the P-APS (NR) packets on the two member ports stably and steadily until received R-APS (NR, RB) packets and known the RPL is blocked. Or the

higher level request happens on the ring (such as SF);

If the local forced or manual switch has existed on the node of this ring instance, clear the

command and then receive the R-APS (NR) packets whose node ID is larger than the local

node ID. Unblock all the ring ports without SF fault and stop sending the R-APS (NR) packets on the two member ports.

Example

Run clear configuration on ERPS ring1 instance1.
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)#clear command

show erps ring {<ring-name> | brief}

Command	show erps ring {<ring-name> brief}																																							
parameter	ring-name		ERPS ring name																																					
	brief		Show the ERPS ring main information																																					
default	-																																							
Mode	Admin Mode																																							
Usage Guide	Read the ERPS ring information.																																							
Example	show all the ERPS rings information. Switch#show erps ring brief ethernet tcn-propagation erps to none. Ring-Name <table><thead><tr><th>Ring-topo</th><th>Port0</th><th>Port1</th><th>Version</th><th>Inst-Coun</th></tr></thead><tbody><tr><td>t</td><td></td><td></td><td></td><td></td></tr><tr><td colspan="5">-----</td></tr><tr><td colspan="5">-----</td></tr><tr><td colspan="5">--</td></tr><tr><td>ring1</td><td></td><td></td><td></td><td>major-</td></tr><tr><td>ring</td><td>-</td><td>-</td><td>V2</td><td>0</td></tr></tbody></table>					Ring-topo	Port0	Port1	Version	Inst-Coun	t					-----					-----					--					ring1				major-	ring	-	-	V2	0
Ring-topo	Port0	Port1	Version	Inst-Coun																																				
t																																								

--																																								
ring1				major-																																				
ring	-	-	V2	0																																				

show erps instance [ring <ring-name> [instance <instance-id>]]

Command	show erps instance [ring <ring-name> [instance <instance-id>]]	
parameter	ring-name	ERPS ring name
	instance-id	ID of ERPS ring instance, range is from 1 to 48. If it is not appointed, show all the ERPS ring instances information.
default	-	
Mode	Admin Mode	
Usage Guide	Show the ERPS ring instance information.	
Example	Show all the ERPS ring instances information. Switch#show erps instance ERPS Ring: 1 Instance: 1 Description: - Protected Instance: - Revertive mode: revertive R-APS MEL: 7	

R-APS Virtual-Channel: with
Control Vlan: -
Ring ID: 1
Guard Timer(10ms): 50
Holdoff Timer(seconds): 0
WTR Timer(min): 5

Port	Role	Port-Status
Port0	common	blocked
Port1	common	blocked

Display content	analyze
Description	ERPS ring instance name
Protected Instance	MSTP instance protected by ERPS ring instance
Revertive mode	ERPS ring link mode: revertive, non-revertive
R-APS MEL	Level of R-APS channel, package R-APS packets
R-APS Virtual-Channel	If the ERPS ring is the sub ring, the R-APS virtual channel of the inherited ring: with, without
Ring ID	The ring-id number carried by the packets sent by ERPS ring instance, range is from 1 to 64.
Contral Vlan	R-APS channel vlan, package R-APS packet of tag
WTR_Timer	Wait to Restore timer, range is from 1 to 12min
Guard_Timer	Guard timer, range is from 10ms to 2s
Holdoff_Timer	Holdoff timer, range is from 0 to 10
Port	ERPS ring port information: port0, port1
Role	ERPS ring node roles: RPL Owner, RPL neighbor, Common
Port-Status	Blocked: port is in block status forwarding: port is in forwarding status

show erps status [ring <ring-name> [instance <instance-id>]]

Command **show erps status [ring <ring-name> [instance <instance-id>]]**

parameter	ring-name	ERPS ring name
	instance-id	ID of ERPS ring instance, range is from 1 to 48. If it is not

appointed, show all the ERPS ring instances status information.

default
Mode Admin Mode

Usage Guide Show the status information of ERPS ring instance.

Example Show all the ERPS ring instances status information.

Switch#show erps status

ERPS ring: 1 instance: 1 status:

Active: 0

Node State: -

Time last topology change:Jan 00 00:00:00 1900

Port	Interface	Port-Status	Signal-Status	R-APS-NodeId
BPR				

Port0	-	-	-	-
-				
Port1	-	-	-	-
-				

ERPS ring: 1 instance: 2 status:

Active: 0

Node State: -

Time last topology change:Jan 00 00:00:00 1900

Port	Interface	Port-Status	Signal-Status	R-APS-NodeId
BPR				

Port0	-	-	-	-
-				
Port1	-	-	-	-
-				

Display content	analyze
Active	Current active status of ERPS ring instance: 1, 0
Node State	Current status of ERPS ring instance: Idle, Protection, Forced-switch, Manual-switch, Pending
Time last topology change	Topology switching last time
Port-Status	Blocked: the port is in block status Forwarding: the port is in forwarding status
Signal-Status	ERPS ring port fault status: Non-failed: no fault

R-APS-NodeId	Failed: fault happened The node ID information is the last bit of the MAC address
BPR	The block link information carried by the receiving last R-APS saved by ERPS ring port, it is port0 or port1 which was blocked.

show erps statistics [ring <ring-name> [instance <instance-id>]]

Command `show erps statistics [ring <ring-name> [instance <instance-id>]]`

parameter	ring-name	ERPS ring name
	instance-id	ID of ERPS ring instance, range is from 1 to 48. If it is not appointed, show the statistic information of all the ERPS ring instances of this device.

default -
Mode Admin Mode

Usage Guide Show the statistic information of ERPS ring instance.

Example Show the statistic information of ERPS ring instance.

Switch#show erps statistics

Statistics for ERPS ring: 1 instance 1:

R-APS	Port0(Tx/Rx)		Port1(Tx/Rx)	

NR:	0	/0	0	/0
NR,RB:	0	/0	0	/0
SF:	0	/0	0	/0
MS:	0	/0	0	/0
FS:	0	/0	0	/0
EVENT:	0	/0	0	/0

TOTAL:	0	/0	0	/0

Statistics for ERPS ring: 1 instance 2:

R-APS	Port0(Tx/Rx)		Port1(Tx/Rx)	

NR:	0	/0	0	/0
NR,RB:	0	/0	0	/0
SF:	0	/0	0	/0
MS:	0	/0	0	/0
FS:	0	/0	0	/0
EVENT:	0	/0	0	/0

TOTAL: 0 /0 0 /0

clear erps statistics [ring <ring-name> [instance <instance-id>]]

Command clear erps statistics [ring <ring-name> [instance <instance-id>]]

parameter	ring-name	ERPS ring name
	instance-id	ID of ERPS ring instance, range is from 1 to 48. If it is not appointed, clear the statistic information of all the ERPS ring instances of this device

default -

Mode Admin Mode

Usage Guide Clear the statistic information of ERPS.

Example Clear the statistic information of ERPS ring1 instance1.
Switch#clear erps statistics ring 1 instance 1

06-Commands for QOS

1 QOS

accounting

Command	Accounting no accounting
Parameter	none
Default	The statistical function has not been set up.
Mode	Strategy Mapping Configuration Mode
Usage	Enable the function of classifying and statistically analyzing traffic. After enabling this function, add the statistical function to the traffic of the policy class mapping. When the message passes through the policy, it can only be red or green. When printing statistical information, classify the packet numbers in the data packets, but color classification is not supported.
Example	Count the packets that meet the c1 rule。 Switch#config Switch(config)#class-map c1 Switch(config-classmap-c1)#exit 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 Switch(config)#

access-group redirect to interface ethernet

Command	access-group <aclname> redirect to interface [ethernet] <IFNAME> no access-group <aclname> redirect
Parameter	<aclname> Process name: Only supports standard IP ACL with numbers, extended IP ACL with numbers, named standard IP ACL, named extended IP ACL, standard MAC ACL with numbers, extended MAC ACL with numbers, named standard MAC ACL, named extended MAC, standard IPv6 ACL, and named standard IPv6 ACL. Parameter for Timerange and Portrange cannot be set in the ACL. The type of the ACL should be "Allow".
Default	<IFNAME> The target port for redirection. None
Mode	Port Configuration Mode

Usage	Specify flow-based redirection; "no access-group <aclname> redirect" Command is used to delete flow-based redirection. "no access-group <aclname> redirect" Command is used to delete flow-based redirection. Flow-based redirection functionality enables the switch to transfer data frames that meet certain specific conditions to another designated port. Note: Redirection does not support redirection to a port-based flow.
Example	Redirect the frame with the source IP of 192.168.1.111 that was received by 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

apply tail-drop-profile

Command	apply tail-drop-profile <profile0-profile15>
Parameter	<profile0-profile15> Tail discard file ID range 0-15
Default	Bind the tail-drop file 0 under the default port.
Mode	Port Configuration Mode
Usage	Used to bind the tail discard configuration template to the interface
Example	Bind the tail-throwing template 1 to port 1. Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# apply tail-drop-profile 1

class

Command	class <class-map-name> [insert-before <class-map-name>] no class <class-map-name>
Parameter	<class-map-name> The class mapping name used in this category. Class-map name<1-64>character. insert-before <class-map-name> Insert the newly configured class before the existing classes to enhance the priority of the new class.。
Default	No strategy configuration exists.
Mode	Strategy Mapping Configuration Mode
Usage	Map the classes and strategies, then enter the Strategy Class Mapping Mode; noCommand deletes the specified class. Before setting the strategy class, create the strategy mapping and enter the Strategy

Mapping Mode. In the Strategy Mapping Mode, data packet traffic classified by class mapping can be classified and next-hop configuration can be performed.

Example	After adding the strategy class mapping c1 to the strategy mapping, add the strategy class mapping c2 and insert it before c1. <pre>Switch(config)#class-map c1 Switch(config)#exit Switch(config)#class-map c2 Switch(config)#exit 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</pre>

class-map

Command	class-map <class-map-name> no class-map <class-map-name>
Parameter	<class-map-name> Class-map name<1-64>character
Default	No class mapping configuration
Mode	Privilege Configuration Mode
Usage	Create a class mapping and enter the class mapping mode; "no" Command is used to delete the specified class mapping.
Example	Create and delete a class mapping with the name "c1" <pre>Switch#config Switch(config)#class-map c1 Switch(config-classmap-c1)#exit Switch(config)#no class-map c1</pre>

clear mls qos statistics

Command	clear mls qos statistics {(interface [ethernet] <interface-name>) (vlan <vlan-id>) in [(interface [ethernet] <interface-name>) (vlan <vlan-id>)] out [(interface [ethernet] <interface-name>) (vlan <vlan-id>)]}								
Parameter	<table> <tr> <td><vlan-id></td><td>VLAN ID<1-4094></td></tr> <tr> <td><interface-name></td><td>Port name</td></tr> <tr> <td>in</td><td>The inbound direction of the port</td></tr> <tr> <td>out</td><td>The outbound direction of the port</td></tr> </table>	<vlan-id>	VLAN ID<1-4094>	<interface-name>	Port name	in	The inbound direction of the port	out	The outbound direction of the port
<vlan-id>	VLAN ID<1-4094>								
<interface-name>	Port name								
in	The inbound direction of the port								
out	The outbound direction of the port								
Default	None								

Mode	Privileged Mode
Usage	Clear the billing data of the specified port or VLAN policy mapping。
Example	Clear the policy mapping statistics information of VLAN 10 Switch#clear mls qos statistics vlan 100

drop

Command	drop no drop
Parameter	none
Default	None
Mode	Strategy-based mapping configuration Mode
Usage	After configuring this Command, the specified data packets will be discarded.
Example	Discard the data packets that meet the criterion c1. Switch#config Switch(config)#policy-map p1 Switch(config-policy-map-p1)#class c1 Switch(config-policy-map-p1-class-c1)#drop Switch(config-policy-map-p1-class-c1)#exit Switch(config-policy-map-p1)#exit

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> exp <exp-list> } no match {access-group ip dscp ip precedence ipv6 access-group ipv6 dscp ipv6 flowlabel vlan cos exp }}	
Parameter	access-group <acl-index-or-name>	Match the specified IP ACL or MAC – IP ACL or standard IPv6 ACL, Parameter is the number or name of the ACL
	ip dscp <dscp-list>	Match the specified DSCP value. This parameter is a DSCP list, which can contain a maximum of 8 DSCP values and ranges from 0 to 63.
	ip precedence <ip-precedence-list>	Match the specified IP priority. This Parameter is an IP priority list, which consists of a maximum of 8 IP priority values. The valid range is from 0 to 7.
	ipv6 access-group <acl-index-or-name>	Match the specified IPv6 ACL. Parameter is the number or name of the IPv6 ACL.

	ipv6 dscp <dscp-list>	Match the specified DSCP value. This parameter is a DSCP list, which can contain a maximum of 8 DSCP values and ranges from 0 to 63.
	ipv6 flowlabel <flowlabel-list>	Match the specified IPv6 flow label. The Parameter represents the value of the IPv6 flow label, and its range is from 0 to 1048575.
	vlan <vlan-list>	Match the specified VLAN ID corresponding to the external VLAN Tag. This parameter is a list of VLAN IDs, with a maximum of 8 VLAN IDs, ranging from 1 to 4094.
	cos <cos-list>	Match the specified CoS value. Parameter is a list of CoS values, with a maximum of 8 values, ranging from 0 to 7.
	exp	Match MPLS Exp (0-7)
Default	By default, there is no matching standard.	
Mode	Class Mapping Mode	
Usage	Define the matching criteria for the configuration class mapping; noCommand deletes the specified matching criteria. Only one matching criterion can be configured in the class mapping. When configuring ACL matching, the allow rule is the match option, which will apply the policy mapping operation. The deny rule is the exclude option, which does not apply the policy mapping operation. If other matching rules have been configured, the operation fails, but configuring the same matching rules will override the previous rules.	
Example	Create a class mapping named "c1" and configure the class rules for this class mapping to match data packets with an IP priority of 0. <pre>Switch(config)#class-map c1 Switch(config-classmap-c1)#match ip precedence 0 Switch(config-classmap-c1)#exit</pre>	

mls qos aggregate-policy

Command	mls qos aggregate-policy WORD <1-100000000 > <0-34000> (pir <1-100000000> <0-34000>) (color-blind color-aware) {conform-action [(drop set-cos-transmit <0-7> set-drop-precedence <0-2> set-dscp-transmit <0-63> set-exp <0-7> set-internal-priority <0-7> set-prec-transmit <0-7> transmit)] exceed-action [(drop set-cos-transmit <0-7> set-drop-precedence <0-2> set-dscp-transmit <0-63> set-exp <0-7> set-internal-priority <0-7> set-prec-transmit <0-7> transmit)] violate-action [(drop set-cos-transmit <0-7> set-drop-precedence <0-2> set-dscp-transmit <0-63> set-exp <0-7> set-internal-priority <0-7> set-prec-transmit <0-7> transmit)]} no mls qos aggregate-policy WORD	
Parameter	WORD	Aggregation strategy name, length ranging from 1 to 64

	<1-100000000 >	The promised information rate, denoted as CIR, is measured in kbit/s and ranges from 1 to 1,0000,0000.
	<0-34000>	Commitment for sudden size, namely CBS, normal peak kilobytes <0 - 34000>
	pir <1-100000000>	Peak information rate, 1000 bits per second < 1 - 1,0000,0000
	<0-34000>	Peak burst size, maximum peak kilobytes < 0 - 34000 >
	color-blind color-aware	Set the Color Mode to Color Blind Mode Set the Color Mode to Color Sensitive Mode
	conform-action	When the data rate does not exceed the CIR limit and the message is green, the corresponding strategy is adopted.
	exceed-action	When the rate exceeds the CIR but is less than the PIR, and the message is displayed in yellow, the corresponding strategy is adopted.
	violate-action	The strategy adopted when the PIR rate is exceeded and the message is displayed in red
	(drop set-cos-transmit set-dscp-transmit set-exp set-prec-transmit set-drop-precedence set-internal-prioriity transmit)	(Discard the message Modify the L2 COS value of the message Modify the dscp Set the Mpls Exp value Modify the TOS Modify the priority of message discard Through the message)
Default	Default to no strategy operation	
Mode	Privilege Configuration Mode	
Usage	Define an aggregation strategy named "Command". The "noCommand" deletion mode configuration is removed. Apply uniform rate limiting and three-color marking actions to a group of traffic (such as the total traffic after multiple ports/flows are combined) to achieve batch traffic control.	
Example	Define an aggregation policy named AGG_POLICY CIR=10000 kbit/s, CBS=512 KB PIR=20000 kbit/s, EBS=1024 KB Color Perception Mode: color-aware Action: Green traffic is directly forwarded, yellow traffic is re-tagged as DSCP 0, and red traffic is directly discarded. Switch (config)# mls qos aggregate-policy AGG_POLICY 10000 512 pir 20000 1024 color-aware conform-action transmit exceed-action set-dscp-transmit 0 violate-action drop	

mls qos cos

Command	mls qos cos <cos0-cos7> no mls qos cos	
Parameter	<cos0-cos7>	The default CoS value of the port ranges from 0 to 7.
Default	CoS is 0	
Mode	Port Configuration Mode	
Usage	Set the default CoS value for the port; "no mls qos cos" Command will restore the default settings. Configure the default CoS value for the switch port. In Default, the message entry CoS for this port is the default value, regardless of whether the message has a label. If the message does not have a label, then the CoS value for the message with a label is specified.	
Example	Set the default CoS value of Ethernet port 1/0/1 to 7. That is, if there is no CoS value, the data packets entering through this port will be assigned the default CoS value of 7. <pre>Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#mls qos cos 7</pre>	

mls qos map

Command	mls qos map (cos-intp <intp1...intp8> cos-dp <dp1...dp8> cos-exp <0-7> to <0-7> dscp-intp <in-dscp list> to <intp> dscp-dp <in-dscp list> to <dp> dscp-dscp <in-dscp list> to <out-dscp> dscp-exp , 0-63> to <0-7> exp-exp <0-7> to <0-7> exp-intp <intp1...intp8> exp-dp<dp1...dp8>) no mls qos map (cos-intp cos-dp dscp-intp dscp-dp dscp-dscp exp-intp exp-dp)	
Parameter	cos-intp <intp1...intp8>	Define the mapping from CoS to intp (queue) values. <intp1...intp8> represents 8 intp values, corresponding to 0 to 7 CoS values. Each intp value is separated by a space and the range is from 0 to 7.
	cos-dp<dp1...dp8>	Define the mapping from cos to intp (queue), <dp1...dp8> represents 8 discard priorities, corresponding to the Cos values (from 0 to 7), each discard priority is separated by a space, and the range is from 0 to 2.
	cos-exp <0-7> to <0-7>	Define the mapping from 802.1p CoS values (0 to 7) to MPLS EXP values (0 to 7), which is used to convert the Layer 2 CoS marking into the Experimental bit of the MPLS label.
	dscp-intp <0-63>	Define the mapping from DSCP to intp (queue).
	dscp-dp <0-63>	Define the mapping from DSCP to discard priority.

dscp-dscp <0-63>	Define the mapping from the input dscp to the output dscp. <in-dscp list> is the input dscp value, with a maximum of 8 and separated by spaces among each other, ranging from 0 to 63. The output <out-dscp> is the dscp value, ranging from 0 to 63.
dscp-exp <0-63> to <0-7>	Define the mapping from DSCP values (0 to 63) to MPLS EXP values (0 to 7), which is used to convert the DSCP marking in the IP header into the Experimental bit of the MPLS label.
exp-exp <0-7> to <0-7>	Define the mapping from the ingress MPLS EXP value (0-7) to the egress MPLS EXP value (0-7), which is used to rewrite or retain the EXP tag in the MPLS network.
exp-intp <intp1...intp8>	Define the mapping from MPLS EXP value (0-7) to queue number (intp, 0-7). There are 8 values, <intp1...intp8>, corresponding to EXP 0-7 respectively. Each value is separated by a space. The range is 0-7, determining which forwarding queue the traffic with different EXP markings enters.
exp-dp <dp1...dp8>	Define the mapping from MPLS EXP values (0-7) to discard priorities (DP, 0-2). There are 8 values, <dp1...dp8>, corresponding to EXP 0-7 respectively. Each value is separated by a space and ranges from 0 to 2. These determine the discard priorities for traffic with different EXP markings.

Default

Default mapping value:

Default CoS-TO-INTP mapping

COS: 0 1 2 3 4 5 6 7

INTP: 0 1 2 3 4 5 6 7

Default CoS-TO-DP mapping

CoS value 0 1 2 3 4 5 6 7

DP value 0 0 0 0 0 0 0 0

Default DSCP-TO-INTP mapping

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

Default DSCP-TO-DP mapping

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						
	Default DSCP-TO-DSCP mapping										
	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						
Mode	Privilege Configuration Mode										
Usage	INTP represents the internal priority setting of the chip. Since the internal DSCP value is only 64, while the chip's internal priority (queue) is only 8, the dscp-intp mapping requires 8 consecutive internal dscp mappings to the same INTP. Tag → Queue (INTP): cos-intp, dscp-intp, exp-intp, determines which hardware queue the traffic enters and affects the scheduling priority. Tag → Drop Priority (DP): cos-dp, dscp-dp, exp-dp, determines the packet loss probability of the traffic during congestion, with dp0 having the least packet loss and dp2 having the most. Tag → Tag: cos-exp, dscp-dscp, dscp-exp, exp-exp, used for converting QoS tags between different network layers (layer 2 / IP/MPLS), ensuring end-to-end QoS consistency.										
Example	Set the mapping values from CoS to INTP to the default values of 0, 8, 16, 24, 32, 40, 48, 56 to 0, 1, 2, 3, 4, 5, 6, 7. Switch(config)#mls qos map cos-intp 0 1 2 3 4 5 6 7										

mls qos queue depth

Command	mls qos queue depth <64-34492>	
	no mls qos queue depth	
Parameter	depth <64-34492>	Set the queue depth, range <64 - 34492>
Default	None	
Mode	Privilege Configuration Mode	
Usage	This Command is used to configure the depth of the interface queue (i.e., the number of data packets or bytes that the queue can hold), by controlling the queue length to balance latency and packet loss rate.	
Example	Set the queue depth to 200. Switch(config)#mls qos queue depth 200	

mls qos queue apply scheduling-profile

Command	mls qos queue apply scheduling-profile <profile1-profile14> no mls qos queue apply scheduling-profile	
Parameter	< profile1-	Select the scheduling file ID. Range: 1 - 14
	profile14>	
Default	Port Default is bound to queue 0.	
Mode	Port Configuration Mode	
Usage	This is used to bind the predefined scheduling policy file to the specified physical port, enabling fine-grained management of queue scheduling policies at the port level. However, the Default binding scheduling file for the port is 0, so the binding starts from file 1.	
Example	Bind the scheduling file 1 to the port. Switch(interface-ethernet1/0/1)# mls qos queue apply scheduling-profile 1	

mls qos queue cir

Command	mls qos queue <queue0-queue7> cir <100-12800000> (cbs <100-4092>) no mls qos queue <queue0-queue7> cir	
Parameter	queue<queue0-	Queue ID range: 0 - 7
	queue7>	
	cir <100-	Commitment rate magnitude: must be a multiple of 100
	12800000>	
	cbs <100-4092>	Commitment to various emergencies and crises: must be a multiple of 4
Default	no assignment	
Mode	Port Configuration Mode	
Usage	It is used to configure the committed information rate (CIR) and committed burst size (CBS) for the specified queue, precisely controlling the outbound traffic bandwidth of a single queue.	
Example	Interface Queue 7, stable speed limit 100000 kbps, burst value 2048 Bytes. Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# mls qos queue 7 cir 100000 cbs 2048	

mls qos trust

Command	mls qos trust (cos dscp exp) no mls qos trust (cos dscp exp)	
Parameter	dscp	Configure the port to trust the DSCP state.
	cos	Configure the port to trust the COS state
	exp	Configure the port to trust the EXP state
Default	Default trust cos	
Mode	Port Configuration Mode	
Usage	Configure current port trust, the “no” command disables the current trust status of the port. Trust dscp mode: Set the intp field based on dscp to intp mapping. Trust cos mode: Set the cos to intp mapping based on the intp field. Trust exp mode: Directly use the EXP (Experimental) field in the packet as the QoS priority basis to achieve end-to-end MPLS network QoS mapping. The trust cos mode is already enabled by default, so it won't be displayed when c onfigured. However, if you cancel the trust for cos, it will be displayed.	
Example	Set port 1/0/1 to trust DSCP and distrust COS.。 <pre>Switch(config)#interface ethernet 1/0/1 Switch(config-if-ehternet1/0/1) # mls qos trust dscp Switch(config-if-ehternet1/0/1)#no mls qos trust cos</pre>	

mls qos egress conform-action

Command	mls qos egress conform-action (drop set-cos-transmit <0-7> set-dscp-transmit <0-63> set-exp <0-7> set-prec-transmit <0-7> transmit) exceed-action(drop set-cos-transmit <0-7> set-dscp-transmit <0-63> set-exp <0-7> set-prec-transmit <0-7> transmit) violate-action(drop set-cos-transmit <0-7> set-dscp-transmit <0-63> set-exp <0-7> set-prec-transmit <0-7> transmit) no mls qos egress	
Parameter	conform-action	When the data rate does not exceed the CIR limit and the message is green, the corresponding strategy is adopted.
	exceed-action	When the rate exceeds the CIR but is less than the PIR, and the message is displayed in yellow, the corresponding strategy is adopted.
	violate-action	The strategy adopted when the PIR rate is exceeded and the message is displayed in red
	(drop set-cos-transmit<0-7> set-dscp-transmit<0-	(Discard packets Process packets Modify DSCP Modify TOS Modify L2 COS value of packets Set MPLS Exp value)

	63> set-exp><0-7> set-prec-transmit<0-7> transmit) no assignment
Default	
Mode	Global Configuration Mode
Usage	Based on CIR (committed information rate) and PIR (peak information rate), the traffic is classified into three colors: green/yellow/red, and different QoS actions are performed respectively to achieve refined bandwidth control and priority adjustment. The noCommand can delete all outbound traffic regulation configurations and restore to the default state.
Example	Green traffic conform-action ($\leq$ CIR): Direct forwarding Yellow traffic exceed-action (CIR < Traffic $\leq$ PIR): Re-label as DSCP 0 and then forward Red traffic violate-action (> PIR): Directly discard. Switch(config)# mls qos egress conform-action transmit exceed-action set-dscp-transmit 0 violate-action drop

Policy

Command	policy <1-100000000> <0-34000> (pir <1-100000000> <0-34000>) color-blind color-aware conform-action(drop set-cos-transmit set-dscp-transmit set-exp set-prec-transmit set-drop-precedence set-internal-priority transmit) no policy	
Parameter	<1-100000000>	Commitment Information Rate - CIR (Commitment Information Rate), measured in Kbps, ranges from 1 to 1,000,000.
	<0-34000>	Commitment for sudden size, namely CBS, normal peak kilobytes <0 - 34000>
	pir <1-100000000>	Peak information rate, 1000 bits per second <1-100000000
	<0-34000>	Peak burst size, maximum peak kilobytes < 0 - 34000 >
	color-blind color-aware	Set the Color Mode to Color Blind Mode Set the Color Mode to Color Sensitive Mode
	conform-action	When the data rate does not exceed the CIR limit and the message is green, the corresponding strategy is adopted.
	exceed-action	When the rate exceeds the CIR but is less than the PIR, and the message is displayed in yellow, the

	corresponding strategy is adopted.
violate-action	The strategy adopted when the PIR rate is exceeded and the message is displayed in red
(drop set-cos-transmit set-dscp-transmit set-exp set-prec-transmit set-drop-precedence set-internal-prioriity transmit)	(Discard the message Modify the L2 COS value of the message Modify the dscp Set the Mpls Exp value Modify the TOS Modify the priority of message discard Through the message)
Default	No strategic operation。
Mode	Strategy-based mapping configuration Mode
Usage	Based on the committed information rate (CIR), peak information rate (PIR), and corresponding burst size (CBS, PBS), the traffic is classified into green/yellow/red three colors and different QoS actions are executed respectively to achieve refined bandwidth control and priority adjustment. It supports two coloring modes: color blindness and color sensitivity, and can flexibly adapt to the scenarios where traffic colors are inherited. This command needs to be configured in the flow classification configuration mode of the policy mapping. The "no" command can delete the traffic regulation configuration under the current flow classification and restore the default no-policy operation state.
Example	Guaranteed bandwidth: 1000 kbps; Guaranteed burst size: 1000 bytes; Excessive burst size: 1000 bytes. Use color-sensitive mode. Forward green messages, forward yellow messages, discard red messages. <pre>Switch(config)#policy-map 1 Switch(config-policy-map-1)#class cm Switch(config-policy-map-1-class-cm)# policy 1000 1000 1000 color-aware conform-action transmit exceed-action transmit violate-action drop</pre>

Policy aggregate

Command	policy aggregate <aggregate-policy-name> no policy aggregate <aggregate-policy-name>
Parameter	<aggregate-policy-name> Strategy Name
Default	No strategic operation
Mode	Strategy-based mapping configuration Mode
Usage	The strategy mapping refers to the aggregation strategy and applies the aggregation strategy to the classified traffic. The "no" command deletes the specified aggregation strategy. The same strategy set can be referenced by different strategy classes in the mapping.

Example	First, create a shared aggregated traffic regulation template globally. Then, reference this template in the flow classification of the policy mapping. In the current flow classification, reference the aggregated regulation template with number 1. Incorporate this type of traffic into the unified bandwidth control of the aggregated template. <pre>Switch(config)# mls qos aggregate-policy 1 1000 1000 1000 color-blind Switch(config)#policy-map 1 Switch(config-policymap-1)#class cm Switch(config-policymap-1-class-cm)#policy aggregate 1</pre>

Policy-map

Command	policy-map <policy-map-name> no policy-map <policy-map-name>
Parameter	<policy-map-name> Strategy mapping name;
Default	No strategy mapping。
Mode	Global Configuration Mode
Usage	Create a policy map and enter the policy map mode; "no policy-map <policy-map-name>" Command deletes the specified policy mapping. Policy class mapping operations can be completed in the Strategy Mapping Configuration Mode.
Example	Create and delete the policy mapping named "p1". <pre>Switch(config)#policy-map p1 Switch(config-policymap-p1)#exit Switch(config)#no policy-map p1</pre>

priority-flow-control [queue <0-7>] enable [receive|send]

Command	priority-flow-control [queue <0-7>] enable [receive send] no priority-flow-control [queue <0-7>] [enable]
Parameter	priority-flow-control Priority-based traffic control queue <0-7> Configure queue parameters 0-7 enable Turn on all directions receive Receiving direction send Sending direction
Default	Default off
Mode	Port Mode
Usage	The enable function for configuring the PFC feature.

Example

Enable the PFC function of Queue 3.

Switch(config-if-ethernet1/0/1)# priority-flow-control queue 3 enable

priority-flow-control queue <0-7> static-threshold <0-196608> dynamic-threshold <0-11>

Command

priority-flow-control queue <0-7> static-threshold <0-196608> dynamic-threshold <0-11>

Parameter

no priority-flow-control [queue <0-7>] [static-threshold] dynamic-threshold]

priority-flow-control	Priority-based traffic control
queue <0-7>	Configure queue parameters 0-7
static-threshold <0-196608>	PFC static trigger threshold, 1 cache unit 128 bytes
dynamic-threshold <0-11>	priority

Default

The default setting for static-threshold is 256, and the default setting for dynamic-threshold is 1.

Mode

Port Mode

Usage

Used for configuring the trigger threshold of the PFC.

Example

Set the PFC static threshold of Queue 3 to 4096 and the dynamic threshold to 0.

Switch(config-if-ethernet1/0/1)#priority-flow-control queue 3 static-threshold 4096 dynamic-threshold 0

scheduling-profile

Command

scheduling-profile PROFILE_ID <0-14> { bytes | packets | <cr>}
no scheduling-profile <1-14> | all

Parameter

PROFILE_ID <0-14> Scheduling file ID range

Default

Default has a scheduling file 0.

Mode

Privilege Configuration Mode

Usage

Create queue scheduling file, the command "no scheduling-profile <1-14>" deletes the specified scheduling file. The default file cannot be deleted. "no scheduling-profile all" deletes all the scheduling files, except for the default file 0.
The "bytes" and "packets" parameters can only be configured on Aldrin2 devices.

Example

Create the scheduling-profile 5.
Switch(config)#scheduling-profile 5

service-policy input

Command	service-policy input <policy-map-name> no service-policy input {<policy-map-name>}	
Parameter	input <policy-map-name>	Apply the specified strategy mapping to the inbound direction of the switch port. If no specific Strategy mapping name is specified, noCommand will remove all the strategy mappings applied to the inbound direction of the port.
Default	By default, no strategy mapping is bound to the port..	
Mode	Port Configuration Mode	
Usage	Apply the strategy mapping to the specified port; noCommand removes the specified strategy mapping applied to this port or deletes all the inbound direction strategy mappings applied to this port.	
Example	Bind the policy "p1" to the input port 1/0/1 Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#service-policy input p1	

service-policy input vlan

Command	service-policy input <policy-map-name> vlan <vlan-list> no service-policy input {<policy-map-name>} vlan <vlan-list>	
Parameter	input <policy-map-name>	Apply the specified strategy mapping to the inbound direction of the switch VLAN ports.
	vlan <vlan-list>	The list of VLANs for the binding strategy mapping.
Default	By default, no strategy mapping is bound to the VLAN port..	
Mode	Privilege Configuration Mode	
Usage	Apply the strategy mapping to the specified VLAN interface; noCommand deletes the specified strategy diagram applied to the VLAN interface, or deletes all the strategy diagrams applied in the inbound direction of the VLAN interface.	
Example	Bind the policy "p1" to the ingress VLAN ports 2-4 and 6. Switch(config)#service-policy input p1 vlan 2-4;6	

service-policy output

Command	service-policy output <policy-map-name> no service-policy output {<policy-map-name>}	
Parameter	output <policy-map-name>	Apply the specified strategy mapping to the outbound direction of the switch port. If no specific Strategy mapping name is specified, noCommand will remove all the strategy mappings applied to the port's outbound direction.
Default	By default, no strategy mapping is bound to the port.。	
Mode	Port Configuration Mode	
Usage	Apply the strategy mapping to the specified port; noCommand removes the specified strategy mapping applied to this port or deletes all the export-directional strategy mappings applied to this port.	
Example	Bind the policy "p1" to the outbound port 1/0/1。 Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#service-policy output p1	

service-policy output vlan

Command	service-policy output <policy-map-name> vlan <vlan-list> no service-policy output {<policy-map-name>} vlan <vlan-list>	
Parameter	input <policy-map-name>	Apply the specified strategy mapping to the outbound direction of the switch VLAN ports.
	vlan <vlan-list>	The list of VLANs for the binding strategy mapping.
Default	By default, no strategy mapping is bound to the VLAN port.	
Mode	Privilege Configuration Mode	
Usage	Apply the strategy mapping to the specified VLAN interface; noCommand deletes the specified strategy diagram applied to the VLAN interface, or deletes all the strategy diagrams applied in the outbound direction of the VLAN interface.	
Example	Bind the policy “p1” to the ingress VLAN ports 2-4 and 6.。 Switch(config)#service-policy output p1 vlan 2-4;6	

set

Command	set {s-vid <new-vid> cos <cos-list> drop-precedence <dp-list> internal-priority <inp-list> ip {dscp <dscp-list> precedence <pri-list> default nexthop (A.B.C.D) vrf<0-252> (A.B.C.D)} s-tpid <tpid-list> nexthop tunnel<1-200> exp ipv6{ default nexthop X:X::X:X vrf <0-252> X:X::X:X }} no set{s-vid cos drop-precedence internal-priority ip {dscp precedence nexthop} s-tpid exp nexthop tunnel ipv6{nexthop}}	
Parameter	<new-vid>	Modify the tunnel VID of the VLAN Tag
	<cos-list>	Modify the cos value of the message
	<dp-list>	Modify and discard priority
	<inp-list>	Modify internal priority
	<dscp-list> <pri-list>	Modify the value or priority of ip dscp
	default	Set to the bottom PBR (valid in the incoming direction)
	nexthop(A.B.C.D)	Set the next hop address
	Vrf<0-4092>	The Vrf value is used to specify the VRF (Virtual Routing and Forwarding) to which the next hop belongs.
	exp	Set the Mpls Exp value
	Nexthop tunnel<1-200>	Set the next hop for the tunnel.
	ipv6	Ipv6
	X:X::X:X	IPv6 address
	<tpid-list>	Modify the tunnel tpid value of the message
Default	No modification value	
Mode	Strategy-based mapping configuration Mode	
Usage	Assign the new cos and vid values to the data packets that match the class mapping, and disable the noCommand operation. Reapply the new values only for the classification streams that correspond to the matching criteria.	
Example	Set the VID of the external VLAN Tag for the data packets that meet the C2 rules to 3. 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	

set-queue

Command	set-queue <queue0-queue7> (sp (wrr0 wrr1)) weight <1-255> no set-queue <queue0-queue7>	
Parameter	<queue0-queue7>	Configuration Queue Parameter 0-7
	sp (wrr0 wrr1)	Strict Priority Scheduling Group (Weighted Round Robin Scheduling Group 0 Weighted Round Robin Scheduling Group 1)

	weight <1-255> Weight Range: 1 - 255
Default	Default has queue 0
Mode	Queue scheduling configuration Mode
Usage	This is used to bind the specified queue to different scheduling groups, and determine the forwarding priority and bandwidth allocation logic of this queue. The sp group queues will prioritize the occupation of all bandwidth, and it is necessary to avoid over-configuration to prevent low-priority queues from "starving". The queues in the wrr0 and wrr1 groups can be configured with weights, and the higher the weight, the greater the proportion of bandwidth allocated.
Example	Configure queue 1 to use strict priority scheduling。 Switch(config)# scheduling-profile 1 Switch(config-scheduling-profile-1)# set-queue 1 sp

show class-map

Command	show class-map [<class-map-name>]								
Parameter	[<class-map-name>] Class mapping name								
Default	None								
Mode	Privileges or Global Configuration Mode								
Usage	This Command displays all the class mapping information or the specified class mapping information.								
Example	Switch#show class-map Class map name:cm, used by 1 time(s) match cos: 0 Class map name:color, used by 0 time(s) match cos: 0 <table border="1"> <thead> <tr> <th>display information</th><th>Explain</th></tr> </thead> <tbody> <tr> <td>Class map name:c1</td><td>Class mapping name</td></tr> <tr> <td>used by 1 times</td><td>hours of use</td></tr> <tr> <td>match acl name:1</td><td>Classification rules of the type mapping</td></tr> </tbody> </table>	display information	Explain	Class map name:c1	Class mapping name	used by 1 times	hours of use	match acl name:1	Classification rules of the type mapping
display information	Explain								
Class map name:c1	Class mapping name								
used by 1 times	hours of use								
match acl name:1	Classification rules of the type mapping								

show policy-map

Command	show policy-map [<policy-map-name>]
Parameter	<policy-map- Strategy mapping name

Default	name> None
Mode	Privileges or Global Configuration Mode
Usage	Display the QOS policy mapping. Display all policy mappings or the specified policy mapping information.
Example	<pre>Switch#show policy-map Policy Map 1, used by 0 time(s) Class Map name: cm Policy Map p1, used by 0 time(s) Class Map name: c1 drop set ip precedence 3 policy CIR: 2000 CBS: 512 conform-action: transmit exceed-action: drop</pre>

display information	explain
Policy map name:c1	Strategy mapping name
Class Map name: c1	The name of the referenced class mapping
policy 20000 512	The implemented strategy
used by 0 port	The number of ports using the strategy

show priority-flow-control | (interface ethernet IFNAME)

Command	show priority-flow-control (interface ethernet IFNAME)	
Parameter	IFNAME	Interface name
Default	None。	
Mode	Privileges or Global Configuration Mode	
Usage	Check the global and interface PFC configuration status, and directly issue including Conf (configuration status) and Dot1pList (priority list), while port issues include queue parameter information, TC = Traffic Class (traffic class / priority queue), Threshold (threshold), Headroom (buffer reservation / head room).	
Example	View the scheduling template bound to port 1/0/1. Switch(config)# show priority-flow-control interface ethernet 1/0/1	

Interface	Conf	Dot1pList
Ethernet1/0/1	OFF	None
TC--Priorty Queue	Therhold--Therhold vlaue	Headroom--Headroom vlaue

TC	Therhold	Headroom
0	1000	196608
1	1000	196608
2	1000	196608
3	1000	196608
4	1000	196608
5	1000	196608
6	1000	196608
7	1000	196608

show scheduling-profile |(interface ethernet IFNAME)

Command	show scheduling-profile (interface ethernet IFNAME)
Parameter	IFNAME Interface name;
Default	None
Mode	Privileges or Global Configuration Mode
Usage	View all scheduling file information and the associated interfaces View the current scheduling-profile number bound to the specified physical interface Display the queue scheduling method (SP / WRR) of this scheduling template Display the weights, priorities and bandwidth allocation of each queue.
Example	View the scheduling template bound to port 1。 Switch(config)# show scheduling-profile interface ethernet 1/0/1 SchedulingProfileID: 0 Queue ID: 0 wrr0 weight: 1 Queue ID: 1 wrr0 weight: 2 Queue ID: 2 wrr0 weight: 3 Queue ID: 3 wrr1 weight: 2 Queue ID: 4 wrr1 weight: 3 Queue ID: 5 wrr1 weight: 5 Queue ID: 6 sp Queue ID: 7 sp

show tail-drop |(interface ethernet IFNAME)

Command	show tail-drop (interface ethernet IFNAME)	
Parameter	IFNAME	Interface name;
Default	None	
Mode	Privileges or Global Configuration Mode	
Usage	Check all the discarded file configuration information and application ports. View the discard file configuration information applied to the port and the application port.	
Example	View the scheduling template bound to port 1 Switch(config)# show tail-drop interface ethernet 1/0/1 TailDropProfileID: 0 ProfileType: wred Params: queue 0: ecn: disable offset: 256 dp0 threshold: 256 dynamic-alpha: 2 wred-window: 12288 probability: 50% dp1 threshold: 128 dynamic-alpha: 2 wred-window: 12288 probability: 73% dp2 threshold: 128 dynamic-alpha: 0 wred-window: 12288 probability: 100%	

show mls qos interface

Command	show mls qos {interface ethernet IFNAME [policy queuing] }	
Parameter	IFNAME	Interface name
	policy	Display the information of the traffic regulation policies applied on this interface
	queuing	Display the queue scheduling and congestion management information of this interface
Default	None	
Mode	Privileges or Global Configuration Mode	
Usage	View the summary information of all QoS modules under this interface, including the basic configuration and status of all QoS functions such as supervision and queues.	
Example	View the summary information of all QoS modules on port 1. Switch#show mls qos interface ethernet 1/0/1 Ethernet1/0/1: Default COS: 0 Trust: DSCP Attached Policy Map for Ingress: p1	

Egress 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 1 2 3 4 5 6 7 8

WrrWeight 1 2 3 4 5 6 7 8

WdrrWeight 10 10 20 20 40 40 80 80

Bandwidth Guarantee Configuration:

Queue 1 2 3 4 5 6 7 8

MinBW(K) 0 0 0 0 0 0 0 0

MaxBW(K) 0 0 0 0 0 0 0 0

display information	explain
Ethernet1/0/1	Port name
default cos:0	The DefaultCOS value of the port
Trust: COS	The trust status of the port
Attached Policy Map for Ingress: p1	Port binding Strategy Name
ClassMap	Class mapping name
classified	The total number of data packets that match this ClassMap. If the class mapping does not have a count, display "NA"
in-profile	The total number of data packets that meet the conditions matches this ClassMap. If the class mapping does not have a count, display "NA".
out-profile	The overall summary file data package matches this ClassMap.。
Internal-Priority-TO-Queue map::	Mapping of internal priorities to queues
Queue Algorithm:	WRR, WDDR or PQ queuing method
Queue weights	Queue weight configuration
Bandwidth Guarantee Configuration	Bandwidth guarantee configuration

Switch(config)#show mls qos interface ethernet 1/0/1 queuing

Ethernet1/0/1:

Egress 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	1	2	3	4	5	6	7	8
WrrWeight	1	2	3	4	5	6	7	8
WdrrWeight	10	10	20	20	40	40	80	80

Bandwidth Guarantee Configuration:

Queue	1	2	3	4	5	6	7	8
MinBW(K)	0	0	0	0	0	0	0	0
MaxBW(K)	0	0	0	0	0	0	0	0

display information	explain
Internal-Priority-TO-Queue map::	Mapping of internal priorities to queues
Queue Algorithm:	WRR, WDDR or PQ queuing method
Queue weights	Queue weight configuration
Bandwidth Guarantee Configuration	Bandwidth guarantee configuration

Switch # show mls qos interface ethernet 1/0/1 policy

Ethernet1/0/1:

Attached Policy Map for Ingress: p1

display information	explain
Ethernet1/0/1	Port name
Attached Policy Map for Ingress: p1	Port binding Strategy Name
ClassMap	Class mapping name
classified	The total data packets that match the mapping type.
in-profile	The total number of data packets that match this ClassMap. If the class mapping does not have a count, display "NA"
out-profile	The overall profile data package that matches this ClassMap.

show mls qos in (interface <interface-name> policy) | (vlan <vlan-id>)

Command	show mls qos in (interface <interface-name> policy) (vlan <vlan-id>)				
Parameter	<table> <tr> <td><interface-name></td><td>Port name</td></tr> <tr> <td><vlan-id></td><td>VLAN ID</td></tr> </table>	<interface-name>	Port name	<vlan-id>	VLAN ID
<interface-name>	Port name				
<vlan-id>	VLAN ID				
Default	None				
Mode	Privileges or Global Configuration Mode				

Usage	Display the configuration information of the port or VLAN direction. Display the configuration information of the inbound direction.
Example	Display the configuration information of the inbound direction strategy Switch#show mls qos in interface ethernet1/0/1 policy Ethernet1/0/1: Attached Policy Map for Ingress: p1

show mls qos maps

Command	show mls qos maps [cos-intp cos-dp cos-exp dscp-intp dscp-dp dscp-dscp dscp-exp exp-dp exp-exp exp-intp] [begin include exclude <regular-expression>]																				
Parameter	<table> <tr> <td>cos-intp</td><td>Mapping from the entrance L2 CoS to the internal priority</td></tr> <tr> <td>cos-dp</td><td>Mapping from the entry L2 CoS to the discard priority</td></tr> <tr> <td>cos-exp</td><td>From the entrance COS to the EXP priority mapping</td></tr> <tr> <td>dscp-intp</td><td>Mapping from the entrance DSCP to the internal priority</td></tr> <tr> <td>dscp-dp</td><td>Mapping from the entry DSCP to the discard priority</td></tr> <tr> <td>dscp-dscp</td><td>Mapping from the internal part of the export to the DSCP priority</td></tr> <tr> <td>dscp-exp</td><td>Mapping from DSCP to EXP priority</td></tr> <tr> <td>exp-dp</td><td>From the entry EXP to the discard priority mapping</td></tr> <tr> <td>exp-exp</td><td>From EXP to EXP priority mapping</td></tr> <tr> <td>exp-intp</td><td>From the entrance EXP to the internal priority mapping</td></tr> </table>	cos-intp	Mapping from the entrance L2 CoS to the internal priority	cos-dp	Mapping from the entry L2 CoS to the discard priority	cos-exp	From the entrance COS to the EXP priority mapping	dscp-intp	Mapping from the entrance DSCP to the internal priority	dscp-dp	Mapping from the entry DSCP to the discard priority	dscp-dscp	Mapping from the internal part of the export to the DSCP priority	dscp-exp	Mapping from DSCP to EXP priority	exp-dp	From the entry EXP to the discard priority mapping	exp-exp	From EXP to EXP priority mapping	exp-intp	From the entrance EXP to the internal priority mapping
cos-intp	Mapping from the entrance L2 CoS to the internal priority																				
cos-dp	Mapping from the entry L2 CoS to the discard priority																				
cos-exp	From the entrance COS to the EXP priority mapping																				
dscp-intp	Mapping from the entrance DSCP to the internal priority																				
dscp-dp	Mapping from the entry DSCP to the discard priority																				
dscp-dscp	Mapping from the internal part of the export to the DSCP priority																				
dscp-exp	Mapping from DSCP to EXP priority																				
exp-dp	From the entry EXP to the discard priority mapping																				
exp-exp	From EXP to EXP priority mapping																				
exp-intp	From the entrance EXP to the internal priority mapping																				
Default	None																				
Mode	Privileges or Global Configuration Mode																				
Usage	Display the configuration of QoS mapping.																				
Example	Display the configuration information of the mapping table Switch#show mls qos maps Ingress COS-TO-Internal-Priority map: COS : 0 1 2 3 4 5 6 7 ----- INTP (DEI=0):0 1 2 3 4 5 6 7 INTP (DEI=1):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 (DEI=0):0	0	0	0	0	0	0	0	0

DP (DEI=1):1	1	1	1	1	1	1	1	1

Ingress DSCP-TO-DSCP 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						

Ingress DSCP-TO-Drop-Precedence map:

d1 : d2	0	1	2	3	4	5	6	7	8	9
0:	0	0	0	0	1	1	2	2	0	0
1:	0	0	1	1	2	2	0	0	0	0
2:	1	1	2	2	0	0	0	0	1	1
3:	2	2	0	0	0	0	1	1	2	2
4:	0	0	0	0	1	1	2	2	0	0
5:	0	0	1	1	2	2	0	0	0	0
6:	1	1	2	2						

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

Ingress COS-TO-EXP map:

COS:	0	1	2	3	4	5	6	7

EXP (DEI=0):0	0	0	0	0	0	0	0	0

EXP (DEI=1):0	0	0	0	0	0	0	0	0

Ingress DSCP-TO-EXP map:

DSCP:EXP	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-EXP map:

EXP: 0	1	2	3	4	5	6	7

EXP: 0	0	0	0	0	0	0	0

show mls qos vlan

Command	show mls qos vlan <v-id>
Parameter	<v-id> VLAN ID
Default	None
Mode	Privileges or Global Configuration Mode
Usage	This Command displays the information of QOS VLAN.
Example	Switch#show mls qos vlan 1 Vlan 1: Attached Policy Map for Ingress: 1 Classmap classified(in packets) c1 0 Rule ID classified(in packets)

show mls qos aggregate-policy

Command	show mls qos aggregate-policy [<aggregate-policy-name>]
Parameter	<aggregate-policy-name> Aggregate policy name
Default	None
Mode	Privileges or Global Configuration Mode

Usage	Display all configured aggregation policies or the information of the specified aggregation policy.
Example	<pre>Switch#show mls qos aggregate-policy a2 aggregate policy a2 CIR: 1000 CBS: 1024 conform-action: transmit exceed-action: drop Not used by any policy map</pre>

display information	explain
aggregate policy a2 CIR: 1000 CBS: 1024 conform-action: transmit exceed-action: drop	Configuration of the aggregation strategy.
Not used by any Policy Map	Reference time for the aggregation strategy.

show mls qos out (interface <interface-name> policy) | (vlan <vlan-id>)

Command	show mls qos out (interface <interface-name> policy) (vlan <vlan-id>)	
Parameter	<interface-name>	Port name
	<vlan-id>	VLAN ID
Default	None	
Mode	Privileges or Global Configuration Mode	
Usage	Display the QOS policy configuration information for the output direction of the port or VLAN. Show the policy configuration information for the output direction.	
Example	<pre>Display the strategic configuration information indicating the direction Switch#show mls qos in interface ethernet1/0/1 policy Ethernet1/0/1: Attached Policy Map for egress: p1</pre>	

tail-drop-profile ecn

Command	tail-drop-profile<profile0-profile15>queue<queue0-queue7> ecn(disable enable offset<64-39320>) no tail-drop-profile<profile0-profile15>queue<queue0-queue7> ecn offset	
Parameter	<profile0-profile15>	Tail discard file ID range 0-15
	<queue0-queue7>	Configuration Queue Parameter 0-7

	disable enable offset <64-39320>	Congestion notification function (Off On Extra cache beyond the tail drop threshold <64-39320>, used to trigger ECN marking)
Default	Default disable ECN	
Mode	Privileged Mode	
Usage	The trigger threshold offset used in the tail-drop template to enable or configure ECN (Explicit Congestion Notification) for the specified queue	
Example	Enable ECN for Queue 1. Switch(config)# tail-drop-profile 1 queue 1 ecn enable	

tail-drop-profile

Command	tail-drop-profile <profile0-profile15> queue <queue0-queue7> minlimitbuff <64-39320> no tail-drop-profile<profile0-profile15>queue<queue0-queue7>	
Parameter	<profile0-profile15>	Tail discard file ID range 0-15
	<queue0-queue7>	Configuration Queue Parameter 0-7
	minlimitbuff<64-39320>	Minimum queue depth. When the buffered messages exceed this value (64 - 39320), they will be discarded at the tail.
Default	Default Disable ECN	
Mode	Privileged Mode	
Usage	Set a minimum guaranteed cache for the designated queue to prevent frequent packet loss in the queue. Even if the device is highly congested, this queue will at least be allocated cache units.	
Example	Set the minimum queue cache of 111 for queue 1。 Switch(config)# tail-drop-profile 1 queue 1 minlimitbuff 111	

tail-drop-wred-profile

Command	tail-drop-wred-profile <profile0-profile15> queue<queue0-queue7> (dp0 dp1 dp2) threshold <64-36864> dynamic-alpha <0-11> wred-window <0-36864> probability <100,89,73,67,50,25> no tail-drop-wred-profile <profile0-profile15> queue<queue0-queue7> (dp0 dp1 dp2)	
Parameter	<profile0-profile15>	Tail discard file ID range 0-15
	<queue0-queue7>	Configuration Queue Parameter 0-7
	(dp0 dp1 dp2)	Discard priority 0 Discard priority 1 Discard priority 2
	threshold<64-36864>	Static minimum threshold. When the average length of the queue reaches this value, random dropping begins.

dynamic-alpha <0-11>	Dynamic excess cache factor: The larger the value, the more external cache that can be applied for.
wred-window	Random discard window size
probability <100,89,73,67,50,25>	Probability of discarding: 100%, 89%, 73%, 67%, 50%, 25%

Default	Default does not enable the WRED tail-drop policy. You need to manually create a template.
Mode	Privileged Mode
Usage	This Command is used to create and configure the WRED (Weighted Random Early Detection) tail-drop template. By setting thresholds and packet loss probabilities for different queues and different discard priorities (DP), it enables random early packet dropping during congestion, avoiding global tail-drop caused by queue overflow and TCP global synchronization issues. This is applicable only to Falcon devices!
Example	In the WRED discard template 1, for queue 1 and discard priority DP1, the discard threshold is set to 1111. Once the threshold is reached, the discard probability is 100%. <pre>Switch(config)# tail-drop-wred-profile 1 queue 1 dp1 threshold 1111 dynamic-alpha 1 wred-window 2222 probability 100</pre>

tail-drop-wrtd-profile

Command	tail-drop-wrtd-profile <profile0-profile15> queue<queue0-queue7> minlimitbuff <64-512>						
Parameter	no tail-drop-wrtd-profile <profile0-profile15> queue<queue0-queue7> <table> <tr> <td><profile0-profile15></td><td>Tail discard file ID range 0-15</td></tr> <tr> <td><queue0-queue7></td><td>Configuration Queue Parameter 0-7</td></tr> <tr> <td>minlimitbuff<64-512></td><td>Minimum queue depth. When the buffered messages exceed this value (64 - 512), they will be discarded at the tail.</td></tr> </table>	<profile0-profile15>	Tail discard file ID range 0-15	<queue0-queue7>	Configuration Queue Parameter 0-7	minlimitbuff<64-512>	Minimum queue depth. When the buffered messages exceed this value (64 - 512), they will be discarded at the tail.
<profile0-profile15>	Tail discard file ID range 0-15						
<queue0-queue7>	Configuration Queue Parameter 0-7						
minlimitbuff<64-512>	Minimum queue depth. When the buffered messages exceed this value (64 - 512), they will be discarded at the tail.						
Default	The Default setting does not enable the WRTD tail drop policy. You need to manually create a template.						
Mode	Privileged Mode						
Usage	This Command is used to create and configure the WRTD tail-drop template. Regardless of how tight the overall cache of the device is, this queue can at least retain a certain number of queue depth cache units, which will not be preempted by other queues. This is only applicable to Aldrin2 devices!						
Example	In the WRTD tail-drop template 1, the queue depth cache of queue 1 is not preempted by other queues.。						

transmit

Command	transmit no transmit
Parameter	none
Default	No action set up
Mode	Strategy Class Mapping Mode
Usage	After configuring this Command, simply send the data packet.
Example	Send data packets that meet the criteria of c1. Switch#config Switch(config)#policy-map p1 Switch(config-policy-map-p1)#class c1 Switch(config-policy-map-p1-class-c1)#transmit Switch(config-policy-map-p1-class-c1)#exit Switch(config-policy-map-p1)#exit

show flow-based-redirect

Command	show flow-based-redirect [interface [ethernet] <IFNAME>]
Parameter	< IFNAME > Port name
Default	none
Mode	Privileged Mode
Usage	Display the current information about flow-based redirection in the system/port. This Command is used to display the current flow-based redirection information in the system/port.
Example	Switch(config)#show flow-based-redirect Flow-based-redirect config on interface Ethernet1/0/1: RX flow (access-list 1) is redirected to interface Ethernet1/0/6

07-Commands for Layer 3 Forward and ARP

1 Commands for Layer 3 Interface

description

Command	description <text> no description
parameter	text is the description information of VLAN interface, the length should not exceed 256 characters
default	Do not configure
Mode	VLAN interface mode
Usage Guide	The description information of VLAN interface behind description and shown under the configured VLAN.
Example	Configure the description information of VLAN interface as test vlan. Switch(config)#interface vlan 2 Switch(config-if-vlan2)#description test vlan

interface vlan

Command	interface vlan <vlan-id> no interface vlan <vlan-id>
parameter	vlan-id is the VLAN ID of the established VLAN, ranging from 1 to 4094.
default	No Layer 3 interface is configured upon switch shipment.
Mode	Global Mode
Usage Guide	this command is used to create the 3-layer interface, no the command is used to delete the 3-layer interface.
Example	Create a VLAN interface (layer 3 interface). Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#

show ip route

Command	show ip route [database]
parameter	database is database information.
default	-
Mode	Admin Mode
Usage Guide	Show kernal routing table, include: routing type, destination network, mask, next-hop address, interface, etc.
Example	shows the routing table. 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 C 127.0.0.0/8 is directly connected, Loopback tag:0 Total routes are : 1 item(s) Display information describe C –connected Direct route, namely the segment directly connected with the layer 3 switch

S –static	Static route, the route manually configured by users
R - RIP derived	RIP route, acquired by layer 3 switch through the RIP protocol.
O - OSPF derived	OSPF route, acquired by layer 3 switch through the OSPF protocol
A- OSPF ASE	Route introduced by OSPF
B- BGP derived	BGP route, acquired by the BGP protocol.

2 Commands for IPv4/v6 configuration

clear ip traffic

Command	clear ip traffic
parameter	-
default	-
Mode	Admin Mode.
Usage Guide	Clear the statistic information of receiving and sending packets for IP kernel protocol, including the statistic of receiving packets, sending packets and dropping packets and the error information of receiving and sending packets for IP protocol, ICMP protocol, TCP protocol and UDP protocol.

Example	Clear statistic information of IP protocol. Switch#clear ip traffic

clear ipv6 neighbor

Command	clear ipv6 neighbors
parameter	-

default	-
Mode	Admin Mode.
Usage Guide	This command can not clear static neighbor

Example	Clear neighbor list. Switch#clear ipv6 neighbors

ip address

Command	ip address {<ip-address/mask> <ip-address> <mask>} [secondary] no ip address [<ip-address/mask> <ip-address> <mask>] [secondary]

parameter	<i>ip-address</i>	is IP address, dotted decimal notation;
	<i>mask</i>	is subnet mask, dotted decimal notation;
	secondary	indicates that the IP address is configured as secondary IP address.

default	The system default is no IP address configuration.

Mode	VLAN interface configuration mode

Usage Guide	This command configures IP address on VLAN interface manually. If optional parameter secondary is not configured, then it is configured as the primary IP address of VLAN interface; if optional parameter secondary is configured, then that means the IP address is the secondary IP address of VLAN. One VLAN interface can only have one primary IP address and more than one secondary IP addresses. Primary IP and Secondary IP all can be used on SNMP/Web/Telnet management. Furthermore, the switch also provides BOOTP/DHCP manner to get IP address.

Example	The IP address of switch VLAN1 interface is set to 192.168.1.10/24. Switch(Config-if-Vlan1)#ip address 192.168.1.10 255.255.255.0

ipv6 address

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

parameter	ipv6-address	is the prefix of IPv6 address, parameter
	prefix-length	is the prefix length of IPv6 address, which is between 3-128

	eui-64	means IPv6 address is generated automatically based on eui64 interface identifier of the interface.
default	-	
Mode	Interface Configuration Mode	
Usage Guide	IPv6 address prefix cannot be multicast address or any other specific IPv6 address, and different layer 3 interfaces cannot configure the same address prefix. For global unicast address, the length of the prefix must be greater than or equal to 3. For site-local address and link-local address, the length of the prefix must be greater than or equal to 10.	
Example	Configure an IPv6 address on VLAN1 Layer 3 interface: the prefix is 2001:3f:ed8::99 and the length of the prefix is 64. Switch(Config-if-Vlan1)#ipv6 address 2001:3f:ed8::99/64	

ipv6 nd dad attempts

Command	ipv6 nd dad attempts <value> no ipv6 nd dad attempts	
parameter	value	is the Neighbor Solicitation Message number sent in succession by Duplicate Address Detection and the value of <value> must be in 0-10, NO command restores to default value 1.
default	The default request message number is 1	
Mode	Interface Configuration Mode	
Usage Guide	When configuring an IPv6 address, it is required to process IPv6 Duplicate Address Detection, this command is used to configure the ND message number of Duplicate Address Detection to be sent, value being 0 means no Duplicate Address Detection is executed.	
Example	The Neighbor Solicitation Message number sent in succession by interface when setting Duplicate Address Detection is 3. Switch(Config-if-Vlan1)# ipv6 nd dad attempts 3	

ipv6 nd ns-interval

Command	ipv6 nd ns-interval <seconds> no ipv6 nd ns-interval	
parameter	<i>seconds</i>	is the time interval of sending Neighbor Solicitation Message, <seconds> value must be between 1-3600 seconds, no command restores the default value 1 second.
default	The default Request Message time interval is 1 second.	
Mode	Interface Configuration Mode	
Usage Guide	The value to be set will include the situation in all routing announcement on the interface. Generally, very short time interval is not recommended.	
Example	Set Vlan1 interface to send out Neighbor Solicitation Message time interval to be 8 seconds. Switch(Config-if-Vlan1)#ipv6 nd ns-interval 8	

ipv6 neighbor

Command	ipv6 neighbor <ipv6-address> <mac-address> interface [WORD ethernet port-channel] < WORD > no ipv6 neighbor <ipv6-address>	
parameter	<ipv6-address>	is static neighbor IPv6 address
	<mac-address>	is static neighbor Mac address
	WORD	is Layer 2 interface name
default	There is not static neighbor table entry	
Mode	Interface Configuration Mode	
Usage Guide	IPv6 address and multicast address for specific purpose and local address cannot be set as neighbor.	
Example	Set static neighbor 2001:1:2::4 on port E1/0/1, and the hardware MAC address is 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	

show ip interface

Command	show ip interface [<i><ifname></i> vlan <i><vlan-id></i>] brief			
parameter	<i>ifname</i>		Interface name	
	<i>vlan-id</i>		VLAN ID	
default	Show all brief information of the configured layer 3 interface when no parameter is specified.			
Mode	All modes.			
Usage Guide	This command is used to view brief information on the configured Layer 3 interface.			
Example	view brief information on vlan1 interface configuration.			
	Switch#show ip interface vlan 1 brief			
	Index	Interface	IP-Address	Protocol
	11001	Vlan1	192.168.2.1	up

show ip traffic

Command	show ip traffic
parameter	-
default	-
Mode	Admin Mode
Usage Guide	Display statistics for IP, ICMP, TCP, UDP packets received/sent.
Example	Displays statistics for IP packets. Switch#show ip traffic IP statistics: Rcvd: 3249810 total, 3180 local destination 0 header errors, 0 address errors 0 unknown protocol, 0 discards Frgs: 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

Display content

IP statistics:

Rcvd: 3249810 total, 3180 local
 destination
 0 header errors, 0 address errors
 0 unknown 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, 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
 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

describe

IP packet statistics

Statistics of total packets received,
 number of packets reached local
 destination, number of packets
 have header errors, number of
 erroneous addresses, number of
 packets of unknown protocols;
 number of packets dropped.

Fragmentation statistics: number of
 packets reassembled, timeouts,
 fragments received, fragments
 discarded, packets that cannot be
 fragmented, number of fragments
 sent, etc.

Statistics for total packets sent,
 including number of local packets,
 forwarded packets, dropped
 packets and packets without route.

ICMP packet statistics.

Statistics of total ICMP packets
 received and classified information

Statistics of total ICMP packets sent
 and classified information

quench
0 parameter, 0 timestamp, 0 timestamp
replies
TCP statistics: TCP packet statistics.
UDP statistics: UDP packet statistics.

show ipv6 interface

Command	show ipv6 interface { IFNAME brief ethernet <interface-name> tunnel <interface-name> vlan <vlan-id> }	
parameter	brief	is the brief summarization of IPv6 status and configuration
	<interface-name>	is Layer 3 interface name
	<vlan-id>	Vlan port number, <1-4094>
default	-	
Mode	Admin and Configuration Mode	
Usage Guide	If only brief is specified, then information of all L3 is displayed, and you can also specify a specific Layer 3 interface.	

Example

View information ipv6 the vlan1 interface.
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)

Display content	describe
Vlan1	Layer 3 interface name
[up/up]	Layer 3 interface status
dev index	Internal index No.
fe80::203:fff:fe00:10	Automatically configured IPv6 address of Layer 3 interface
3001::1	Configured IPv6 address of Layer 3 interface

show ipv6 route

Command `show ipv6 route <ipv6-address> | <ipv6-prefix> | database [process-detail] | fib [local | statistics | vrf <vrf-id> [statistics]] | nsm {[bgp | connected | database | isis | kernel | ospf | rip | static]} | process-detail | statistics [vrf <vrf-name>] | vrf <vrf-name> [database]`

parameter	database	is router database

default	-
Mode	Admin and Configuration Mode

Usage Guide `show ipv6 route` only shows IPv6 kernal routing table (routing table in tcpip), database shows all routers except the local router.

Example

Display IPv6 Routing Table.

```
Switch#show ipv6 route
```

IPv6 Routing Table

Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
 I - IS-IS, B - BGP

Timers: Uptime

```
C    ::1/128 via ::, Loopback, 02:55:37 tag:0
```


Display content	describe
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	Abbreviation display sign of every entry

show ipv6 neighbors

Command `show ipv6 neighbors [{vlan <vlan-id> | ethernet <interface-name> | IFNAME | count | tunnel <interface-name> | vrf <vrf-name> | address <ipv6address>}]`

parameter	{vlan ethernet}	specify the lookup based on interface
	interface-name	Interface name
	<vlan-id >	Vlan port number
	<vrf-name>	VRF name
	ipv6address	specifies the lookup based on IPv6 address. It displays the whole neighbor table entry if without parameter.

default -
Mode Admin and Configuration Mode

Usage Guide Displays neighbor table information. If there are no parameters, the entire neighbor table entry is displayed.

Example Check ipv6 Neighbor Table Information.

```
Switch#show ipv6 neighbors
IPv6 neighbour unicast items: 2, valid: 1, matched: 1, incomplete: 0, delayed: 0,
manage items: 0
```

IPv6 Address	State	Age-time(sec)	Hardware Addr	Interface
fe80::d8e4:a662:88e4:dc24	reachable	563	00-e0-4c-21-00-34	Vlan1

IPv6 neighbour table: 1 entries

Display content	describe
IPv6 Address	Neighbor IPv6 address
Hardware Addr	Neighbor MAC address
Interface	Exit interface name
Port	Exit interface name

State	Neighbor status (reachable. statle. delay. probe. permanent. incomplete. unknow)

show ipv6 traffic

Command	show ipv6 traffic
parameter	-
default	-
Mode	Admin and Configuration Mode
Usage Guide	Display IPv6 transmit packet statistics.

Example

Display IPv6 transmit packet statistics.
Switch#show ipv6 traffic
IPv6 statistics:
Rcvd: 27 total, 21 local destination
0 header errors, 0 address errors
0 unknown protocol, 0 discards
Frgs: 0 reassembled, 0 timeouts
0 fragment rcvd, 0 fragment dropped
0 fragmented, 0 couldn't fragment, 0 fragment sent
Sent: 24 generated, 0 forwarded
0 dropped, 0 no route
ICMPv6 statistics:
Rcvd: 21 total, 0 errors
0 unreachable, 0 too big, 0 time exceeded, 0 parameter problems
0 echo requests, 0 echo replies
0 group queries, 0 group responses, 0 group reduces
0 router solicits, 0 router adverts, 0 redirects
9 neighbor solicits, 12 neighbor adverts
Sent: 24 total, 0 errors
0 unreachable, 0 too big, 0 time exceeded, 0 parameter problems
0 echo requests, 0 echo replies
0 group queries, 0 group responses, 0 group reduces
0 router solicits, 0 router adverts, 0 redirects
9 neighbor solicits, 9 neighbor adverts
TCP statistics:
Rcvd: 0 total segments, 0 errors
Sent: 0 total segments, 0 retransmitted segments
UDP statics:
Rcvd: 0 total, 0 errors, 0 no port

Sent: 0 total

Display content

describe

IPv6 statistics:

IPv6 data report statistics

Rcvd: 27 total, 21 local destination
0 header errors, 0 address

IPv6 received packets statistics

errors

0 unknown protocol, 0
discards

Frgs: 0 reassembled, 0 timeouts
0 fragment rcvd, 0 fragment

IPv6 fragmenting statistics

dropped

0 fragmented, 0 couldn't
fragment, 0 fragment sent

Sent: 24 total, 0 errors
0 unreachable, 0 too big, 0

IPv6 sent packets statistics

time exceeded, 0 parameter problems

0 echo requests, 0 echo
replies

0 group queries, 0 group
responses, 0 group reduces

0 router solicits, 0 router
adverts, 0 redirects

9 neighbor solicits, 9
neighbor adverts

ip route

Command

```
ip route {<ip-prefix> <mask> | <ip-prefix/mask> | public [<ip-prefix/mask> <ip-prefix>  
vrf <vrf-name>] | vrf <vrf-name> [<ip-prefix> | <ip-prefix/mask>] }  
{ <ip-prefix> | null0 | tunnel <1-200> | vlan <vlan-id> <ip-prefix> }  
{<1-255>| bfd | tag | track <track-id>} {<1-255> tag <tag-value>}  
no ip route {<ip-prefix> <mask> | <ip-prefix/mask> | public [<ip-prefix/mask> <ip-  
prefix> vrf <vrf-name>] | vrf <vrf-name> [<ip-prefix> | <ip-prefix/mask>] }  
{ <ip-prefix> | null0 | tunnel <1-200> | vlan <vlan-id> <ip-prefix> }  
{<1-255>| bfd} <1-255>
```

parameter

ip-prefix	Routing destination address, for example :1.1.1.1
mask	Routing destination address subnet mask, for example :255.255.255.0

prefix-length	Routing destination address prefix
gateway-address	Address IP next hop, for example :1.1.1.1
null0	Forwarding interface
distance	Routing priority, size range :1-255

default
Mode Default static routing has a priority of 1
Global mode.

Usage Guide This command can be used to configure switch static routing. both the address and the forwarding interface are available by specifying the next hop IP the routing packet when configuring the next hop of the static route.

Example Add static routing to the switch.
Switch(config)#ip route 192.168.2.8/24 null0

3 Commands for ARP Configuration

arp

Command **arp** {timeout [<timeout-value> | **default**] | <ip_address> <mac_address>} {interface [WORD | ethernet | blackhole | port-channel] <portName>}
no arp <ip_address>

parameter	<i>ip_address</i>	is the IP address, at the same field with interface address
	<i>mac_address</i>	is the MAC address
	ethernet	stands for Ethernet port
	<i>portName</i>	for the name of layer2 port

default No static ARP entry is set by default.

Mode VLAN Interface Mode

Usage Guide Static ARP entries can be configured in the switch.

Example Configuring static ARP for interface VLAN1.
Switch(Config-if-Vlan1)#arp 1.1.1.1 00-03-0f-f0-12-34 interface eth 1/0/2

clear arp-cache

Command	clear arp-cache {vlanid <vlan-id>}
parameter	<vlan-id> <1-4094>
default	-
Mode	Admin Mode
Usage Guide	this command is used to clear the arp table.
Example	Clear the arp table. Switch#clear arp-cache

clear arp traffic

Command	clear arp traffic
parameter	-
default	-
Mode	Admin Mode
Usage Guide	Clear the switch ARP message statistics. box switches, this command only clears the statistics of APP messages received and sent from the current card.
Example	Clear switch ARP message statistics. Switch#clear arp traffic

show arp

Command	show arp [traffic] [source-suppression] [<ipaddress>] [<mac-address>] [<vlan-id>] [type {static dynamic}] [count] [vrf word]	
parameter	<i>ipaddress</i>	is a specified IP address
	<i>vlan-id</i>	Vlan id
	<i>mac-address</i>	for entry of specified MAC address
	static	for static ARP entry
	dynamic	for dynamic ARP entry
	count	displays number of ARP entries
	vrf word	is the specified vrf name

default
Mode

-
Admin Mode

Usage Guide

Displays the content of current ARP table such as IP address, MAC address, hardware type, interface name, etc.

Example

Displays the current ARP table content information.

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

Display content

describe

Total arp items

Total number of ARP entries.

Valid

ARP entry number matching the filter conditions and attributing the legality states.

Matched

ARP entry number matching the filter conditions.

Verifying

ARP entry number at verifying again validity for ARP

InCompleted

ARP entry number have ARP request sent without ARP reply.

Failed

ARP entry number at failed state.

None

ARP entry number at begin-found state.

Address

IP address of ARP entries.

Hardware Address

MAC address of ARP entries.

Interface

Layer 3 interface corresponding to the ARP entry.

Port

Physical (Layer2) port corresponding to the ARP entry.

Flag

Describes whether ARP entry is dynamic or static.

show arp traffic

Command

show arp traffic

parameter

-

default	-
Mode	Admin and Config Mode
Usage Guide	Display statistics information of received and sent APP messages.

Example	Displays current ARP statistics. Switch#show arp traffic ARP statistics: Rcvd: 0 request, 0 response Sent: 0 request, 0 response

4 Commands for ARP Scanning Prevention

anti-arpscan enable

Command	anti-arpscan enable no anti-arpscan enable
parameter	-
default	Disable ARP scanning prevention function.
Mode	Global configuration mode
Usage Guide	When remotely managing a switch with a method like telnet, users should set the uplink port as a Super Trust port before enabling anti-ARP-scan function, preventing the port from being shutdown because of receiving too many ARP messages. After the anti-ARP-scan function is disabled, this port will be reset to its default attribute, that is, Untrust port.

Example	Enable the ARP scanning prevention function of the switch. Switch(config)#anti-arpscan enable

anti-arpscan port-based threshold

Command	anti-arpscan port-based threshold <threshold-value> no anti-arpscan port-based threshold		
parameter	<table> <tr> <td>threshold-value</td><td>rate threshold, ranging from 2 to 200.</td></tr> </table>	threshold-value	rate threshold, ranging from 2 to 200.
threshold-value	rate threshold, ranging from 2 to 200.		
default	10 packets /second.		

Mode	Global Configuration Mode
Usage Guide	the threshold of port-based ARP scanning prevention should be larger than the threshold of IP-based ARP scanning prevention, or, the IP-based ARP scanning prevention will fail.
Example	Set the threshold of port-based ARP scanning prevention as 10 packets/second. Switch(config)#anti-arpscan port-based threshold 10

anti-arpscan ip-based threshold

Command	anti-arpscan ip-based threshold <threshold-value> no anti-arpscan ip-based threshold	
parameter	<i>threshold-value</i>	rate threshold, ranging from 1 to 200.
default	3 packets/second.	
Mode	Global configuration mode	
Usage Guide	The threshold of port-based ARP scanning prevention should be larger than the threshold of IP-based ARP scanning prevention, or, the IP-based ARP scanning prevention will fail.	
Example	Set the threshold of IP-based ARP scanning prevention as 6 packets/second. Switch(config)#anti-arpscan ip-based threshold 6	

anti-arpscan trust

Command	anti-arpscan trust [port supertrust-port iptrust-port] no anti-arpscan trust [port supertrust-port iptrust-port]	
parameter	-	
default	By default all the ports are non- trustful.	
Mode	Port configuration mode	
Usage Guide	If a port is configured as a trusted port, then the ARP scanning prevention function will not deal with this port, even if the rate of received ARP messages exceeds the set threshold, this port will not be closed, but the non- trustful IP of this port will still be checked. If a port is set as a super trusted port, then neither the port nor the IP of the port will be dealt with. If the port is already closed by ARP scanning prevention, it will be opened right after being set as a trusted port.	

Example

Set port ethernet 1/0/5 of the switch as a trusted port.
Switch(config-if-ethernet1/0/5)# anti-arpscan trust port

anti-arpscan trust ip

Command

anti-arpscan trust ip <ip-address> [<netmask>]
no anti-arpscan trust ip <ip-address> [<netmask>]

parameter

<i>ip-address</i>	Configure trusted IP address

<i>netmask</i>	Net mask of the IP.

default

By default all the IP are non-trustful. Default mask is 255.255.255.255

Mode

Global configuration mode

Usage Guide

If a port is configured as a trusted port, then the ARP scanning prevention function will not deal with this port, even if the rate of received ARP messages exceeds the set threshold, this port will not be closed. If the port is already closed by ARP scanning prevention, its traffic will be recovered right immediately.

Example

Set 192.168.1.0/24 as trusted IP
Switch(config)#anti-arpscan trust ip 192.168.1.0 255.255.255.0

anti-arpscan recovery enable

Command

anti-arpscan recovery enable
no anti-arpscan recovery enable

parameter

-

default

Enable the automatic recovery function

Mode

Global configuration mode

Usage Guide

If the users want the normal state to be recovered after a while the port is closed or the IP is disabled, they can configure this function.

Example

Enable the automatic recovery function of the switch.
Switch(config)#anti-arpscan recovery enable

anti-arpscan recovery time

Command	anti-arpscan recovery time <seconds> no anti-arpscan recovery time	
parameter	<i>seconds</i>	Automatic recovery time, in second ranging from 5 to 86400.
default	300s	
Mode	Global configuration mode	
Usage Guide	this command is used to configure automatic recovery time, no command is used to restore default configuration.	
Example	Set the automatic recovery time as 3600 seconds. Switch(config)#anti-arpscan recovery time 3600	

anti-arpscan log enable

Command	anti-arpscan log enable no anti-arpscan log enable	
parameter	-	
default	Enable ARP scanning prevention log function.	
Mode	Global configuration mode	
Usage Guide	After enabling ARP scanning prevention log function, users can check the detailed information of ports being closed or automatically recovered by ARP scanning prevention or IP being disabled and recovered by ARP scanning prevention. The level of the log is “Warning”.	
Example	Enable ARP scanning prevention log function of the switch. Switch(config)#anti-arpscan log enable	

anti-arpscan trap enable

Command	anti-arpscan trap enable no anti-arpscan trap enable
parameter	-
default	Disable ARP scanning prevention SNMP Trap function.
Mode	Global configuration mode
Usage Guide	After enabling ARP scanning prevention SNMP Trap function, users will receive Trap message whenever a port is closed or recovered by ARP scanning prevention, and whenever IP t is closed or recovered by ARP scanning prevention.
Example	Enable ARP scanning prevention SNMP Trap function of the switch. Switch(config)#anti-arpscan trap enable

show anti-arpscan

Command	show anti-arpscan [trust [ip port supertrust-port iptrust-port] prohibited [ip port]]
parameter	-
default	Display every port to tell whether it is a trusted port and whether it is closed. If the port is closed, then display how long it has been closed. Display all the trusted IP and disabled IP.
Mode	Admin Mode
Usage Guide	Use “show anti-arpscan trust port” if users only want to check trusted ports. The reset follow the same rule.

Example

Check the operating state of ARP scanning prevention function after enabling it.

Switch#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	trust	N	0
Ethernet1/0/5	trust	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
Ethernet1/0/13	untrust	N	0
Ethernet1/0/14	untrust	N	0
Ethernet1/0/15	untrust	N	0
Ethernet1/0/16	untrust	N	0
Ethernet1/0/17	untrust	N	0
Ethernet1/0/18	untrust	N	0
Ethernet1/0/19	untrust	N	0
Ethernet1/0/20	untrust	N	0
Ethernet1/0/21	untrust	N	0
Ethernet1/0/22	untrust	N	0
Ethernet1/0/23	untrust	N	0
Ethernet1/0/24	untrust	N	0
Ethernet1/0/25	untrust	N	0
Ethernet1/0/26	untrust	N	0
Ethernet1/0/27	untrust	N	0
Ethernet1/0/28	untrust	N	0

No prohibited IP.

Trust IP:

192.168.1.0 255.255.255.0

5 Commands for Preventing ARP Spoofing

ip arp-security updateprotect

Command	ip arp-security updateprotect no ip arp-security updateprotect
parameter	-
default	ARP table automatic update.
Mode	Global Mode/ Interface configuration.
Usage Guide	Forbid ARP table automatic update, the ARP packets conflicting with current ARP item (e.g. with same IP but different MAC or port) will be dropped, the others will be received to update aging timer or create a new item; so, the current ARP item keep unchanged and the new item can still be learned.

Example	Automatic update of ARP table is prohibited.

```
Switch(Config-if-Vlan1)#ip arp-security updateprotect.  
Switch(config)#ip arp-security updateprotect
```

ip arp-security learnprotect

Command	ip arp-security learnprotect no ip arp-security learnprotect
parameter	-
default	ARP learning enabled.
Mode	Global Mode/ Interface Configuration
Usage Guide	This command is for preventing the automatic learning and updating of ARP. Unlike ip arp-security updateprotect, once this command implemented, there will still be timeout even if the switch keeps sending Request/Reply messages.

Example	Prohibit IPv4 version of the ARP learning function. Switch(config)# ip arp-security learnprotect

ip arp-security convert

Command	ip arp-security convert
parameter	-
default	-
Mode	Global Mode/ Interface configuration
Usage Guide	This command will convert the dynamic ARP entries to static ones, which, in combination with disabling automatic learning, can prevent ARP binding. Once implemented, this command will lose its effect.

Example	To change all dynamic ARP to static ARP. Switch(config)#ip arp -security convert

clear ip arp dynamic

Command	clear ip arp dynamic
parameter	-
default	-
Mode	Interface Configuration
Usage Guide	This command will clear dynamic entries before binding ARP. Once implemented, this command will lose its effect.
Example	Clear all dynamic ARP. on the interface. Switch(Config-if-Vlan1)#clear ip arp dynamic

clear ipv6 nd dynamic

Command	clear ipv6 nd dynamic
parameter	-
default	-
Mode	Vlan Interface Mode
Usage Guide	It used in dynamic table when use ND bind function to clear. After executeit, the command will be useless.
Example	Clear all dynamic ND. in ports. Switch(Config-if-Vlan1)#clear ipv6 nd dynamic

6 Command for ARP GUARD

arp-guard ip

Command	arp-guard ip <addr> no arp-guard ip <addr>
parameter	Addr is the protected IP address, in dotted decimal notation

default	There is no ARP GUARD address by default
Mode	Port configuration mode
Usage Guide	After configuring the ARP GUARD address, the ARP messages received from the ports configured ARP GUARD will be filtered. If the source IP addresses of the ARP message match the ARP GUARD address configured on this port, these messages will be judged as ARP cheating messages, which will be directly dropped instead of sending to the CPU of the switch or forwarding. 16 ARP GUARD addresses can be configured on each port.
Example	Configure the ARP GUARD address on port ethernet1/0/1 as 100.1.1.1 <pre>switch(config)#interface ethernet1/0/1 switch(Config-If-Ethernet 1/0/1)#arp-guard ip 100.1.1.1</pre>

7 Commands for Gratuitous ARP Configuration

ip gratuitous-arp

Command	ip gratuitous-arp [<i><interval-time></i>] no ip gratuitous-arp	
parameter	<i>interval-time</i>	is the update interval for gratuitous ARP with its value limited between 5 and 1200 seconds and with default value as 300 seconds.
default	Gratuitous ARP is disabled by default.	
Mode	Global configuration mode and vlan interface configuration mode	
Usage Guide	When configuring gratuitous ARP in global configuration mode, all the Layer 3 interfaces in the switch will be enabled to send gratuitous ARP request. If gratuitous ARP is configured in interface configuration mode, then only the specified interface is able to send gratuitous ARP requests. When configuring the gratuitous ARP, the update interval configuration from interface configuration mode has higher preference than that from the global configuration mode.	
Example	To enable gratuitous ARP in global configuration mode, and set the update interval to be 400 seconds. <pre>Switch#config Switch(config)#ip gratuitous-arp 400</pre>	

show ip gratuitous-arp

Command	show ip gratuitous-arp [interface vlan <vlan-id>]	
parameter	vlan-id	VLAN ID
default	-	
Mode	All the Configuration Modes.	
Usage Guide	Displays gratuitous ARP configuration information.	
Example	Displays gratuitous ARP configuration information. 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	

8 Commands for Dynamic ARP Inspection

ip arp inspection

Command	ip arp inspection {vlan <vlan-id> port [recovery-time <time-value>] } no ip arp inspection {vlan <vlan-id> port [recovery-time] }	
parameter	vlan-id	is the vlan which is enabled the dynamic ARP inspection function
	<time-value>	port recovery time <1-3600s>
default	Disable.	
Mode	Global Mode.	
Usage Guide	After configured the dynamic ARP inspection function in global mode, the administrator can intercept, record and drop the ARP data packets which have the invalid MAC address/IP address.	

Example

Enable the dynamic ARP inspection function of vlan10.
Switch(config)#
Switch(config)#ip arp inspection vlan 10
Switch(config)#exit

ip arp inspection trust

Command

ip arp inspection trust
no ip arp inspection trust

parameter

-

default

All the ports are the untrusted ports as default.

Mode

Port Mode

Usage Guide

After configured this command under the port mode, the configured port will not inspect the received ARP packet and it will forward it directly. If the ARP data packet is received from the untrusted port, the switch will only forward the lawful data packet. For the illegal data, it will drop the data directly and record this action.

Example

Configure the port 1/0/1 as the trusted port.
Switch(config)#
Switch(config)#interface 1/0/1
Switch(config-if-ethernet1/0/1)#ip arp inspection trust

ip arp inspection limit-rate

Command

ip arp inspection limit-rate <rate>
no ip arp inspection limit-rate

parameter

rate	is the configured limited rate of the ARP packet of the untrusted port, the unit is pps

default

Do not limit the rate for the ARP packets of the trusted or untrusted ports.

Mode

Port Mode

Usage Guide

This command can limit the ARP packet rate of the untrusted port. The rate of the lawful ARP data packets forwarding is in the limited range.

Example

Configure the rate of the ARP packet of the untrusted port 1/0/1 as 100pps.

```
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
```

08-Commands for DHCP

1 DHCP

bootfile

Command	Bootfile <filename> no bootfile	
Parameter	<filename>	name of the file to be imported, up 1 to 128 characters are allowed.
Default	None	
Mode	DHCP Address Pool Mode	
Usage	Specify the name of the file to be imported for the client. This is usually used for diskless workstations that need to download a configuration file from the server on boot up. This command is together with the “next sever”.	
Example	The path and filename for the file to be imported is “temp\nos.img” Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#bootfile \temp\nos.img	

clear ip dhcp binding

Command	clear ip dhcp binding (<A.B.C.D> all)	
Parameter	<A.B.C.D>	IP address that has a binding record in decimal format
	all	all IP addresses that have a binding record
Default	None	
Mode	Admin Mode	
Usage	“show ip dhcp binding” command can be used to view binding information for IP addresses and corresponding DHCP client hardware addresses. If the DHCP server is informed that a DHCP client is not using the assigned IP address for some reason before the lease period expires, the DHCP server would not remove the binding information automatically. The system administrator can use this command to delete that IP address-client hardware address binding manually, if “all” is specified, then all auto binding records will be deleted, thus all addresses in the DHCP address pool will be reallocated.	
Example	Removing all IP-hardware address binding records Switch#clear ip dhcp binding all	

clear ip dhcp conflict

Command	clear ip dhcp binding (<A.B.C.D> all)	
Parameter	<A.B.C.D>	IP address that has a conflict record;
	all	All stands for all addresses that have conflict records.
Default	None	
Mode	Admin Mode	
Usage	show ip dhcp conflict” command can be used to check which IP addresses are conflicting for use. The “clear ip dhcp conflict” command can be used to delete the conflict record for an address. If "all" is specified, then all conflict records in the log will be removed. When records are removed from the log, the addresses are available for allocation by the DHCP server	
Example	The network administrator finds 10.1.128.160 that has a conflict record in the log and is no longer used by anyone, so he deletes the record from the address conflict log. Switch#clear ip dhcp conflict 10.1.128.160	

clear ip dhcp server statistics

Command	clear ip dhcp server statistics	
Parameter	None	
Default	None	
Mode	Admin Mode	
Usage	DHCP count statistics can be viewed with “show ip dhcp server statistics” command, all information is accumulated. You can use the “clear ip dhcp server statistics” command to clear the count for easier statistics checking	
Example	Clearing the count for DHCP server. Switch#clear ip dhcp server statistics	

client-identifier

Command	client-identifier <unique-identifier> no client-identifier	
Parameter	<unique-identifier>	user identifier, in dotted Hex format

Default	None
Mode	DHCP Address Pool Mode
Usage	This command is used with “host” when binding an address manually. If the requesting client identifier matches the specified identifier, DHCP server assigns the IP address defined in “host” command to the client.
Example	Specifying the IP address 10.1.128.160 to be bound to user with the unique id of 00-10-5a-60-af-12 in manual address binding. Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#client-identifier 00-10-5a-60-af-12 Switch(dhcp-1-config)#host 10.1.128.160 24

default-router

Command	default-router <A.B.C.D> [<A.B.C.D>[...<A.B.C.D>]] no default-router
Parameter	<A.B.C.D> IP addresses, in decimal format.
Default	No default gateway is configured for DHCP clients by default.
Mode	DHCP Address Pool Mode
Usage	The IP address of default gateway(s) should be in the same subnet as the DHCP client IP, the switch supports up to 8 gateway addresses. The gateway address assigned first has the highest priority, and therefore address1 has the highest priority, and address2 has the second, and so on.
Example	Configuring the default gateway for DHCP clients to be 10.1.128.2 and 10.1.128.100. Switch#config Switch(config) # ip dhcp pool 1 Switch(dhcp-1-config)#default-router 10.1.128.2 10.1.128.100

dns-server

Command	dns-server <A.B.C.D> [<A.B.C.D>[...<A.B.C.D>]] no dns-server
Parameter	<A.B.C.D> IP addresses, in decimal format.
Default	No DNS server is configured for DHCP clients by default.

Mode	DHCP Address Pool Mode
Usage	Up to 8 DNS server addresses can be configured. The DNS server address assigned first has the highest priority, therefore address 1 has the highest priority, and address 2 has the second, and so on.
Example	Set 10.1.128.2 as the DNS server address for DHCP clients. Switch#config Switch(config) # ip dhcp pool 1 Switch(dhcp-1-config)#dns-server 10.1.128.2

domain-name

Command	domain-name <domain> no domain-name
Parameter	<domain> domain name, up to 255 characters are allowed.
Default	None
Mode	DHCP Address Pool Mode
Usage	Specifies a domain name for the client.
Example	Specifying “switch.com.cn” as the DHCP clients’ domain name. Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#domain-name switch.com.cn

hardware-address

Command	hardware-address <hardware-address> [Ethernet IEEE802 <type-number>] no hardware-address
Parameter	<hardware-address> hardware address in Hex Ethernet IEEE802 Ethernet protocol type <type-number> RFC number defined for protocol types, from 1 to 255, e.g., 0 for Ethernet and 6 for IEEE 802.
Default	The default protocol type is Ethernet
Mode	DHCP Address Pool Mode
Usage	This command is used with the “host” when binding address manually. If the requesting client hardware address matches the specified hardware address, the DHCP server assigns the IP address defined in “host” command to the client.

Example	Specify IP address 10.1.128.160 to be bound to the user with hardware address 00-00-e2-3a-26-04 in manual address binding. Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#hardware 00-00-e2-3a-26-04 Switch(dhcp-1-config)#host 10.1.128.160 24

host

Command	host <address> [<mask> <prefix-length>] no host	
Parameter	<address>	IP address in decimal format
	<mask>	subnet mask in decimal format
	<prefix-length>	mask is indicated by prefix. For example, mask 255.255.255.0 in prefix is “24”, and mask 255.255.255.252 in prefix is “30”.
Default	None	
Mode	DHCP Address Pool Mode	
Usage	If no mask or prefix is configured when configuring the IP address, and no information in the IP address pool indicates anything about the mask, the system will assign a mask automatically according to the IP address class. This command is used with “hardware address” command or “client identifier” command when binding addresses manually. If the identifier or hardware address of the requesting client matches the specified identifier or hardware address, the DHCP server assigns the IP address defined in “host” command to the client.	
Example	Specifying IP address 10.1.128.160 to be bound to user with hardware address 00-10-5a-60-af-12 in manual address binding. Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#hardware-address 00-10-5a-60-af-12 Switch(dhcp-1-config)#host 10.1.128.160 24	

ip dhcp conflict logging

Command	ip dhcp conflict logging no ip dhcp conflict logging
Parameter	none
Default	Logging for address conflict is enabled by default.
Mode	Global Mode

Usage	When logging is enabled, once the address conflict is detected by the DHCP server, the conflicting address will be logged. Addresses present in the log for conflicts will not be assigned dynamically by the DHCP server until the conflicting records are deleted.
Example	Disable logging for DHCP server. Switch#config Switch(config)#no ip dhcp conflict logging

ip dhcp disable

Command	ip dhcp disable no ip dhcp disable
Parameter	none
Default	Enable
Mode	Port mode
Usage	After the port disables DHCP services, directly drop all DHCP packets sent by the port.
Example	The port disables DHCP services. Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#ip dhcp disable

ip dhcp excluded-address

Command	ip dhcp excluded-address <low-address> [<high-address>] no ip dhcp excluded-address <low-address> [<high-address>]
Parameter	<low-address> starting IP address <high-address> ending IP address
Default	Only individual address is excluded by default
Mode	Global Mode
Usage	This command can be used to exclude one or several consecutive addresses in the pool from being assigned dynamically so that those addresses can be used by the administrator for other purposes.
Example	Reserving addresses 1.1.1.1 from dynamic assignment. Switch#config Switch(config)#ip dhcp excluded-address 1.1.1.1

ip dhcp pool

Command	ip dhcp pool <name> no ip dhcp pool <name>
Parameter	<name> address pool name, up to 32 characters are allowed
Default	None
Mode	Global Mode
Usage	This command is used to configure a DHCP address pool under Global
Example	Defining an address pool named "1". Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#

ip dhcp conflict ping-detection enable

Command	ip dhcp conflict ping-detection enable no ip dhcp conflict ping-detection enable
Parameter	None
Default	By default, Ping-detection of conflict is disabled.
Mode	Global Mode
Usage	To enable Ping-detection of conflict, one should enable the log of conflict addresses, when which is disabled, so will the ping-detection of conflict. When a client is unable to receive Ping request messages (when blocked by firewall, for example), this function will check local ARP according to allocated IP: if a designated IP has a corresponding ARP, then an address conflict exists; otherwise, allocate it to the client.
Example	Enable Ping-detection of conflict. Switch#config Switch(config)#ip dhcp conflict ping-detection enable

ip dhcp ping packets

Command	ip dhcp ping packets <request-num> no ip dhcp ping packets

Parameter	<request num> number of Ping request message to be sent in Ping-detection of conflict.
Default	No more than 2 Ping request messages will be sent by default.
Mode	Global Mode
Usage	Set the max number of Ping request (Echo Request) message to be sent in Ping-detection of conflict on DHCP server, whose default value is 2; the no operation of this command will restore the default value.
Example	Set the max number of Ping request (Echo Request) message to be sent in Ping-detection of conflict on DHCP server as 3. Switch#config Switch(config)#ip dhcp ping packets 3

ip dhcp ping timeout

Command	ip dhcp ping timeout <timeout-value> no ip dhcp ping timeout
Parameter	<timeout-value> <i><timeout-value></i> is the timeout period of waiting for a reply message after each Ping request message in Ping-detection of conflict.
Default	The timeout period is 500ms by default.
Mode	Global Mode
Usage	Set the timeout period (in ms) of waiting for a reply message (Echo Request) after each Ping request message (Echo Request) in Ping-detection of conflict on DHCP server, whose default value is 500ms. The no operation of this command will restore the default value.
Example	Set the timeout period (in ms) of waiting for each reply message (Echo Request) in Ping-detection of conflict on DHCP server as 600ms. Switch#config Switch(config)#ip dhcp ping timeout 600

lease

Command	lease (<days> [<hours>][<minutes>] infinite) no lease
Parameter	<days> number of days from 0 to 365;
	<hours> number of hours from 0 to 23
	<minutes> number of minutes from 0 to 59
	infinite perpetual use

Default	The default lease duration is 1 day.
Mode	DHCP Address Pool Mode
Usage	DHCP is the protocol to assign network addresses dynamically instead of permanently, hence the introduction of lease duration. Lease settings should be decided based on network conditions: too long lease duration offsets the flexibility of DHCP, while too short duration results in increased network traffic and overhead. The default lease duration of switch is 1 day.
Example	Setting the lease of DHCP pool “sd” to 3 days 12 hours and 30 minutes. <pre>Switch#config Switch(config)#ip dhcp pool sd Switch(dhcp-sd-config)#lease 3 12 30</pre>

max-lease-time

Command	max-lease-time (<days> [<hours>][<minutes>] infinite) no max-lease-time	
Parameter	<days>	number of days from 0 to 365;
	<hours>	number of hours from 0 to 23
	<minutes>	number of minutes from 0 to 59
	infinite	perpetual use
Default	The default lease time is 1 day.	
Mode	DHCP Address Pool Mode	
Usage	This command is used to DHCP request packets with option51. If the lease time (user requests the address) exceeds the maximum lease time configured, the lease that DHCP server assigns the address is the maximum lease time configured. If the lease time requested by the user is less than the maximum lease time configured, the lease that DHCP server assigns the address is the lease time requested by the user. The maximum lease time is able to be set by the administrator according to the actual network condition, and the maximum lease time is 1 day by default.	
Example	Set the maximum lease time of DHCP address pool1 to 3 days 12 hours and 30 minutes. <pre>Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#max-lease-time 3 12 30</pre>	

netbios-name-server

Command	netbios-name-server <address1> [address2[...<address8>]] no netbios-name-server	
Parameter	<address1>...<ad	IP addresses, in decimal format.

Default	dress8> No WINS server is configured by default.
Mode	DHCP Address Pool Mode
Usage	This command is used to specify WINS server for the client, up to 8 WINS server addresses can be configured. The WINS server address assigned first has the highest priority. Therefore, address 1 has the highest priority, and address 2 the second, and so on.
Example	Setting the server address of DHCP pool “1” to 192.168.1.1. Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#netbios-name-server 192.168.1.1

netbios-node-type

Command	netbios-node-type {b-node h-node m-node p-node <type-number>} no netbios-node-type	
Parameter	b-node	broadcasting node
	h-node	hybrid node that broadcasts after point-to-point communication
	m-node	hybrid node to communicate in point-to-point after broadcast;
	p-node	point-to-point node
	<type-number>	node type in Hex from 0 to 255
Default	No client node type is specified by default.	
Mode	DHCP Address Pool Mode	
Usage	If client node type is to be specified, it is recommended to set the client node type to h-node that broadcasts after point-to-point communication.	
Example	Setting the node type for client of pool 1 to broadcasting node. Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)# netbios-node-type b-node	

network-address

Command	network-address <network-number> [<mask> <prefix-length>] no network-address	
Parameter	<network-number>	network number;
	<mask>	subnet mask in the decimal format
	<prefix-length>	mask in prefix form. For example, mask 255.255.255.0 in prefix is “24”, and mask 255.255.255.252 in prefix is “30”. Note: When using DHCP server, the pool mask should be longer or equal to that of layer 3 interface IP address in the

	corresponding segment.
Default Mode	If no mask is specified, default mask will be assigned according to the address class. DHCP Address Pool Mode
Usage	This command sets the scope of addresses that can be used for dynamic assignment by the DHCP server; one address pool can only have one corresponding segment. This command is exclusive with the manual address binding command “hardware address” and “host”.
Example	Configuring the assignable address in pool 1 to be 10.1.128.0/24. Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#network-address 10.1.128.0 24

next-server

Command	next-server <address1>[<address2>[...<address8>]] no next-server
Parameter	<address1>...<address8> IP addresses, in the decimal format
Default Mode	None DHCP Address Pool Mode
Usage	This command configures the address for the server hosting client import file. This is usually used for diskless workstations that need to download configuration files from the server on boot up. This command is used together with “bootfile”.
Example	Setting the hosting server address as 10.1.128.4. Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#next-server 10.1.128.4

option

Command	option <code> {ascii <string> hex <hex> ipaddress <ipaddress>} no option <code>
Parameter	<code> code for network parameters
	<string> ASCII string up to 255 characters
	<hex> a value in Hex that is no greater than 510 and must be of even length
	<ipaddress> IP address in decimal format, up to 63 IP addresses can be configured.
Default Mode	none DHCP Address Pool Mode

Usage	The switch provides common commands for network parameter configuration as well as various commands useful in network configuration to meet different user needs. The definition of option code is described in detail in RFC2123.
Example	Setting the WWW server address as 10.1.128.240. Switch#config Switch(config)# ip dhcp pool 1 Switch(dhcp-1-config)#option 72 ip 10.1.128.240

service dhcp

Command	service dhcp no service dhcp
Parameter	None
Default	DHCP service is disabled by default.
Mode	Global Mode
Usage	Both DHCP server and DHCP relay are included in the DHCP service. When DHCP services are enabled, both DHCP server and DHCP relay are enabled. Switch can only assign IP address for the DHCP clients and enable DHCP relay when DHCP server function is enabled.
Example	Enabling DHCP server. Switch#config Switch(config)#service dhcp

show ip dhcp binding

Command	show ip dhcp binding [[<ip-addr>] [type {all manual dynamic}] [count]]	
Parameter	<ip-addr>	a specified IP address in decimal format
	all	all binding types (manual binding and dynamic assignment)
	manual	manual binding
	dynamic	dynamic assignment
	count	displays statistics for DHCP address binding entries.
Default	None	
Mode	Admin and Configuration Mode	
Usage	Displays IP-MAC binding information.	
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	

Displayed information	Explanation
IP address	IP address IP address assigned to a DHCP client
Hardware address	MAC address of a DHCP client
Lease expiration	Valid time for the DHCP client to hold the IP address
Type	Type of assignment: manual binding or dynamic assignment

show ip dhcp conflict

Command	show ip dhcp conflict
Parameter	none
Default	none
Mode	Admin and Configuration Mode

Usage Displays log information for addresses that have a conflict record.

Example
Switch# show ip dhcp conflict
IP Address Detection method Detection Time
10.1.1.1 Ping FRI JAN 02 00:07:01 2002

Displayed information	Explanation
IP Address	Conflicting IP address
Detection method	Method in which the conflict is detected
Detection Time	Time when the conflict is detected.

show ip dhcp relay information option

Command	show ip dhcp relay information option
Parameter	none
Default	none
Mode	Admin and Configuration Mode

Usage Show the relative configuration for DHCP relay option82

Example
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

show ip dhcp server statistics

Command	show ip dhcp server statistics		
Parameter	none		
Default	none		
Mode	Admin and Configuration Mode		
Usage	Displays statistics of all DHCP packets for a DHCP server		
Example	Switch# show ip dhcp server statistics		
	Address pools	1	
	Database agents	0	
	Automatic bindings	0	
	Manual bindings	0	
	Conflict bindings	0	
	Expiried bindings	0	
	Malformed message	0	
	Message	Received	
	BOOTREQUEST	0	
	DHCPDISCOVER	0	
	DHCPREQUEST	0	
	DHCPDECLINE	0	
	DHCPRELEASE	0	
	DHCPIFORM	0	
	Message	Send	
	BOOTREPLY	0	
	DHCPOFFER	0	
	DHCPACK	0	
	DHCPNAK	0	
	DHCPRELAY	0	
	DHCPFORWARD	0	
	Switch#		
	Displayed information	Explanation	
	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 are expired		
Malformed message	Number of error messages.		
Message Received	Statistics for DHCP packets received		
BOOTREQUEST	Total 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 for DHCP packets sent
BOOTREPLY	Total packets sent
DHCPOFFER	Number of DHCPOFFER packets
DHCPACK	Number of DHCPACK packets
DHCNNAK	Number of DHCNNAK packets
DHCPRELAY	Number of DHCPRELAY packets
DHCPFORWARD	Number of DHCPFORWARD packets

ip dhcp broadcast suppress

Command	ip dhcp broadcast suppress no ip dhcp broadcast suppress
Parameter	none
Default	Disable
Mode	Global Mode
Usage	Enable DHCP broadcast suppress function, the no command disables the function Suppress the forwarding about DHCP broadcast packets, namely, drop or copy DHCP broadcast packets to CPU.
Example	Enable DHCP broadcast suppress function. Switch# config Switch(config)#ip dhcp broadcast suppress

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 <vlanid>
Parameter	<vlanid> VLAN ID of share-vlan <vlanlist> sub-vlan list
Default	None
Mode	Global Mode
Usage	Specify sub-vlan of a share-vlan, the no command cancels sub-vlan. share-vlan may include many sub-vlan, but a sub-vlan only corresponds to a share-vlan. When layer 2 device of DHCP Relay receive DHCP Request, firstly judge whether VLAN with layer 3 interface for receiving package. If there is layer 3 interface in package, use the interface to process DHCP Relay, or else use layer 3 interface of share-vlan to process DHCP Relay when the vlan is sub-vlan of share-vlan.

Example

```
Switch#config
Switch(config)#ip dhcp relay share-vlan 2 sub-vlan 2-4
```

ip forward-protocol udp bootps

Command	ip forward-protocol udp bootps no ip forward-protocol udp bootps
Parameter	none
Default	Not forward UPD broadcast packets by default.
Mode	Global Mode
Usage	Sets DHCP relay to forward UPD broadcast packets on the port; the “ no ip forward-protocol udp bootps ” command cancels the service. The forwarding destination address is set in the “ ip helper-address ” command and described later
Example	Setting DHCP packets to be forwarded to 192.168.1.5. Switch#config Switch(config)#ip forward-protocol udp boots Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip helper-address 192.168.1.5

ip helper-address

Command	ip helper-address <ip-address> no ip helper-address <ip-address>
Parameter	ip-address IP addresses, in the decimal format
Default	none
Mode	Port mode
Usage	Specifies the destination address for the DHCP relay to forward UDP packets. The “ no ip helper-address <ip-address> ” command cancels the setting. The DHCP relay forwarding server address corresponds to the port forwarding UDP, i.e. DHCP relay forwards corresponding UDP packets only to the corresponding server instead of all UDP packets to all servers. When this command is run after “ip forward-protocol udp <port>” command, the forwarding address configured by this command receives the UDP packets from <port>. The combination of “ip forward-protocol udp <port>” command and this command should be used for configuration.
Example	Switch#config Switch(config)#ip forward-protocol udp bootps Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip helper-address 192.168.2.5

show ip forward-protocol

Command	show ip forward-protocol
Parameter	none
Default	none
Mode	Admin and Configuration Mode
Usage	Show the configured port ID of the protocol which support the forwarding of broadcast packets, it means the port ID for forwarding DHCP packets.
Example	Switch#show ip forward-protocol Forward protocol(UDP port): 67(active)

show ip helper-address

Command	show ip helper-address
Parameter	none
Default	none
Mode	Admin and Configuration Mode
Usage	Show the configuration relation for the port ID of the protocol (It can forward broadcast packets), the interface (It supports forwarding function) and the forwarded destination IP.
Example	Switch#show ip helper-address Forward protocol Interface Forward server 67(active) Vlan1 192.168.2.5

clear ipv6 dhcp binding

Command	clear ipv6 dhcp binding [<ipv6-address>] [pd <ipv6-prefix prefix-length>]
Parameter	<ipv6-address> specified IPv6 address with binding record <ipv6-prefix prefix-length> specified IPv6 prefix with binding record; To clear all IPv6 address binding record if there is no specified record.
Default	none
Mode	Admin Configuration Mode
Usage	To clear one specified DHCPv6 assigned address binding record or all the IPv6 address binding records. DHCPv6 IPv6 address binding information can be displayed through the command show ipv6 dhcp binding . If DHCPv6 client does not use the DHCPv6 allocated IPv6 address but when the life time of the IPv6 address does not end, the DHCPv6 server will not remove its bind for this address. In this situation, the address binding information can be removed manually through this command; and if no parameter is appended, this command will remove all the address binding information, then all addresses and prefix will be assigned again in the DHCPv6 address pool.

Example	To delete all binding record of IPv6 address and prefix Switch#clear ipv6 dhcp binding

clear ipv6 dhcp conflict

Command	clear ipv6 dhcp conflict [address]
Parameter	address specified address with the conflict record, no specified address will clear all conflict records.
Default	none
Mode	Admin Mode
Usage	Clear the address with the conflict record in address conflict log. With show ipv6 dhcp conflict command, the user can check the conflict in which IP addresses. With this command, the user can clears the conflict record of an address. If no specified address will clear the conflict record of all addresses in log. After the conflict records are cleared in log, these addresses can be used by DHCPv6 server again.
Example	When administrator checks the conflict logs, administrator discovers that address 2001::1 with the conflict record is not used, so its record will be cleared from address conflict files. Switch#clear ipv6 dhcp conflict 2001::1

clear ipv6 dhcp statistics

Command	clear ipv6 dhcp statistics
Parameter	none
Default	none
Mode	Admin Mode
Usage	Clear the statistic records of DHCPv6 packets, the statistic counter of DHCPv6 packets is cleared. With show ipv6 dhcp statistics command, the user can check the statistic information of the counter for DHCPv6 packets, all statistic information is an accumulative value. With this command will clear the counter to check the debugging conveniently.
Example	Clear the counter of DHCPv6 packets. Switch#clear ipv6 dhcp statistics

dns-server

Command	dns-server <ipv6-address>

	no dns-server <ipv6-address>
Parameter	<ipv6-address> IPv6 address of DNS Server
Default	none
Mode	DHCPv6 Address Pool Configuration Mode.
Usage	To configure the IPv6 address of the DNS server for DHCPv6 client; the no form of this command will remove the DNS configuration. For each address pool, at most three DNS server can be configured, and the addresses of the DNS server must be valid IPv6 addresses.
Example	To configure the DNS Server address of DHCPv6 client as 2001:da8::1. Switch(dhcp-1-config)#dns-server 2001:da8::1

domain-name

Command	domain-name <domain-name> no domain-name <domain-name>
Parameter	<domain-name> domain name, less than 32 characters
Default	The domain name parameter of address pool is not configured by default
Mode	DHCPv6 Address Pool Configuration Mode.
Usage	To configure domain name of DHCPv6 client; the no form of this command will delete the domain name. At most 3 domain names can be configured for each address pool.
Example	To set the domain name of DHCPv6 client as test.com.cn Switch(dhcp-1-config)#domain-name test.com.cn

excluded-address

Command	excluded-address <ipv6-address> no excluded-address <ipv6-address>
Parameter	<ipv6-address> IPv6 address to be excluded from being allocated to hosts in the address pool
Default	Disabled
Mode	DHCPv6 Address Pool Configuration Mode.
Usage	To configure the specified IPv6 address to be excluded from the address pool, the excluded address will not be allocated to any hosts; the no form of this command will remove the configuration. This command is used to preserve the specified address from DHCPv6 address allocation.
Example	To configure to exclude 2001:da8:123::1 from DHCPv6 address allocation. Switch(config)#ipv6 dhcp pool vlan11 Switch(dhcpv6-vlan11-config)#excluded-address 2001:da8:123::1

ipv6 address

Command	ipv6 address <prefix-name> <ipv6-prefix/prefix-length> no ipv6 address <prefix-name> <ipv6-prefix/prefix-length>	
Parameter	<prefix-name> a string with its length no more than 32, designating or manual configuring the name of the address prefix defined in the prefix pool	
	<ipv6-prefix/prefix-length> latter part of the IPv6 address excluding the address prefix, as well as its length.	
Default	No global address is configured for interfaces by default.	
Mode	Port mode	
Usage	To configure the specified interface to use prefix delegation for address allocation. The no form of this command will disable the using of prefix delegation for address allocation. The IPv6 address of an interface falls into two parts: <i><prefix-name></i> and <i><ipv6-prefix/prefix-length></i>. If routing advertisement has been enabled, the first 64 bits of the addresses will be advertised. The address generated by <i><prefix-name></i> and <i><ipv6-prefix/prefix-length></i> combination will be removed, and the advertising of the prefix will be disabled. Only one <i><ipv6-prefix/prefix-length></i> can be configured for one prefix name.	
Example	If the prefix name my-prefix designates 2001:da8:221::/48, then the following command will add the address 2001:da8:221:2008::2008 to interface VLAN1. <pre>Switch(Config-if-Vlan1)# ipv6 address my-prefix 0:0:0:2008::2008/64</pre>	

ipv6 dhcp client pd

Command	ipv6 dhcp client pd <prefix-name> [rapid-commit] no ipv6 dhcp client pd	
Parameter	<prefix-name> <prefix-name> is the string with its length no more than 32, which designates the name of the address prefix.	
	rapid-commit If rapid-commit optional is specified and the prefix delegation server enables the rapid-commit function, then the prefix delegation server will reply the prefix delegation client with the REPLY message directly. And the prefix delegation request will be accomplished by exchanging messages once.	
Default	DHCPv6 prefix delegation client is not enabled by default.	
Mode	Port mode	
Usage	To configure DHCPv6 prefix delegation client for the specified interface. The no form of this command will disable the DHCPv6 prefix delegation client and remove the allocated address prefix. This command is used to configure the prefix delegation client on the specified interface, an interface with prefix delegation client enabled will send SOLICIT packets to try to get address prefix from the server. If the prefix is retrieved correctly, the address prefix in the global address pool can be used by the ipv6 address command to generate a valid IPv6	

address. This command is exclusive with **ipv6 dhcp server** and **ipv6 dhcp relay destination**. If the prefix delegation client is disabled for an interface, then the address prefix which is get from this interface through prefix delegation client, will be removed from the global address pool. Also the interface address which is generated by the prefix delegation client will be removed, and routing advertisement with the prefix will be disabled. If any general prefix has been configured by the **ipv6 general-prefix** command, the same prefix learnt from prefix delegation will be disagreed.

Example	Switch(Config-if-Vlan1)#ipv6 dhcp client pd ClientA rapid-commit

ipv6 dhcp client pd hint

Command	ipv6 dhcp client pd hint <prefix prefix-length> no ipv6 dhcp client pd hint <prefix prefix-length>
Parameter	<prefix prefix-length> prefix demanded by the client and its length.
Default Mode	There is no such configuration in the system by default. Port mode
Usage	Designate the prefix demanded by the client and its length. The no operation of this command will delete that prefix and its length from the specified interface. The system designates a prefix and its length on the interface for a client. If client prefix-proxy demanding function is enabled on the interface and hint function is enabled on the switch, the user will have prior claim to the prefix it demands and the prefix length when the server allocates them. Only one hint prefix is allowed in the system.
Example	Switch(vlan-1-config)#ipv6 dhcp client pd hint 2001::/48

ipv6 dhcp pool

Command	ipv6 dhcp pool <poolname> no ipv6 dhcp pool <poolname>
Parameter	<poolname> address pool name of DHCPv6 with its length no more than 32.
Default Mode	Any DHCPv6 address pool are not configured by default. Global Mode
Usage	To configure the address pool for DHCPv6, and enter the DHCPv6 address pool configuration mode. In this mode, information such as the address prefix to be allocated, the DNS server addresses, and domain names, can be configured for the DHCPv6 client. The no form of this command will remove the configuration of the address pool. This command should be launched in global configuration mode, and falls in DHCPv6 address pool configuration mode if launched successfully. To remove a configured address pool, interface bindings related to the address pool, as well as the related address bindings will be removed.

Example	To define an address pool, named 1.
	Switch#config
	Switch(config)#ipv6 dhcp pool 1

ipv6 dhcp relay destination

Command	ipv6 dhcp relay destination { [<i><ipv6-address></i>] [interface { <i><interface-name></i> vlan <i><1-4096></i> }] } no ipv6 dhcp relay destination { [<i><ipv6-address></i>] [interface { <i><interface-name></i> vlan <i><1-4096></i> }] }	
Parameter	<i><ipv6-address></i>	address of the destination to which the DHCPv6 relay forwards;
	<i><interface-name></i>	interface name which is used for forwarding of DHCPv6 requests
	<i><1-4096></i>	VLAN ID
Default Mode Usage	If <i><ipv6-address></i> is a global unicast address, the interface parameter should not be configured; If <i><ipv6-address></i> is an local address, the interface parameter is required be configured; The destination address for the DHCPv6 server will be the multicast address of ALL_DHCP_Servers (FF05::1:3) , if the interface parameter is configured only.	
	By default, destination address for DHCPv6 relay is not configured.	
	Port mode To configure the destination to which the DHCPv6 relay forwards the DHCPv6 requests from the clients, the destination should be the address of an external DHCPv6 relay or the DHCPv6 server. The no form of this command will remove the configuration. This command is used to configure the DHCPv6 relay for the specified interface, the address should be the address of another DHCPv6 relay or the address DHCPv6 server. At most three relay addresses can be configured for an interface. To be mentioned, the DHCPv6 relay stops working only if all the relay destination address configurations have been removed. This command is mutually exclusive to “ipv6 dhcp server” and “ipv6 dhcp client pd” commands.	
Example	Switch#config Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ipv6 dhcp relay destination 2001:da8::1	

ipv6 dhcp server

Command	ipv6 dhcp server <i><poolname></i> [preference <i><value></i>] [rapid-commit] [allow-hint] no ipv6 dhcp server <i><poolname></i>	
Parameter	<i><poolname></i>	Name of the created DHCPv6 address pool
	<i><value></i>	The priority of the DHCPv6 server, the larger the value, the higher the priority, the range: 0-255, the default is 0.
	rapid-commit	The DHCPv6 server sends the REPLY packet to the client immediately after receiving the SOLICIT packet

	allow-hint	Append the client's expected parameter value to its request packet
Default	DHCPv6 address pool based on port is not configured by default.	
Mode	Port mode	
Usage	This command configures the address pool which will be allocated by the DHCPv6 server through the specified interface. The no form of this command will remove the address pool configuration. This command configure the DHCPv6 address pool which is applied by the DHCPv6 server for the specified interface, as well as optional parameters. One VLAN can bind many DHCPv6 address pools and assign the address for DHCPv6 request packet from direct-link and relay delegation.	
Example	<pre>Switch#config Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ipv6 dhcp server PoolA preference 80 rapid-commit allow-hint</pre>	

ipv6 general-prefix

Command	ipv6 general-prefix <prefix-name> <ipv6-prefix/prefix-length> no ipv6 general-prefix <prefix-name>	
Parameter	<prefix-name>	<i><prefix-name></i> is a character string less than 32 characters, to use as IPv6 general prefix name.
	<ipv6-prefix/prefix-length>	<i><ipv6-prefix/prefix-length></i> is defined as IPv6 general prefix.
Default	IPv6 general prefix is not configured by default.	
Mode	Global Mode	
Usage	To define an IPv6 general prefix. The no form of this command will delete the configuration. If IPv6 general prefix is configured, the interface will use the configured prefix for IPv6 address generating. Commonly, the general prefix is used for enterprise IPv6 prefix, and when entering an IPv6 address, users can simply add the address suffix of to the name of the general prefix. The configured address prefix will be reserved in the general address prefix pool. At most 8 general prefix can be configured at the same time. When trying to remove a configured general prefix name, the operation will fail if any interfaces used the configured prefix. Only one general prefix for a prefix name. The general prefix cannot use the same prefix definition with prefixes learnt from prefix delegation.	
Example	<pre>To set the prefix of 2001:da8:221::/48 to general prefix my-prefix. Switch#config Switch(config)# ipv6 general-prefix my-prefix 2001:da8:221::/48</pre>	

ipv6 local pool

Command	ipv6 local pool <poolname> <prefix/prefix-length> <assigned-length> no ipv6 local pool <poolname>	
Parameter	<poolname>	<i><poolname></i> is the name for the IPv6 address pool of the prefix delegation, the length name string should be less than 32.
	<prefix/prefix-length>	<i><prefix/prefix-length></i> is the address prefix and its length of the prefix delegation.
	<assigned-length>	<i><assigned-length></i> is the length of the prefix in the address pool which can be retrieved by the client, the assigned prefix length should be no less than the value of <i><prefix-length></i>
Default Mode	No IPv6 prefix delegation address pool is configured by default. Global Mode	
Usage	To configure the address pool for prefix delegation. The no form of this command will remove the IPv6 prefix delegation configuration. This command should be used with the “prefix delegation pool” command to allocate address prefixes to the clients. If IPv6 prefix delegation is removed, the associated “prefix delegation” command will be in-effective either.	
Example	Switch#config Switch(config)#ipv6 local pool 1 1100::1/24 24	

lifetime

Command	lifetime {<valid-time> infinity} {<preferred-time> infinity} no lifetime	
Parameter	<valid-time>	The valid lifetime of the IPv6 address allocated in the local address pool, 1-31536000 seconds, must be greater than <preferred-time>
	<preferred-time>	The preferred lifetime of the IPv6 address allocated in the local address pool, 1-31536000 seconds, must be less than <valid-time>
	infinity	Longest service life
Default	The default valid life time and preferred life time are 2592000 seconds (30 days) and 604800 seconds (7 days) respectively	
Mode	DHCPv6 Address Pool Configuration Mode.	
Usage	To configure the life time for the addresses or the address prefixes allocated by DHCPv6. The no form of this command will restore the default setting.	
Example	To configure the valid life time as 1000 seconds, and the preferred life time as 600 seconds. Switch#config Switch(config)#ipv6 dhcp pool vlan11	

network-address

Command	network-address <ipv6-pool-start-address> <ipv6-pool-end-address> <prefix-length> [eui-64]) no network-address	
Parameter	<ipv6-pool-start-address>	start of the address pool;
	<ipv6-pool-end-address>	end of the address pool
	<prefix-length>	The length of the address prefix, ranging from 3 to 128, the default is 64
Default	No address pool is configured by default.。	
Mode	DHCPv6 Address Pool Configuration Mode.	
Usage	To configure the DHCPv6 address pool; the no form of this command will remove the address pool configuration.	
	This command configures the address pool for the DHCPv6 server to allocate addresses, only one address range can be configured for each address pool. To be noticed, if the DHCPv6 server has been enabled, and the length of the IPv6 address prefix has been configured, the length of the prefix in the address pool should be no less than the length of the prefix of the IPv6 address of the respective layer three interfaces in the switch. If <ipv6-pool-end-address> is bigger than <ipv6-pool-start-address>, this command returns at once.	
Example	To configure the address range for address pool as 2001:da8:123::100-2001:da8:123::200. Switch#config Switch(config)#ipv6 dhcp pool 1 Switch(dhcp-1-config)#network-address 2001:da8:123::100 2001:da8:123::200	

prefix-delegation

Command	prefix-delegation <ipv6-prefix/prefix-length> <client-DUID> { [iaid <iaid> lifetime lifetime } {<valid-time> infinity } [iaid <iaid>] no prefix-delegation <ipv6-prefix/prefix-length> <client-DUID> [iaid <iaid>]	
Parameter	<ipv6-prefix/prefix-length>	<ipv6-prefix/prefix-length> is the length of the prefix to be allocated to the client.
	<client-DUID>	<client-DUID> is the DUID of the client. DUID with the type of DUID-LLT and DUID-LL are supported, the DUID of DUID-LLT type should be of 14 characters.
	<iaid>	<iaid> is the value to be appended in the IA_PD field of the

	clients' requests.
<valid-time>	The valid life cycle (in seconds) of the IPv6 address assigned to the client, the range is 1-31536000, the default is 2592000, and it must be greater than the preferred-time
Default	Disabled
Mode	Port mode
Usage	To configure dedicated prefix delegation for the specified user. The no form of this command will remove the dedicated prefix delegation. This command configures the specified IPv6 address prefix to bind with the specified client. If no IAID is configured, any IA of any clients will be able get this address prefix. At most eight static binding address prefix can be configured for each address pool. For prefix delegation, static binding is of higher priority than the prefix address pool.
Example	The following command will allocate 2001:da8::/48 to the client with DUID as 0001000600000005000BBFAA2408, and IAID as 12. Switch#config Switch(config)#ipv6 dhcp pool 1 Switch(dhcp-1-config)#prefix-delegation 2001:da8::/48 0001000600000005000BBFAA240812

prefix-delegation pool

Command	prefix-delegation pool <poolname> lifetime [<valid-time> infinity <preferred-time>] no prefix-delegation pool <poolname>	
Parameter	<poolname>	<poolname> is the name of the address prefix pool, the length name string should be less than 32.
	<valid-time>	The valid life cycle (in seconds) of the IPv6 address assigned to the client, the range is 1-31536000, the default is 2592000, and it must be greater than the preferred-time
	<preferred-time>	The preferred lifetime of the IPv6 address assigned to the client (in seconds), the range is 1-31536000, the default is 604800, and it must be less than valid-time
Default	The prefix delegation name used by DHCPv6 address pool is not configured.	
Mode	DHCPv6 Address Pool Configuration Mode.	
Usage	To configure prefix delegation name used by DHCPv6 address pool. The no form of this command deletes the configuration. This command configures the name of the address prefix pool for address allocation. If configured, the addresses in the prefix address pool will be allocated to the clients. This command can be used in association with the ipv6 local pool command. For one address pool, only one prefix delegation pool can be bound. When trying to remove the prefix name configuration, the prefix delegation service of the server will be unavailable, if both the address pool is not associated with the prefix delegation pool and no static prefix delegation binding is enabled.	

Example	Switch#show subnet-vlan Switch(config)#ipv6 dhcp pool 1 Switch(dhcp-1-config)#prefix-delegation pool abc

service dhcpv6

Command	service dhcpv6 no service dhcpv6
Parameter	none
Default	Disabled
Mode	Global Mode
Usage	To enable DHCPv6 server function; the no form of this command disables the configuration. The DHCPv6 services include DHCPv6 server function, DHCPv6 relay function, DHCPv6 prefix delegation function. All of the above services are configured on ports. Only when DHCPv6 server function is enabled, the IP address assignment of DHCPv6 client, DHCPv6 relay and DHCPv6 prefix delegation functions enabled can be configured on ports.
Example	To enable DHCPv6 server. Switch#config Switch(config)# service dhcpv6

show ipv6 dhcp

Command	show ipv6 dhcp
Parameter	none
Default	none
Mode	Admin and Configuration Mode
Usage	To show the enable switch and DUID of DHCPv6 service To show the enable switch and DUID of DHCPv6 service, server identifier options only use DUID of DUID-LLT type.
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>

show ipv6 dhcp binding

Command	show ipv6 dhcp binding [<ipv6-address> pd <ipv6-prefix prefix-length> count]

Parameter	ipv6-address	specified IPv6 address;
	count	show the number of DHCPv6 address bindings
Default	none	
Mode	Admin and Configuration Mode	
Usage	To show all the address and prefix binding information of DHCPv6, include type, DUID, IAID, prefix, valid time and so on.	
Example	Switch#show ipv6 dhcp binding Client: iatype IANA, iaaid 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	

show ipv6 dhcp conflict

Command	show ipv6 dhcp conflict	
Parameter	none	
Default	none	
Mode	Admin and Configuration Mode	
Usage	Show the log for the address that have a conflict record.	
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>	

show ipv6 dhcp interface

Command	show ipv6 dhcp interface { IFNAME <interface-name> vlan <vlan-id> }	
Parameter	<interface-name>	<i><interface-name></i> is the name and number of interface, if the <i><interface-name></i> parameter is not provided, then all the DHCPv6 interface information will be shown.
	<vlan-id>	Vlan port number<1-4094>
Default	none	
Mode	Admin and Configuration Mode	
Usage	To show the information for DHCPv6 interface, include Port Mode (Prefix delegation	

client. DHCPv6 server. DHCPv6 relay) , and the relative conformation information under all kinds of mode.

Example

```
Switch#show ipv6 dhcp interface vlan10
Vlan10 is in server mode
Using pool: poolv6
Preference value: 20
Rapid-Commit is disabled
```

show ipv6 dhcp pool

Command

show ipv6 dhcp pool [poolname]

Parameter

[poolname] *<poolname>* is the DHCPv6 address pool name which configured already, and the length less than 32 characters. If the *<poolname>* parameter is not provided, then all the DHCPv6 address pool information will be shown.

Default

none

Mode

Admin and Configuration Mode

Usage

To display the configuration and dynamic assignment information for DHCPv6 address pool, include the name of DHCPv6 address pool, the prefix of DHCPv6 address pool, excluded address, DNS server configuration, relative prefix information and so on. To display assigned address binding number of address pool that is used as address assignment server. To display assigned prefix number of address pool that is used as prefix delegation server

Example

```
Switch#show ipv6 dhcp pool poolv6
```

show ipv6 dhcp statistics

Command

show ipv6 dhcp statistics

Parameter

none

Default

none

Mode

Admin and Configuration Mode

Usage

To show the statistic of all kinds of DHCPv6 packets by DHCPv6 server.

Example

```
Switch#show ipv6 dhcp statistics
Address pools          1
Active bindings        0
Expiried bindings      0
Malformed message      0
```

Message

Received

Send

DHCP6SOLICIT	0	0
DHCP6ADVERTISE	0	0
DHCP6REQUEST	0	0
DHCP6REPLY	0	0
DHCP6RENEW	0	0
DHCP6REBIND	0	0
DHCP6RELEASE	0	0
DHCP6DECLINE	0	0
DHCP6CONFIRM	0	0
DHCP6RECONFIGURE	0	0
DHCP6INFORMREQ	0	0
DHCP6RELAYFORW	0	0
DHCP6RELAYREPLY	0	0

Show information	Explanation
Address pools	To configure the number of DHCPv6 address pools;
Active bindings	The number of auto assign addresses;
Expiried bindings	The number of expiried bindings;
Malformed message	The number of malformed messages;
Message Recieved	The statistic 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

show ipv6 general-prefix

Command	show ipv6 general-prefix
Parameter	none
Default	none
Mode	Admin and Configuration Mode

Usage	To show the IPv6 general prefix pool information, include the prefix number in general prefix pool, the name of every prefix, the interface of prefix obtained, and the prefix value.
Example	Switch#show ipv6 general-prefix IPv6 Prefix my, acquired via Manual configuration 2001:da8:221::/48

show ipv6 local pool

Command	show ipv6 local pool {WORD <cr>}
Parameter	WORD Show prefix allocation for a specific pool
Default	none
Mode	Admin and Configuration Mode
Usage	To show the statistic information of DHCPv6 prefix pool, include the name of prefix pool, the prefix and prefix length as well as assigned prefix length, the number of assigned prefix and information in DHCPv6 address pool.
Example	Switch#show ipv6 local pool Pool Prefix Free In use a 2010::1/0/48 65536 0

ip dhcp relay information option

Command	ip dhcp relay information option no ip dhcp relay information option
Parameter	none
Default	The system disables the option82 function by default
Mode	Global Mode
Usage	Set this command to enable the option82 function of the switch Relay Agent. The “ no ip dhcp relay information option ” command is used to disable the option82 function of the switch Relay Agent. Only the DHCP Relay Agents configuring with this command can add option82 to the DHCP request message, and let the server to process it. Before enabling this function, users should make sure that the DHCP service is enabled and the Relay Agent will transmit the udp broadcast messages whose destination port is 67.
Example	Enable the option82 function of the Relay Agent. Switch#config Switch(config)#service dhcp Switch(config)# ip forward-protocol udp bootps Switch(config)# ip dhcp relay information option

ip dhcp relay information option delimiter

Command	ip dhcp relay information option delimiter [colon dot slash space] no ip dhcp relay information option delimiter
Parameter	none
Default	Slash("/")
Mode	Global Mode
Usage	Set the delimiter of each parameter for suboption of option82 in global mode, no command restores the delimiter as slash. Divide the parameters with the configured delimiters after users have defined them which are used to create suboption (remot-de, circuit-id) of option82 in global mode.
Example	Set the parameter delimiters as dot (".") for suboption of option82. Switch#config Switch(config)#ip dhcp relay information option delimiter dot

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				
Parameter	<table><tr><td>standard</td><td>standard means the default VLAN MAC format.</td></tr><tr><td><remote-id></td><td><remote-id> means the remote-id content of option 82 specified by users, its length cannot exceed 64 characters.</td></tr></table>	standard	standard means the default VLAN MAC format.	<remote-id>	<remote-id> means the remote-id content of option 82 specified by users, its length cannot exceed 64 characters.
standard	standard means the default VLAN MAC format.				
<remote-id>	<remote-id> means the remote-id content of option 82 specified by users, its length cannot exceed 64 characters.				
Default	Use standard format to set remote-id of option 82				
Mode	Global Mode				
Usage	Set the suboption2 (remote ID option) content of option 82 added by DHCP request packets (They are received by the interface). The no command sets the additive suboption2 (remote ID option) format of option 82 as standard. The additive option 82 information needs to associate with third-party DHCP server, it is used to specify the remote-id content by users when the standard remote-id format cannot satisfy server's request.				
Example	Set the suboption remote-id of DHCP option82 as street-1-1. Switch#config Switch(config)#ip dhcp relay information option remote-id street-1-1				

ip dhcp relay information option remote-id format

Command	ip dhcp relay information option remote-id format {default vs-hp}				
Parameter	<table><tr><td>default</td><td>default means that remote-id is the VLAN MAC address with hexadecimal format.</td></tr><tr><td>vs-up</td><td>vs-hp means that remote-id is compatible with the remote-id format of HP manufacturer.</td></tr></table>	default	default means that remote-id is the VLAN MAC address with hexadecimal format.	vs-up	vs-hp means that remote-id is compatible with the remote-id format of HP manufacturer.
default	default means that remote-id is the VLAN MAC address with hexadecimal format.				
vs-up	vs-hp means that remote-id is compatible with the remote-id format of HP manufacturer.				

Default Mode	default Global Mode
Usage	Set remote-id format of Relay Agent option82. The default remote-id format defined as below:

Remote option type **Length**



MAC means VLAN MAC address.

The compatible remote-id format with HP manufacturer defined as below:

Remote option type **Length**



IP means the primary IP address of layer 3 interface where DHCP packets from.

Example	Set remote-id of Relay Agent option82 as the compatible format with HP manufacturer. Switch#config Switch(config)#ip dhcp relay information option remote-id format vs-hp

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	
Parameter	WORD	WORD the defined character string of remote-id by themselves, the maximum length is 64.
Default Mode	Using standard method. Global Mode	
Usage	Set creation method for option82, users can define the parameters of remote-id suboption by themselves. After configure this command, if users do not configure remote-id on interface, it will create remote-id suboption for option82 according to self-defined method. For mac, use the format such as 00-02-d1-2e-3a-0d if it is filled to packets with ascii format, but hex format occupies 6 bytes. Each option will be filled to packets according to the configured order of the commands and divide them with delimiter (delimiter is ip dhcp relay information option delimiter configuration).	

Example	Set self-defined method and character string of remote-id suboption are hostname and abc respectively for option82. Switch#config Switch(config)# ip dhcp relay information option self-defined remote-id hostname string abc

ip dhcp relay information option self-defined remote-id format

Command	ip dhcp relay information option self-defined remote-id format [ascii hex]
Parameter	none
Default	ascii
Mode	Global Mode
Usage	Set self-defined format of remote-id for relay option82. self-defined format use ip dhcp relay information option type self-defined remote-id to create remote-id format.
Example	Set self-defined method of remote-id as hex for relay option82. Switch#config Switch(config)# ip dhcp relay information option self-defined remote-id format hex

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	
Parameter	WORD	WORD the defined character string of circuit-id by themselves, the maximum length is 64.
Default	Using standard method.	
Mode	Global Mode	
Usage	Set creation method for option82, users can define the parameters of circute-id suboption by themselves. After configure this command, if users do not configure circuit-id on interface, it will create circuit-id suboption for option82 according to self-defined method. Self-defined format of circuit-id: if self-defined format is ascii, the filled format of vlan such as "Vlan2", the format of port such as "Ethernet1/0/1", the format of mac and remote-mac such as "00-02-d1-2e-3a-0d". If self-defined format is hex, the filled format of vlan occupies 2 bytes, port occupies 4 bytes, a byte means slot (for chassis switch, it means slot ID, for box switch, it is 1), a byte means Module (the default is 0), two bytes means port ID beginning from 1, mac and remote-mac occupy 6 bytes. Each option will be filled to packets according to the configured order of the commands and divide them with delimiter (delimiter is ip dhcp relay information option delimiter configuration).	
Example	Set self-defined method of circuit-id suboption as port, mac for option82.	

```
Switch#config
Switch(config)#ip dhcp relay information option self-defined subscriber-id port id switch-id mac
```

ip dhcp relay information option self-defined subscriber-id format

Command	ip dhcp relay information option self-defined subscriber-id format [ascii hex]
Parameter	none
Default	ascii
Mode	Global Mode
Usage	Set self-defined format of circuit-id for relay option82. self-defined format use ip dhcp relay information option type self-defined subscriber-id to create circuit-id format.
Example	Set self-defined format of circuit-id as hex for relay option82. Switch#config Switch(config)#ip dhcp relay information option self-defined subscriber-id format hex

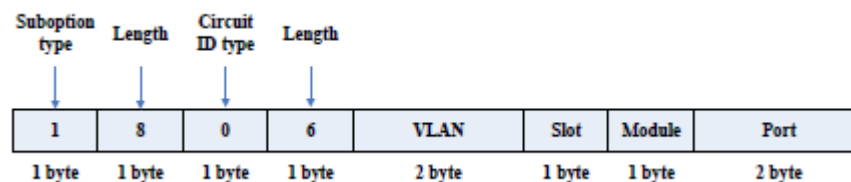
ip dhcp relay information option subscriber-id

Command	ip dhcp relay information option subscriber-id {standard <circuit-id>} no ip dhcp relay information option subscriber-id	
Parameter	<circuit-id>	<i><circuit-id></i> is the circuit-id contents of option82 specified by users, which is a string no longer than 64 characters.
	standard	standard means the standard vlan name and physical port name format
Default	The system uses the standard format to set the circuit-id of option 82 by default.	
Mode	Port mode	
Usage	Because the option 82 information added for the switch should cooperate with the third party DHCP server, if the standard circuit-id format of the switch cannot satisfy the server's request, this method will be provided for users to specify the contents of circuit-id according to the situation of the server.	
Example	Set the sub-option circuit-id of DHCP option82 as foobar. Switch#config Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip dhcp relay information option subscriber-id foobar	

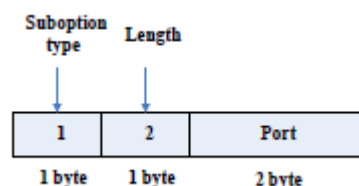
ip dhcp relay information option subscriber-id format

Command	ip dhcp relay information option subscriber-id format {hex ascii vs-hp}

Parameter	hex	hex means that subscriber-id is VLAN and port information with hexadecimal format
	ascii	ascii means that subscriber-id is VLAN and port information with ACSII format.
	vs-hp	vs-hp means that subscriber-id is compatible with the format of HP manufacturer.
Default	ascii	
Mode	Global Mode	
Usage	Set subscriber-id format of Relay Agent option82. VLAN and port information with ASCII format, such as “Vlan1+Ethernet1/0/11”, VLAN and port information with hexadecimal format defined as below:	



VLAN field fills in VLAN ID. For chassis switch, Slot means slot number, for box switch, Slot is 1; default Module is 0; Port means port number which begins from 1.
The compatible subscriber-id format with HP manufacturer defined as below:



Port means port number which begins from 1.

Example	Set subscriber-id format of Relay Agent option82 as hexadecimal format. Switch#config Switch(config)#ip dhcp relay information option subscriber-id format hex	

ip dhcp relay information policy

Command	ip dhcp relay information policy {drop keep replace} no ip dhcp relay information policy	
Parameter	drop	drop mode means that if the message has option82, then the system will drop it without processing;
	keep	keep mode means that the system will keep the original option82 segment in the message, and forward it to the server to process
	replace	replace mode means that the system will replace the option 82 segment in the existing message with its own option 82, and forward the message to the server to process
Default	The system uses replace mode to replace the option 82 segment in the existing message with its own option 82.	
Mode	Port mode	

Usage	This command is used to set the retransmitting policy of the system for the received DHCP request message which contains option82. The “no ip dhcp relay information policy” will set the retransmitting policy of the option 82 DHCP message as “replace”. Since the DHCP client messages might go through several DHCP Relay Agents when passed to the DHCP server, the latter Relay Agents on the path should set policies to decide how to process the option82 added by Relay Agents before them. The selection of option 82 retransmitting policies should take the configuration policy of the DHCP server into account.
Example	Set the retransmitting policy of DHCP messages option 82 as keep. <pre>Switch#config Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ip dhcp relay information policy keep</pre>

ip dhcp server relay information enable

Command	ip dhcp server relay information enable no ip dhcp server relay information enable
Parameter	none
Default	The system disable the option82 identifying function by default.
Mode	Global Mode
Usage	This command is used to enable the switch DHCP server to identify option82. The “no ip dhcp server relay information enable” command will make the server ignore the option 82. If the users want the switch DHCP server to identify option82 and return option 82 information in the reply message, this command needs to be set, or, the switch DHCP server will ignore the option82.
Example	Set the DHCP server to support option82 <pre>Switch#config Switch(config)#ip dhcp server relay information enable</pre>

show ip dhcp relay information option

Command	show ip dhcp relay information option
Parameter	none
Default	none
Mode	Admin and Configuration Mode
Usage	This command will display the state information of the DHCP option 82 in the system, including option82 enabling switch, the interface retransmitting policy, the circuit ID mode and the switch DHCP server option82 enabling switch. Use this command to check the state information of Relay Agent option82 during

Example	operation.
	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

option 43 ascii LINE

Command	option 43 ascii LINE no option 43	
Parameter	LINE	The configured option 43 character string with ascii format, its length range between 1 and 255.
Default	No option 43 character string is configured.	
Mode	DHCP Address Pool Mode	
Usage	Configure option 43 character string with ascii format in ip dhcp pool mode. The no command deletes the configured option 43.	
Example	Configure option 43 with ascii format to be "AP 1000". Switch#config Switch(config)#ip dhcp pool a switch (dhcp-a-config)#option 43 ascii AP 1000	

option 43 hex WORD

Command	option 43 hex WORD no option 43	
Parameter	WORD	The configured option 43 character string with hex format, such as a1241b.
Default	No option 43 is configured.	
Mode	DHCP Address Pool Mode	
Usage	Configure option 43 character string with hex format in ip dhcp pool mode. The no command deletes the configured option 43. When using hex method to configure option 43, the string needs to be written according to TLV (Type-Length-Value) format. For example, issue ip address of 10.1.1.1 through option 43, then the hex string here should be 01040A010101; Type=0x01, it means IP address; Length=0x04, it means the length of IP address is 4 Bytes; Value=0x0A010101, it means the hexadecimal format of 10.1.1.1.	

Example	Configure option 43 with hex format to be "01040a010101". Switch#config Switch(config)#ip dhcp pool a switch (dhcp-a-config)#option 43 hex 01040a010101

option 43 ip A.B.C.D

Command	option 43 ip A.B.C.D no option 43
Parameter	A.B.C.D The configured option 43 with IP format, such as 192.168.1.1. The upper limit for configurable IP addresses is 62.
Default	No option 43 is configured.
Mode	DHCP Address Pool Mode
Usage	Configure option 43 character string with IP format in ip dhcp pool mode. The no command deletes the configured option 43. Using this command to configure option 43, such as "192.168.1.1", then option 43 filled in packets is "C0A80101".
Example	Configure option 43 with IP format to be "192.168.1.1". Switch#config Switch(config)#ip dhcp pool a switch (dhcp-a-config)#option 43 ip 192.168.1.1

option 60 ascii LINE

Command	option 60 ascii LINE no option 60
Parameter	LINE The configured option 60 character string with ascii format, its length range between 1 and 255.
Default	No option 60 character string is configured.
Mode	DHCP Address Pool Mode
Usage	Configure option 60 character string with ascii format in ip dhcp pool mode. The no command deletes the configured option 60.
Example	Configure option 60 with ascii format to be "AP 1000". Switch#config Switch(config)#ip dhcp pool a switch (dhcp-a-config)#option 60 ascii AP 1000

option 60 hex WORD

Command	option 60 hex WORD no option 60
Parameter	WORD The configured option 60 character string with hex format, such as a1241b
Default	No option 60 is configured.
Mode	DHCP Address Pool Mode
Usage	Configure option 60 character string with hex format in ip dhcp pool mode. The no command deletes the configured option 60.
Example	Configure option 60 with hex format to be "01040a010101". Switch#config Switch(config)#ip dhcp pool a switch (dhcp-a-config)#option 60 hex 01040a010101

option 60 ip A.B.C.D

Command	option 60 ip A.B.C.D no option 60
Parameter	A.B.C.D The configured option 60 with IP format, such as 192.168.1.1. The upper limit for configurable IP addresses is 62.
Default	No option 60 is configured.
Mode	DHCP Address Pool Mode
Usage	Configure option 60 character string with IP format in ip dhcp pool mode. The no command deletes the configured option 60. Using this command to configure option 60, such as "192.168.1.1", option 60 of packets matched with the configured option 60 is "C0A80101".
Example	Configure option 60 with IP format to be "192.168.1.1". Switch#config Switch(config)#ip dhcp pool a switch (dhcp-a-config)#option 60 ip 192.168.1.1

address range

Command	address range <start-ipv6> <end-ipv6> no address range <start-ipv6> <end-ipv6>
Parameter	<start-ipv6> defines the start ipv6 address of the address pool <end-ipv6> defines the end ipv6 address of the address pool
Default	None
Mode	DHCPv6 address pool class configuration mode

Usage	This command is used to set address range for a DHCPv6 class in DHCPv6 address pool configuration mode, the no command is used to remove the address range. The prefix/plen form is not supported. It is necessary to check the address range assigned to class in order to make sure that it doesn't exceed the address range of relevant address pool. A class is assigned a single address range and the address range assigned to different class in the same address pool can overlap. If you do not use this command to assign address range for a DHCPv6 class, then the range for it will be the whole subnet of the address pool by default.
Example	Associate a DHCPv6 class named CLASS1 to dhcpv6 pool 1 and assign the address range from 2001:da8:100:1::2 to 2001:da8:100:1::30 for CLASS1. <pre>Switch#config 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</pre>

class

Command	class <class-name> no class <class-name>
Parameter	<class-name> name of DHCPv6 class.
Default	none
Mode	DHCPv6 address pool class configuration mode
Usage	This command associates class to address pool in DHCPv6 address pool configuration mode and enters class configuration mode in address pool. Use the no command to remove the link. It is recommended to define this class first using global command of IPv6 DHCP class. No class will be created if you input a class name which doesn't exist.
Example	Associate the DHCPv6 class named CLASS1 to dhcpv6 pool 1. <pre>Switch(Config)#ipv6 dhcp pool 1 Switch(dhcp-1-config)#class CLASS1</pre>

ipv6 dhcp class

Command	ipv6 dhcp class <class-name> no ipv6 dhcp class <class-name>
Parameter	<class-name> the name of DHCPv6 class which is a string with a length of less than 32
Default	none

Mode	Global Mode
Usage	This command defines a DHCPv6 class and enters DHCPv6 class configuration mode, the no operation of this command removes this DHCPv6 class. Configure a group of option 37 or option 38, or configure option 37 and option 38 simultaneously in a DHCPv6 class. This command can be used when the server supports DHCPv6 class only.
Example	Define a DHCPv6 class named CLASS1. Switch(config)#ipv6 dhcp class CLASS1

ipv6 dhcp relay remote-id

Command	ipv6 dhcp relay remote-id <remote-id> no ipv6 dhcp relay remote-id
Parameter	<remote-id> user-defined content of option 37.
Default	Using vlan MAC address as remote-id content by default such as “00-01-ac-12-23” with ‘-’ hyphen.
Mode	Port mode
Usage	This command is used to set the form of adding option 37 in received DHCPv6 request packets, of which <remote-id> is the remote-id in user-defined option 37 and it is a string with a length of less than 128. The no operation of this command restores remote-id in option 37 to enterprise-number together with vlan MAC address. Because the option 37 information added by switch may associate with third-party DHCPv6 servers, users can specify the remote-id content based on server condition when default remote-id of the switch cannot satisfy the demand of server. The enterprise-number together with vlan MAC address is used as the remote-id by default.
Example	Enable abc as the remote-id of DHCPv6 option 37. Switch#config Switch(config)#interface vlan 1 Switch(config-if-vlan1)# ipv6 dhcp relay remote-id abc

ipv6 dhcp relay remote-id option

Command	ipv6 dhcp relay remote-id option no ipv6 dhcp relay remote-id option
Parameter	none
Default	Disable the relay option 37.
Mode	Global Mode
Usage	This command enables switch relay to support the option 37, the no form of this

command disables it.

Only after this command is configured, DHCPv6 relay agent can add option 37 in DHCPv6 request packets before sending it to server or next relay agent. Make sure that DHCPv6 service has been enabled before execute this command.

Example

```
Enable the switch relay to support option 37.  
Switch#config  
Switch(config)#service dhcpv6  
Switch(config)#ipv6 dhcp relay remote-id option
```

ipv6 dhcp relay subscriber-id

Command	ipv6 dhcp relay subscriber-id <subscriber-id> no ipv6 dhcp relay subscriber-id
Parameter	<subscriber-id> user-defined content of option 38
Default	Set subscriber-id in option 38 to vlan name together with port name.
Mode	Port mode
Usage	This command is used to set the form of adding option 38 in received DHCPv6 request packets, of which <subscriber-id> is the subscriber-id in user-defined option 38 and it is a string with a length of less than 128. Because the option 38 information added by switch may associate with third-party DHCPv6 servers, users can specify the subscriber-id content based on server condition when standard subscriber-id of the switch cannot satisfy the demand of server. The vlan name together with physical port name is used as the subscriber-id in option 38 by default.
Example	<pre>Enable abc as the subscriber-id of DHCPv6 option 38. Switch#config Switch(config) # interface vlan 1 Switch(config-if-vlan1)# ipv6 dhcp relay subscriber-id abc</pre>

ipv6 dhcp relay subscriber-id option

Command	ipv6 dhcp relay subscriber-id option no ipv6 dhcp relay subscriber-id option
Parameter	none
Default	Disable the relay option 38.
Mode	Global Mode
Usage	Only after this command is configured, DHCPv6 relay agent can add option 38 in DHCPv6 request packets before sending it to server or next relay agent. Make sure that

DHCPv6 service has been enabled before execute this command. The option 38 of switch relay is disabled by default.

Example

```
Enable the switch relay to support option 38.  
Switch#config  
Switch(config) # service dhcpv6  
Switch(Config)#ipv6 dhcp relay subscriber-id option
```

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	
Parameter	(sp sv pv spv)	a selection in combinations of slot, port and vlan, among which sp represents slot and port, sv represents slot and vlan, pv represents port and vlan, and spv represents slot, port and vlan.
	WORD	the delimiter between slot, port and vlan which ranges among (# . . : / space). Note that there're two delimiter WORDs here, of which the former is the delimiter between slot and port and the latter is the one between port and vlan.
Default	Null	
Mode	Global Mode	
Usage	Configures user configuration options to generate subscriber-id. The no form of this command restores to its original default configuration, i.e. vlan name together with port name.	
	The command has no effect on ports with self-defined subscriber-id. If user redefines the subscriber-id of the port after using the command, the user-defined one prevails. This configuration is null by default.	
Example	Switch#config Switch(config)#ipv6 dhcp relay subscriber-id select sp delimiter #	

ipv6 dhcp server remote-id option

Command	ipv6 dhcp server remote-id option no ipv6 dhcp server remote-id option	
Parameter	None	
Default	Do not support option 37.	
Mode	Global Mode	
Usage	This command enables DHCPv6 server to support the identification of option 37, the no form of this command disables it.	

Configure this command if option 37 options is expected to be identified and processed by DHCPv6 server, otherwise they will be ignored. Option 37 is not supported by default.

Example

Enable the DHCPv6 server to support option 37.

Switch#config

Switch(config)#ipv6 dhcp server remote-id option

ip dhcp server select relay-forw

Command

ipv6 dhcp server select relay-forw

no ipv6 dhcp server select relay-forw

Parameter

none

Default

Selecting option 37 and option 38 of the original packets.

Mode

Global Mode

Usage

This command enables the DHCPv6 server to support selections when multiple option 37 or option 38 options exist and the option 37 and option 38 of relay-forw in the innermost layer are selected. The no operation of it restores the default configuration, i.e. selecting option 37 and option 38 of the original packets.

Make sure that the server has been enabled to support option 37 and option 38 before use this command. The system selects option 37 and option 38 of the original packets by default.

Example

Configure that the vlan1 interface of DHCPv6 server selects option 37 and option 38 of relay-forw in the innermost layer.

Switch#config

Switch(config)#interface vlan 1

Switch(config-if-vlan1)# ipv6 dhcp server select relay-forw

ipv6 dhcp server subscriber-id option

Command

ipv6 dhcp server subscriber-id option

no ipv6 dhcp server subscriber-id option

Parameter

none

Default

Do not support option 38.

Mode

Global Mode

Usage

This command enables DHCPv6 server to support the identification of option 38, the no operation of this command disables it.

Configure this command if option 38 is expected to be identified and processed by DHCPv6 server, otherwise they will be ignored. option 38 is not supported by default.

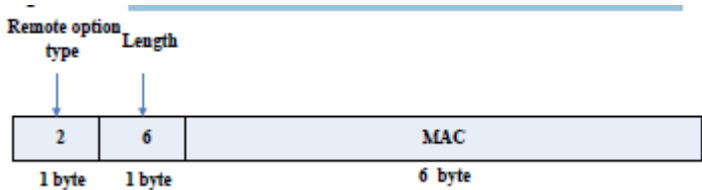
Example

Enable DHCPv6 server to support option 38.

Switch#config

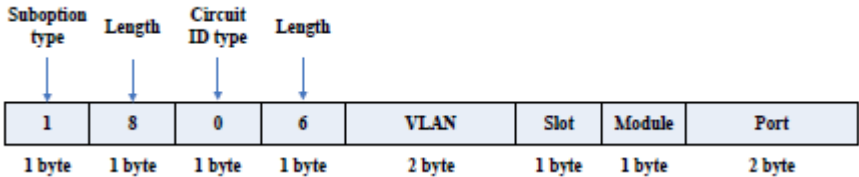
Switch(config)#ipv6 dhcp server subscriber-id option

ipv6 dhcp snooping information option remote-id format

Command	ipv6 dhcp snooping information option remote-id format {hex ascii }	
Parameter	hex	Hex means that the remote-id is the VLAN MAC address of the hexadecimal switch.
	ascii	ascii means that the remote-id is the VLAN MAC address of the ascii format switch.
Default	ascii	
Mode	Global Mode	
Usage	This command can configure the remote-id format of the switch relay agent's DHCPv6 option37. The hexadecimal remote-id format's definition is as below: 	
	The MAC is the VLAN MAC address of the switch.	
Example	Configure the default remote-id format of the switch relay agent's DHCPv6 option37. <pre>Switch#config Switch(config)#ipv6 dhcp snooping information option remote-id format ascii</pre>	

+

ipv6 dhcp snooping information option subscriber-id format

Command	ipv6 dhcp snooping information option subscriber-id format {hex ascii }	
Parameter	hex	hex means that the subscriber-id is the hexadecimal VLAN and port information
	ascii	ascii means that the subscriber-id is the ACSII VLAN and port information.
Default	ascii	
Mode	Global Mode	
Usage	Configure the default subscribe-id format of the switch DHCPv6 snooping option38. The ACSII VLAN and port information is as Vlan1+Ethernet1/0/11. The hexadecimal VLAN and port information is defined as below: 	
	The VLAN field is written with the switch VLAN ID. For the rackmount switch, Slot means the slot number; for the cassette switch, it is 1. The default module is 0. Port means	

the port number and starts from 1.

Example

Configure the subscribe-id format of the switch DHCPv6 snooping option38 as the hexadecimal format.

Switch#config

Switch(config)#ipv6 dhcp snooping information option subscriber-id format hex

ipv6 dhcp snooping remote-id

Command

ipv6 dhcp snooping remote-id <remote-id>

no ipv6 dhcp snooping remote-id

Parameter

<remote-id> user-defined content of option 37.

Default

Using vlan MAC address as remote-id content by default such as “00-01-ac-12-23” with ‘-’ hyphen.

Mode

Port mode

Usage

This command is used to set the form of adding option 37 in received DHCPv6 request packets, of which <remote-id> is the content of remote-id in user-defined option 37 and it is a string with a length of less than 128. The no form of this command restores remote-id in option 37 to enterprise-number together with vlan MAC address.

Because option 37 information added by switch may associate with third-party DHCPv6 servers, users can specify remote-id content based on server condition when standard remote-id of the switch cannot satisfy the demand of server. The enterprise-number together with vlan MAC address is used as the remote-id by default.

Example

Enable abc as remote-id of DHCPv6 option 37.

Switch#config

Switch(config)#interface ethernet 1/0/1

Switch(config-if-Ethernet1/0/1)#ipv6 dhcp snooping remote-id abc

ipv6 dhcp snooping remote-id option

Command

ipv6 dhcp snooping remote-id option

no ipv6 dhcp snooping remote-id option

Parameter

none

Default

Disable.

Mode

Global Mode

Usage

This command enables DHCPv6 SNOOPING to support option 37, the no form of this command disables it.

Only after this command is configured, DHCPv6 SNOOPING can add option 37 in DHCPv6 packets before sending it to server or relay agent. Make sure that DHCPv6 SNOOPING has been enabled before execute this command. The system disables option 37 of DHCPv6 SNOOPING by default.

Example

Enable option 37 in DHCPv6 SNOOPING.

Switch#config
Switch(config)#savi enable
Switch(config)#ipv6 dhcp snooping remote-id option

ipv6 dhcp snooping remote-id policy

Command	ipv6 dhcp snooping remote-id policy {drop keep replace} no ipv6 dhcp snooping remote-id policy	
Parameter	drop	The system only discards it via option 37
	keep	The system keeps option 37 unchanged and forwards the packet
	replace	The system will replace the option 37 field in the existing message with its own option 37 before forwarding the message to the server.
Default Mode	Using replace mode to replace option 37 of current packets with system's own. Global Mode	
Usage	Since DHCPv6 client packets may already include option 37 information, corresponding processing policy of DHCPv6 SNOOPING is required to develop. If the forwarding policy is set as replace , option 37 has to be enabled in advance. Use replace mode to replace option 37 of current packets with system's own by default.	
Example	Configure the reforward policy of DHCPv6 packets with option 37 as keep for DHCPv6 SNOOPING Switch#config Switch(config)#ipv6 dhcp snooping remote-id policy keep	

ipv6 dhcp snooping subscriber-id

Command	ipv6 dhcp snooping subscriber-id <subscriber-id> no ipv6 dhcp snooping subscriber-id	
Parameter	<subscriber-id>	user-defined content of option 38
Default Mode	Set subscriber-id in option 38 to vlan name together with port name. Port mode	
Usage	This command is used to set the form of adding option 38 in received DHCPv6 request packets, of which <subscriber-id> is the content of subscriber-id in user-defined option 38 and it is a string with a length of less than 128. The no operation of this command restores subscriber-id in option 38 to vlan name together with port name such as "Vlan2+Ethernet1/0/2". Because option 38 information added by switch may associate with third-party DHCPv6 servers, users can specify subscriber-id content based on server condition when standard subscriber-id of the switch cannot satisfy the demand of server. The vlan name together with physical port name is used as subscriber-id in option 38 by default.	

Example	Enable abc as subscriber-id of DHCPv6 option 38. Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#ipv6 dhcp snooping subscriber-id abc

ipv6 dhcp snooping subscriber-id optionen

Command	ipv6 dhcp snooping subscriber-id option no ipv6 dhcp snooping subscriber-id option
Parameter	none
Default	Disable option 38 of DHCPv6 SNOOPING.
Mode	DHCP Address Pool Mode
Usage	This command enables DHCPv6 SNOOPING to support option 38, the no form of this command disables it. Only after this command is configured, DHCPv6 SNOOPING can add option 38 in DHCPv6 packets before sending it to server or relay agent. Make sure that DHCPv6 SNOOPING has been enabled before executing this command. The system disables option 38 of DHCPv6 SNOOPING by default.
Example	Enable option 38 in DHCPv6 SNOOPING. Switch#config Switch(config)#savi enable Switch(config)#ipv6 dhcp snooping subscriber-id option

ipv6 dhcp snooping subscriber-id policy

Command	ipv6 dhcp snooping subscriber-id policy {drop keep replace} no ipv6 dhcp snooping subscriber-id policy
Parameter	drop The system only discards it via option 38
	keep The system keeps option 38 unchanged and forwards the packet
	replace The system will replace the option 38 field in the existing message with its own option 38 before forwarding the message to the server.
Default	Using replace mode to replace option 38 of current packets with system's own.
Mode	Global Mode
Usage	Since DHCPv6 client packets may already include option 38 information, corresponding processing policy of DHCPv6 SNOOPING is requested to develop. If the reforward policy is set as replace, option 38 has to be enabled in advance. The system disables option 38 of DHCPv6 SNOOPING by default.
Example	Set the reforward policy of DHCPv6 packets with option 38 as keep for DHCPv6 SNOOPING. Switch#config

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	
Parameter	(sp sv pv spv)	a selection from combinations of slot, port and vlan, among which sp represents slot and port, sv represents slot and vlan, pv represents port and vlan, and spv represents slot, port and vlan.
	WORD	the delimiter between slot, port and vlan which ranges among (# . . ; :/ space). Note that there're two delimiter WORDs here, of which the former is the delimiter between slot and port while the latter is that between port and vlan.
Default	null	
Mode	Global Mode	
Usage	Configure user configuration options to generate subscriber-id. The no form of this command restores to its original default configuration, i.e. vlan name together with port name. This command has no effect on ports with self-defined subscriber-id. If a user redefines subscriber-id of the port after configuring the command, the user-defined one prevails. This configuration is null by default.	
Example	Switch#config Switch(config)#ipv6 dhcp snooping subscriber-id select sv delimiter #	

ipv6 dhcp use class

Command	ipv6 dhcp use class no ipv6 dhcp use class	
Parameter	none	
Default	DHCPv6 server supports DHCPv6 class during address assignment.	
Mode	Global Mode	
Usage	This command enables DHCPv6 server to support DHCPv6 class during address assignment, the no operation of this command disables it without removing the relative DHCPv6 class information that has been configured. By default, DHCPv6 servers support DHCPv6 class during address assignment and the no form of this command doesn't remove DHCPv6 class information that has been configured. Make sure that DHCPv6 service has been enabled before using this command. DHCPv6 server supports DHCPv6 class during address assignment by	

	default.
Example	Configure DHCPv6 server to support DHCPv6 class during address assignment. Switch#config Switch(config)# ipv6 dhcp use class

remote-id subscriber-id

Command	{remote-id [*] <remote-id> [*] subscriber-id [*] <subscriber-id> [*]} no {remote-id [*] <remote-id> [*] subscriber-id [*] <subscriber-id> [*]}	
Parameter	<remote-id>	a string with a length ranging from 1 to 128 bytes is used to match remote-id in option 37.
	<subscriber-id>	a string with a length ranging from 1 to 128 bytes is used to match subscriber-id in option 38.
Default Mode	[*]	match zero or more characters.
	None	
	IPv6 DHCP Class configuration mode	
Usage	This command configures option 37 and option 38 that match the class in IPv6 DHCP class configuration mode. This command configures a mode which matches with the already-defined DHCPv6 class, and a DHCPv6 class may configure multiple commands. If this command is ignored and no mode configured in IPv6 DHCP Class mode, any remote-id or subscriber-id is considered to match with the DHCPv6 class, however, remote-id or subscriber-id must exist in DHCPv6 packet.	
Example	Configure some remote-id or subscriber-id belonging to DHCPv6 class named CLASS1. <pre>Switch#config Switch(config)#ipv6 dhcp class CLASS1 Switch(dhcpv6-class-class1-config)#remote-id abc* subscriber-id bcd* Switch(dhcpv6-class-class1-config)#remote-id edf* Switch(dhcpv6-class-class1-config)#subscriber-id *mmn</pre>	

show ipv6 dhcp relay option

Command	show ipv6 dhcp relay option
Parameter	none
Default	none
Mode	Admin and Configuration Mode
Usage	Use this command to check relay agents' configuration status for option 37 and option 38.
Example	<pre>Switch#show ipv6 dhcp relay option remote-id option enable subscriber-id option enable Interface Vlan 1: remote-id option configure "abc"</pre>

show ipv6 dhcp snooping option

Command	show ipv6 dhcp snooping option
Parameter	none
Default	none
Mode	Admin and Configuration Mode
Usage	Use this command to check snooping configuration status for option 37 and option 38.
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 : #

enable trustview key

Command	enable trustview key {0 7} <password> no enable trustview key	
Parameter	<password>	<i><password></i> is character string length less than 16, which use as encrypted key.
	{0 7}	0 for un-encrypted text for the password, while 7 for encrypted.
Default	Disabled	
Mode	Global Mode	
Usage	To configure DES encrypted key for private packets, this command is also the switch for the private packets encrypt and hash function enabled or not. The switch communicates with the TrustView management system through private protocols. By default these packets are not encrypted. In order to prevent spoofing, it can be configured to encrypt these packets. And at the same time, the same password should be configured on TrustView server.	
Example	Enable encrypt or hash function of private message Switch#config Switch(config)# enable trustview key 0 switch	

ip dhcp snooping

Command	ip dhcp snooping enable no ip dhcp snooping enable

Parameter	none
Default	DHCP Snooping is disabled by default
Mode	Global Mode
Usage	Enable the DHCP Snooping function. When this function is enabled, it will monitor all the DHCP Server packets of non-trusted ports.
Example	Enable the DHCP Snooping function. Switch#config Switch(config)#ip dhcp snooping enable

ip dhcp snooping action

Command	ip dhcp snooping action {shutdown blackhole} [recovery <second>] no ip dhcp snooping action	
Parameter	shutdown	When the port detects a fake DHCP Server, it will be shutdown.
	blackhole	When the port detects a fake DHCP Server, the vid and source MAC of the fake packet will be used to block the traffic from this MAC.
	recovery	Users can set to recover after the automatic defense action being executed.(no shut ports or delete corresponding blackhole) .
	<second>	Users can set how long after the execution of defense action to recover. The unit is second, and valid range is 10-3600.
Default	No default defense action.	
Mode	Port mode	
Usage	Set or delete the automatic defense action of a port. Only when DHCP Snooping is globally enabled, can this command be set. Trusted port will not detect fake DHCP Server, so, will never trigger the corresponding defense action. When a port turns into a trusted port from a non-trusted port, the original defense action of the port will be automatically deleted.	
Example	Set the DHCP Snooping defense action of port ethernet1/0/1 as setting blackhole, and the recovery time is 30 seconds. Switch#config Switch(config)#interface ethernet 1/0/1 Switch(Config-Ethernet1/0/1)#ip dhcp snooping action blackhole recovery 30	

ip dhcp snooping action MaxNum

Command	ip dhcp snooping action {<maxNum> default}	
Parameter	<maxNum>	the number of defense action on each port, the range of which is 1-200, and the value of which is 10 by default.
	default	recover to the default value.

Default	The default value is 10.
Mode	Global Mode
Usage	Set the number of defense action that can be simultaneously took effect. Set the max number of defense actions to avoid the resource exhaustion of the switch caused by attacks. If the number of alarm information is larger than the set value, then the earliest defense action will be recovered forcibly in order to send new defense actions.
Example	Set the number of port defense actions as 100. Switch#config Switch(config)#ip dhcp snooping action 100

ip dhcp snooping binding

Command	ip dhcp snooping binding enable no ip dhcp snooping binding enable
Parameter	none
Default	DHCP Snooping binding is disabled by default.
Mode	Global Mode
Usage	Enable the DHCP Snooping binding funciton When the function is enabled, it will record the binding information allocated by DHCP Server of all trusted ports. Only after the DHCP SNOOPING function is enabled, the binding function can be enabled.
Example	Enable the DHCP Snooping binding funciton. Switch#config Switch(config)#ip dhcp snooping binding enable

ip dhcp snooping binding dot1x

Command	ip dhcp snooping binding dot1x no ip dhcp snooping binding dot1x
Parameter	none
Default	By default, the binding DOT1X funciton is disabled on all ports.
Mode	Port mode
Usage	When this function is enabled, DHCP SNOOPING will notify the DOT1X module about the captured bindng information as a DOT1X controlled user. This command is mutually exclusive to "ip dhcp snooping binding user-contro" command. Only after the DHCP SNOOPING binding function is enabled, the binding dot1x function can be set.
Example	Enable the binding DOT1X funciton on port ethernet1/0/1. Switch#config

```
Switch(config) #interface ethernet 1/0/1
switch(Config-Ethernet 1/0/1)# ip dhcp snooping binding dot1x
```

ip dhcp snooping binding user

Command	ip dhcp snooping binding user <mac> address <ipaddress> vlan <vlan-id> interface [WORD ethernet port-channel] <ifname> no ip dhcp snooping binding user <mac> interface [Ethernet] <ifname>	
Parameter	<mac>	The MAC address of the static binding user, which is the only index of the binding user.
	<ipaddress>	The IP address of the static binding user
	<vlan-id>	The VLAN ID of static binding user
	<ifname>	The access interface of static binding user
Default Mode	DHCP Snooping has no static binding list entry by default. Global Mode	
Usage	The static binding users is deal in the same way as the dynamic binding users captured by DHCP SNOOPING; the follwoing actions are all allowed: notifying DOT1X to be a controlled user of DOT1X, adding a trusted user list entry directly, adding a bingding ARP list entry. The static binding uses will never be aged, and have a priority higher than dynamic binding users. Only after the DHCP SNOOPING binding function is enabled, the static binding users can be enabled.	
Example	Configure static binding users. Switch#config Switch(config)#ip dhcp snooping binding user 00-11-22-33-44-55 address 1.1.1.1 vlan 1 interface ethernet 1/0/14	

ip dhcp snooping binding user-control

Command	ip dhcp snooping binding user-control no ip dhcp snooping binding user-control	
Parameter	None	
Default Mode	By default, the binding user funciton is disabled on all ports. Port mode	
Usage	When this function is enabled, DHCP SNOOPING will treat the captured binding information as trusted users allowed to access all resources. This command is mutually exclusive to “ip dhcp snooping binding dot1x” command. Only after DHCP SNOOPING binding function is enabled, the binding user function can be set. This command is not limited by “ip dhcp snooping” based on VLAN, but it is only limited by the global “ip dhcp snooping enable” command.	
Example	Enable the binding USER funciton on port ethernet1/0/1.	

```
Switch#config
Switch(config)#interface ethernet 1/0/1
Switch(Config-Ethernet 1/0/1)# ip dhcp snooping binding user-control
```

ip dhcp snooping binding user-control max-user

Command	ipv6 dhcp snooping binding user-control max-user <number> no ip dhcp snooping binding user-control max-user
Parameter	<number> <number> the max number of users allowed to access the port, from 0 to 1024.
Default	The max number of users allowed by each port to access is 1024.
Mode	Port mode
Usage	Set the max number of users allowed to access the port when enabling DHCP Snooping binding user function; the no operation of this command will restore default value. This command defines the max number of trust users distributed according to binding information, with ip dhcp snooping binding user-control enabled on the port. By default, the number is 1024. Considering the limited hardware resources of the switch, the actual number of trust users distributed depends on the resource amount. If a bigger max number of users is set using this command, DHCP Snooping will distribute the binding information of untrust users to hardware to be trust users as long as there is enough available resources. Otherwise, DHCP Snooping will change the distributed binding information according to the new smaller max user number. When the number of distributed binding information entries reaches the max limit, no new DHCP will be able to become trust user or to access other network resources via the switch.
Example	Enable DHCP Snooping binding user function on Port ethernet1/0/1, setting the max number of user allowed to access by Port Ethernet1/0/1 as 5. 。 Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-ethernet 1/0/1)#ip dhcp snooping binding user-control max-user 5

ip dhcp snooping information enable

Command	ip dhcp snooping information enable no ip dhcp snooping information enable
Parameter	none
Default	Option 82 function is disabled in DHCP Snooping by default.
Mode	Global Mode
Usage	This command will enable option 82 function of DHCP Snooping on the switch, the no operation of this command will disable that function. Only by implementing this command, can DHCP Snooping add standard option 82 to DHCP request messages and forward the message. The format of option1 in option 82

(Circuit ID option) is standard vlan name plus physical port name, like vlan1+ethernet1/0/12. That of option2 in option 82 (remote ID option) is CPU MAC of the switch, like 00030f023301. If a DHCP request message with option 82 options is received, DHCP Snooping will replace those options in the message with its own. If a DHCP reply message with option 82 options is received, DHCP Snooping will dump those options in the message and forward it.

Example	Enable option 82 function of DHCP Snooping on the switch. <pre>Switch#config Switch(config)#ip dhcp snooping enable Switch(config)# ip dhcp snooping binding enable Switch(config)# ip dhcp snooping information enable</pre>

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)
Parameter	(replace) When the "replace" is setting, the option82 option is allowed to replace.
Default	Drop DHCP packets with option82 option received by untrusted ports.
Mode	Global Mode
Usage	This command is used to set that allow untrusted ports of DHCP snooping to receive DHCP packets with option82 option. When disabling this command, all untrusted ports will drop DHCP packets with option82 option. Usually the switch with DHCP snooping function connects the terminal user directly, so close allow-untrusted by default to avoid option82 option added by user privately. Please set uplink port as trust port when enabling the uplink of DHCP snooping function.
Example	Enable the function that receives DHCP packets with option82 <pre>Switch#config Switch(config)#ip dhcp snooping information option allow-untrusted</pre>

ip dhcp snooping information option delimiter

Command	ip dhcp snooping information option delimiter [colon dot slash space] no ip dhcp snooping information option delimiter
Parameter	none
Default	slash (“/”)
Mode	Global Mode
Usage	Set the delimiter of each parameter for suboption of option82 in global mode, no command restores the delimiter as slash. Divide parameters with the configured delimiters after users have defined them which are used to create suboption (remote-id, circuit-id) of option82 in global mode.
Example	Set the parameter delimiters as dot (“.”) for suboption of option82.

```
Switch#config
Switch(config)#ip dhcp snooping information option delimiter dot
```

ip dhcp snooping information option remote-id

Command	ip dhcp snooping information option remote-id {standard <remote-id> vs-cisco vs-huawei } no ip dhcp snooping information option remote-id	
Parameter	standard	standard means the default VLAN MAC format
	<remote-id>	<remote-id> means the remote-id content of option 82 specified by users, its length can not exceed 64 characters.
Default	Use standard format to set remote-id.	
Mode	Global Mode	
Usage	The additive option 82 needs to associate with third-party DHCP server, it is used to specify the remote-id content by users when the standard remote-id format can not satisfy server's request .	
Example	Set the suboption remote-id of DHCP option82 as street-1-1. Switch#config Switch(config)#ip dhcp snooping information option remote-id street-1-1	

ip dhcp snooping information option self-defined remote-id

Command	ip dhcp snooping information option self-defined remote-id {cpe-mac hostname mac string WORD} no ip dhcp snooping information option self-defined remote-id	
Parameter	WORD	WORD the defined character string of remote-id by themselves, the maximum length is 1-64.
Default	Using standard method.	
Mode	Global Mode	
Usage	Set creation method for option82, users can define the parameters of remote-id suboption by themselves. After configure this command, if users do not configure ip dhcp snooping information option remote-id globally, it will create remote-id suboption for option82 according to self-defined method. For mac, use the format such as 00-02-d1-2e-3a-0d if it is filled to packets with ascii format, but hex format occupies 6 bytes. Each option will be filled to packets according to the configured order of the commands and divide them with delimiter (delimiter is ip dhcp snooping information option delimiter configuration).	
Example	Set self-defined method and character string of remote-id suboption are mac and abc respectively for option82. Switch#config Switch(config)#ip dhcp snooping information option self-defined remote-id mac string abc	

ip dhcp snooping information option self-defined remote-id format

Command	ip dhcp snooping information option self-defined remote-id format [ascii hex]	
Parameter	hex	hex means that the remote-id is the hexadecimal VLAN and port information
	ascii	ascii means that the remote-id is the ACSII VLAN and port information.
Default	ascii	
Mode	Global Mode	
Usage	Set self-defined format of remote-id for snooping option82. self-defined format use ip dhcp snooping information option type self-defined remote-id to create remote-id format.	
Example	Set self-defined format of remote-id as hex for snooping option82. Switch#config Switch(config)#ip dhcp snooping information option self-defined remote-id format hex	

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	
Parameter	WORD	WORD the defined character string of circuit-id by themselves, the maximum length is 64.
Default	Using standard method.	
Mode	Global Mode	
Usage	Set creation method for option82, users can define the parameters of circute-id suboption by themselves. After configure this command, if users do not configure circuit-id on port, it will create circuit-id suboption for option82 according to self-defined method. Self-defined format of circuit-id: if self-defined subscriber-id format is ascii, the filled format of vlan such as "Vlan2", the format of port such as "Ethernet1/0/1", the format of mac and remote-mac such as "00-02-d1-2e-3a-0d". If self-defined format is hex, the filled format of vlan occupies 2 bytes, port occupies 4 bytes, a byte means slot (for chassis switch, it means slot ID, for box switch, it is 1), a byte means Module (the default is 0), two bytes means port ID beginning from 1, mac and remote-mac occupy 6 bytes. Each option will be filled to packets according to the configured order of the commands and divide them with delimiter (delimiter is ip dhcp snooping information option delimiter configuration).	
Example	Set self-defined method of circuit-id suboption as vlan, port, mac and remote-mac for option82.	

```
Switch#config
Switch(config)#ip dhcp snooping information option self-defined subscriber-id vlan port
id remote-mac
```

ip dhcp snooping information option self-defined subscriber-id format

Command	ip dhcp snooping information option self-defined subscriber-id format [ascii hex]	
Parameter	hex	hex means that the subscriber-id is the hexadecimal VLAN and port information
	ascii	ascii means that the subscriber-id is the ACSII VLAN and port information.
Default Mode	ascii	Global Mode
Usage	Set self-defined format of circuit-id for snooping option82. self-defined format uses ip dhcp snooping information option type self-defined subscriber-id to create circuit-id format.	
Example	Set self-defined format of circuit-id as hex for snooping option82. Switch#config Switch(config)#ip dhcp snooping information option self-defined subscriber-id format hex	

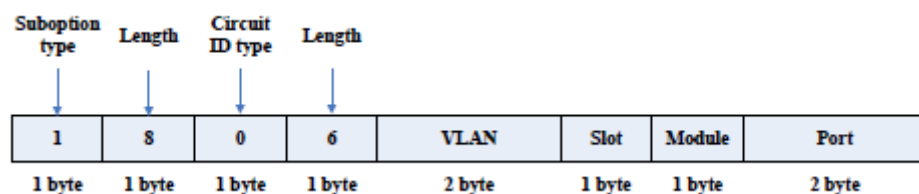
ip dhcp snooping information option subscriber-id

Command	ip dhcp snooping information option subscriber-id {standard <circuit-id>} no ip dhcp snooping information option subscriber-id	
Parameter	standard	standard means the standard format of VLAN name and physical port name, such as Vlan2+Ethernet1/0/12.
	<circuit-id>	<circuit-id> means the circuit-id content of option 82 specified by users, its length can not exceed 64 characters.
Default Mode	Use standard format to set circuit-id.	Port mode
Usage	Set the suboption1 (circuit ID option) content of option 82 added by DHCP request packets (they are received by the port). The no command sets the additive suboption1 (circuit ID option) format of option 82 as standard. The additive option 82 needs to associate with third-party DHCP server, it is used to specify the circuit-id content by user when the standard circuit-id format can not satisfy server's request.	
Example	Set the suboption circuit-id of DHCP option82 as P2. Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#ip dhcp snooping information option subscriber-id P2	

ipv6 dhcp snooping information option subscriber-id format

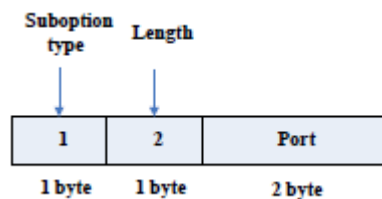
Command	ip dhcp snooping information option subscriber-id format {hex ascii vs-hp vs-huawei }	
Parameter	hex	hex means that subscriber-id is VLAN and port information with hexadecimal format
	ascii	ascii means that subscriber-id is VLAN and port information with ASCII format.
	vs-hp	vs-hp means that subscriber-id is compatible with the format of HP manufacturer.
	vs-huawei	Vendor specific HuaWei format
Default Mode	ascii Global Mode	

Usage This command is used to set subscriber-id format of DHCP snooping option82. VLAN and port information with ASCII format, such as Vlan1+Ethernet1/0/11, VLAN and port information with hexadecimal format defined as below:



VLAN field fill in VLAN ID. For chassis switch, Slot means slot number, for box switch, Slot is 1; default Module is 0; Port means port number which begins from 1.

The compatible subscriber-id format with HP manufacturer defined as below:



Port means port number which begins from 1.

Example	Set subscriber-id format of DHCP snooping option82 as hexadecimal format.	
	Switch#config	
	Switch(config)#ip dhcp snooping information option subscriber-id format hex	

ip dhcp snooping limit-rate

Command	ip dhcp snooping limit-rate <pps> no ip dhcp snooping limit-rate	
Parameter	<pps>	The number of DHCP messages transmitted in every minute, ranging from 0 to 100. Its default value is 100. 0 means that

	no DHCP message will be transmitted.
Default	The default value is 100.
Mode	Global Mode
Usage	Set the DHCP message rate limit After enabling DHCP snooping, the switch will monitor all the DHCP messages and implement software transmission. The software performance of the switch is relative to the type of the switch, its current load and so on.
Example	Set the message transmission rate as 50pps. Switch#config Switch(config)# ip dhcp snooping limit-rate 50

ip dhcp snooping trust

Command	ip dhcp snooping trust no ip dhcp snooping trust
Parameter	none
Default	By default, all ports are non-trusted ports
Mode	Port mode
Usage	Set or delete the DHCP Snooping trust attributes of a port. Only when DHCP Snooping is globally enabled, can this command be set. When a port turns into a trusted port from a non-trusted port, the original defense action of the port will be automatically deleted; all the security history records will be cleared (except the information in system log)
Example	Set port ethernet1/0/1 as a DHCP Snooping trusted port Switch#config Switch(config)#interface ethernet 1/0/1 switch(config- ethernet 1/0/1)#ip dhcp snooping trust

ip dhcp snooping vlan

Command	ip dhcp snooping vlan (WORD) no ip dhcp snooping vlan (WORD)
Parameter	WORD VLAN ID
Default	Disable
Mode	Global Mode
Usage	Enable the dhcp snooping in vlan. no ip dhcp snooping vlan <vlan-id> means to disable the dhcp snooping function on the appointed vlan.
Example	Enable DHCP snooping function. Switch#config

```
Switch(config)#ip dhcp snooping vlan 10
Switch(config)#no ip dhcp snooping vlan 10
```

ip user helper-address

Command	ip user helper-address <svr_addr> [port <udp_port>] source <src_addr> [secondary] no ip user helper-address [secondary]	
Parameter	<svr_addr>	The IP address of HELPER SERVER IP in dotted-decimal notation
	<udp_port>	The UDP port of HELPER SERVER, the range of which is 1 — 65535, and its default value is 9119.
	<src_addr>	The local management IP address of the switch, in dotted-decimal notation.
Default Mode	[secondary]	Whether it is a secondary SERVER address.
	There is no HELPER SERVER address by default.	
Usage	Set the address and port of HELPER SERVER. DHCP SNOOPING will send the monitored binding information to HELPER SERVER to save it. If the switch starts abnormally, it can recover the binding data from HELPER SERVER. The HELPER SERVER function usually is integrated into DCBI packet. The DHCP SNOOPING and HELPER SERVER use the UDP protocol to communicate, and guarantee the arrival of retransmitted data. HELPER SERVER configuration can also be used to sent DOT1X user data from the server, the detail of usage is described in the chapter of dot1x configuration. Two HELPER SERVER addresses are allowed, DHCP SNOOPING will try to connect to PRIMARY SERVER in the first place. Only when the PRIMARY SERVER is unreachable, will the switch c HELPER SERVER connects to SECONDARY SERVER. Please pay attention: source address is the effective management IP address of the switch, if the management IP address of the switch changes, this configuration should be updated in time.	
Example	Set the local management IP address as 100.1.1.1, primary HELPER SERVER address as 100.1.1.100 and the port as default value. <pre>Switch#config 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</pre>	

ip user private packet version two

Command	ip user private packet version two no ip user private packet version two
Parameter	none
Default	The switch choose private packet version one to communicate with DCBI.
Mode	Global Mode
Usage	The switch choose private packet version two to communicate with trustview. If the DCBI access control system is applied, the switch should be configured to use private protocol of version one to communicate with the DCBI server. However, if TrustView is applied, version two should be applied.
Example	To configure the switch choose private packet version two to communicate with inter security management background system. Switch#config Switch(config)#ip user private packet version two

show ip dhcp snooping

Command	show ip dhcp snooping [interface [ethernet] <interfaceName>]																													
Parameter	<interfaceName> The name of the specific port.																													
Default	none																													
Mode	Admin and Configuration Mode																													
Usage	If there is no specific port, then display the current cofiguration information of dhcp snooping, otherwise, display the records of defense actions of the specific port																													
Example	Switch#show ip dhcp snooping User primary helper server 1.1.1.1:9119, source 100.1.1.1, socket 0 seq no 0, connection 0, retry 0, renew 0, binding count 0 00:00:00 retry, 01:16:57 keep alive, 00:00:00 dead Get PrivateDESMD5 Ack 0, Get FreeResource Ack 0, Get HttpRedirPage Ack 0, Get Binding Ack 0 DHCP Snooping is enabled DHCP Snooping maxnum of action info:100 DHCP Snooping limit rate is 100 pps, switch ID 10-f0-13-f1-72-3a DHCP Snooping dropped packets 0, discarded packets 0 DHCP Snooping alarm count 0, binding count 1, static binding count 1, from shell 1, from server 0 expired binding 0, request binding 0 <table><tr><td>interface</td><td>trust</td><td>action</td><td>recovery</td><td>alarm num</td><td>bind num</td></tr><tr><td colspan="6">-----</td></tr><tr><td>Ethernet1/0/1</td><td>trust</td><td>none</td><td>0</td><td>0</td><td>0</td></tr><tr><td>Ethernet1/0/2</td><td>untrust</td><td>none</td><td>0</td><td>0</td><td>0</td></tr></table>						interface	trust	action	recovery	alarm num	bind num	-----						Ethernet1/0/1	trust	none	0	0	0	Ethernet1/0/2	untrust	none	0	0	0
interface	trust	action	recovery	alarm num	bind num																									

Ethernet1/0/1	trust	none	0	0	0																									
Ethernet1/0/2	untrust	none	0	0	0																									

Ethernet1/0/3	untrust	none	0	0	0
Ethernet1/0/4	untrust	none	0	0	0
Ethernet1/0/5	untrust	none	0	0	0
Ethernet1/0/6	untrust	none	0	0	0
Ethernet1/0/7	untrust	none	0	0	0
Ethernet1/0/8	untrust	none	0	0	0
Ethernet1/0/9	untrust	none	0	0	0
Ethernet1/0/10	untrust	none	0	0	0
Ethernet1/0/11	untrust	none	0	0	0
Ethernet1/0/12	untrust	none	0	0	0
Ethernet1/0/13	untrust	none	0	0	0
Ethernet1/0/14	untrust	none	0	0	1
Ethernet1/0/15	untrust	none	0	0	0
Ethernet1/0/16	untrust	none	0	0	0
Ethernet1/0/17	untrust	none	0	0	0
Ethernet1/0/18	untrust	none	0	0	0
Ethernet1/0/19	untrust	none	0	0	0
Ethernet1/0/20	untrust	none	0	0	0
Ethernet1/0/21	untrust	none	0	0	0
Ethernet1/0/22	untrust	none	0	0	0
Ethernet1/0/23	untrust	blackhole	30	0	0
Ethernet1/0/24	untrust	none	0	0	0
Ethernet1/0/25	untrust	none	0	0	0
Ethernet1/0/26	untrust	none	0	0	0
Ethernet1/0/27	untrust	none	0	0	0
Ethernet1/0/28	untrust	none	0	0	0

Displayed Information	Explanation
DHCP Snooping is enable	Whether the DHCP Snooping is globally enabled or disabled.
DHCP Snooping binding arp	Whether the ARP binding function is enabled.
DHCP Snooping maxnum of action info	The number limitation of port defense actions
DHCP Snooping limit rate	The rate limitation of receiving packets
switch ID	The switch ID is used to identify the switch, usually using the CPU MAC address
DHCP Snooping dropped packets	The number of dropped messages when the received DHCP messages exceeds the rate limit.
discarded packets	The number of discarded packets caused by the communication failure within the system. If the CPU of the switch is too busy to schedule the DHCP SNOOPING task and thus can not handle the received DHCP messages, such situation might happen.
DHCP Snooping alarm count:	The number of alarm information.
binding count	The number of binding information.
expired binding	The number of binding information which is already expired but

	has not been deleted. The reason why the expired information is not deleted immediately might be that the switch needs to notify the helper server about the information, but the helper server has not acknowledged it.
request binding	The number of REQUEST information
interface	The name of port
trust	The trust attributes of the port
action	The automatic defense action of the port
recovery	The automatic recovery time of the port
alarm num	The number of history records of the port automatic defense actions
bind num	The number of port-relative binding information.

show ip dhcp snooping binding all

Command	show ip dhcp snooping binding all				
Parameter	none				
Default	none				
Mode	Admin and Configuration Mode				
Usage	This command can check the global binding information of DHCP snooping, each table entry includes the corresponding MAC address, IP address, port name, VLAN ID and the flag of the binding state. Besides, DHCP Snooping must be enabled globally, this command can be configured.				
Example	Switch#show ip dhcp snooping binding all ip dhcp snooping static binding count:1, dynamic binding count:0				
	MAC	IP address	Interface	Vlan ID	Flag

	00-11-22-33-44-55	1.1.1.1	Ethernet1/0/14	1	SE

show trustview status

Command	show trust status
Parameter	none
Default	none
Mode	Admin and Configuration Mode

Usage	This command can be used for debugging the communication messages between the switch and the TrustView server, messages such as protocol version notification, encryption negotiation, free resource and web URL redirection, and the number of forced log-off messages, as well as the number of forced accounting update messages, can be displayed.
Example	<pre>Switch#show trustview status Primary trustview Server 1.1.1.1:9119 trustview version2 message inform failed trustview inform free resource failed trustview inform web redirect address failed trustview inform user binding data failed trustview version 2 message encrypt/digest not enabled Rcvd 0 force log-off packets Rcvd 0 force accounting update packets using version two private packet</pre>

ip dhcp snooping information enable

Command	ip dhcp snooping information enable no ip dhcp snooping information enable
Parameter	none
Default	Option 82 function is disabled in DHCP Snooping by default.
Mode	Global Mode
Usage	Only by implementing this command, can DHCP Snooping add standard option 82 to DHCP request messages and forward the message. The format of option1 in option 82 (Circuit ID option) is standard vlan name plus physical port name, like “vlan1+ethernet1/0/12”. That of option2 in option 82 (remote ID option) is CPU MAC of the switch, like “00030f023301”. If a DHCP request message with option 82 options is received, DHCP Snooping will replace those options in the message with its own. If a DHCP reply message with option 82 options is received, DHCP Snooping will dump those options in the message and forward it.
Example	<pre>Enable option 82 function of DHCP Snooping on the switch. Switch#config Switch(config)#ip dhcp snooping enable Switch(config)#ip dhcp snooping binding enable Switch(config)#ip dhcp snooping information enable</pre>

ip dhcp snooping timeout quiet

Command	ip dhcp snooping timeout quiet <0-4294967295> no ip dhcp snooping timeout quiet
Parameter	<0-4294967295> time-out period

Default Mode	By default, the silent timeout period in DHCP Snooping is set to 0 seconds. Global Mode
Usage	Set the silent timeout period.
Example	Switch#config Switch(config)#ip dhcp snooping enable Switch(config)# ip dhcp snooping timeout quiet 6

ip dhcp snooping timeout detection

Command	ip dhcp snooping timeout detection <0-7200> no ip dhcp snooping timeout detection
Parameter	<0-7200> time-out period
Default	By default, the detection timeout period in DHCP Snooping is set to 3 seconds.
Mode	Global Mode
Usage	Configure the MAC hit detection timeout period. The default value is 3 seconds.
Example	Switch#config Switch(config)#ip dhcp snooping enable Switch(config)# ip dhcp snooping timeout detection 60 Switch(config)#

ip dhcp snooping mac-base control pass

Command	ip dhcp snooping mac-base control pass no ip dhcp snooping mac-base control pass
Parameter	none
Default	By default, the MAC authentication function in DHCP Snooping is disabled.
Mode	Global Mode
Usage	Enable control of DHCP messages based on MAC addresses.
Example	Enable the option82 function of DHCP snooping on the switch Switch#config Switch(config)#ip dhcp snooping enable Switch(config)# ip dhcp snooping mac-base control pass Switch(config)#

ip dhcp snooping blocked record enable

Command	ip dhcp snooping blocked record enable

	no ip dhcp snooping blocked record enable
Parameter	none
Default	By default, the function of recording illegal information in DHCP Snooping is disabled.
Mode	Global Mode
Usage	Enable the function of recording illegal information.
Example	Enable the option82 function of DHCP snooping on the switch Switch#config Switch(config)#ip dhcp snooping enable Switch(config)# ip dhcp snooping blocked record enable Switch(config)#

09-Multicast Protocol

1 IPv4 Multicast

access-list (Multicast Destination Control)

Command	access-list <6000-7999> (((add delete) profile-id WORD) ((deny permit) ip ((<source> <wildcard-bit>) (host-source <source-host-ip> [range <2-65535>]) any-source) ((<destination> <wildcard-bit>) (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)	
Parameter	<6000-7999>	destination control access-list number.
	add delete	add or delete the profile
	WORD	File id
	deny permit	deny or permit
	<source>	multicast source address
	<wildcard-bit>	Address wildcard
	<source-host-ip>	multicast source host address.
	<2-65535>	the range of multicast source host.
	<destination>	multicast destination address
	<destination-host-ip>	multicast destination host address
	<2-255>	the range of multicast destination host.
Default	none	
Mode	Global Mode	
Usage	ACL of Multicast destination control list item is controlled by specifical ACL number from 6000 to 7999, the command applies to configure this ACL. ACL of ip Multicast destination control only needs to configure source IP address and destination IP address controlled (group IP address), the configuration mode is basically the same to other ACLs, and use mask length to configure address range, and also specify a host address or all address. Remarkable, “all address” is 224.0.0.0/4 according to group IP address, not 0.0.0.0/0 in other access-list. And adding or deleting the profile-id can be used to change the multicast destination control ACL.	
Example	Switch#config Switch(config)#access-list 6000 permit ip 10.1.1.1 0.0.0.255 232.0.0.0 0.0.0.255 Switch(config)#access-list 6000 add profile-id 1 profile id 1 is not exist % Operation failed Switch(config)#	

access-list (Multicast Source Control)

Command	access-list <5000-5099> (deny permit) ip ((<source> <wildcard-bit>) (host <source-host-ip>) any-source) ((<destination> <wildcard-bit>) (host-destination <destination-host-ip>) any-destination) no access-list <5000-5099> (deny permit) ip ((<source> <wildcard-bit>) (host <source-host-ip>) any-source) ((<destination> <wildcard-bit>) (host-destination <destination-host-ip>) any-destination)	
Parameter	<5000-5099>	source control access-list number
	deny permit	deny or permit.
	<source>	multicast source address..
	<wildcard-bit>	address wildcard character.
	<source-host-ip>	multicast source host address.
	<destination>	multicast destination address.
	<destination-host-ip>	multicast destination host address.
Default	None	
Mode	Global Mode	
Usage	ACL of Multicast source control list item is controlled by specifical ACL number from 5000 to 5099, the command applies to configure this ACL. ACL of Multicast source control only needs to configure source IP address and destination IP address controlled (group IP address), the configuration mode is basically the same to other ACLs, and use wildcard character to configure address range, and also specify a host address or all address. Remarkable, “all address” is 224.0.0.0/4 according to group IP address, not 0.0.0.0/0 in other access-list.	
Example	Switch(config)#access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255	

ip multicast destination-control access-group

Command	ip multicast destination-control access-group <6000-7999> no ip multicast destination-control access-group <6000-7999>	
Parameter	<6000-7999>	destination-control access-list number.
Default	None	
Mode	Interface Configuration Mode	
Usage	The command is only working under global multicast destination-control enabled, after configuring the command, if IGMP-SPOOPING is enabled, for adding the interface to	

multicast group, and match configured access-list, such as matching: permit, the interface can be added, otherwise do not be added.

Example

```
Switch#config
Switch(config)#interface ethernet 1/0/4
Switch(config-if-ethernet1/0/4)#ip multicast destination-control access-group 6000
Switch(config-if-ethernet1/0/4)#
```

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>	
Parameter	<IPADDRESS/M	IP address and mask length
	>	
	<6000-7999>	Destination control access-list number
Default	None	
Mode	Global Mode	
Usage	The command is only working under global multicast destination-control enabled, after configuring the command, if IGMP-SPOOFING or IGMP is enabled, for adding the members to multicast group. If configuring multicast destination-control on specified net segment of transmitted igmp-report, and match configured access-list, such as matching permit, the interface can be added, otherwise do not be added. If relevant group or source in show ip igmp groups detail has been established before executing the command, it needs to execute clear ip igmp groups command to clear relevant groups in Admin mode.	
Example	Switch#config Switch(config)#ip multicast destination-control 10.1.1.0/24 access-group 6000	

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>	
Parameter	<1-4094>	VLAN ID
	<macaddr >	Transmitting source MAC address of IGMP-REPORT, the format is “xx-xx-xx-xx-xx-xx”;
	<6000-7999>	Destination-control access-list number.
Default	None	
Mode	Global Mode	
Usage	The command is only working under global multicast destination-control enabled, after	

configuring the command, if IGMP-SPOOPING is enabled, for adding the members to multicast group. If configuring multicast destination-control to source MAC address of transmitted igmp-report, and match configured access-list, such as matching: permit, the interface can be added, otherwise do not be added.

Example

```
Switch#config
Switch(config)#ip multicast destination-control 1 00-01-03-05-07-09 access-group 6000
```

ip multicast policy

Command	ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos <priority> no ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos	
Parameter	<IPADDRESS/M>	are multicast source address, mask length, destination address, and mask length separately.
	<priority>	specified priority, range from 0 to 7
Default	None	
Mode	Global Mode	
Usage	The command configuration modifies to a specified value through the switch matching priority of specified range multicast data packet, and the TOS is specified to the same value simultaneously. Carefully, the packet transmitted in UNTAG mode does not modify its priority.	
Example	Switch(config)#ip multicast policy 10.1.1.0/24 225.1.1.0/24 cos 7	

ip multicast source-control

Command	ip multicast source-control no ip multicast source-control	
Parameter	None	
Default	Disabled	
Mode	Global Mode	
Usage	The source control access-list applies to interface with only enabling global multicast source control, and configure to disabled global multicast source control without configuring source control access-list on every interface. After configuring the command, multicast data received from every interface does not have matching multicast source control list item, and then they will be thrown away by switches, namely only multicast data matching to PERMIT can be received and forwarded. 。	
Example	Switch(config)#ip multicast source-control	

ip multicast source-control access-group

Command	ip multicast source-control access-group <5000-5099> no ip multicast source-control access-group <5000-5099>	
Parameter	<5000-5099>	Source control access-list number.
Default	None	
Mode	Interface Configuration Mode	
Usage	The command configures with only enabling global multicast source control. After that, it will match multicast data message imported from the interface according to configured access-list, such as matching: permit, the message will be received and forwarded; otherwise the message will be thrown away.	
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)#	

ip multicast destination-control

Command	ip multicast destination-control	
Parameter	None	
Default	Disabled	
Mode	Global Mode	
Usage	Only after globally enabling the multicast destination control, the other destination control configuration can take effect; the destination access list can be applied to ports, VLAN-MAC and SIP. After configuring this command, IGMP-SNOOPING and IGMP will match according to the rules mentioned above when they try to add ports after receiving IGMP-REPORT.	
Example	Switch(config)#ip multicast destination-control	

profile-id (Multicast Destination Control Rule List)

Command	profile-id <1-50> (deny permit) ip ((<source> <wildcard-bit>) (host-source <source-host-ip> [range <2-65535>])) any-source} ((<destination> <wildcard-bit>) (host-destination <destination-host-ip> [range <2-65535>])) any-destination}

	(host-destination <destination-host-ip> [range <2-255>]) any-destination) no profile-id <1-50>	
Parameter	<1-50>	profile-id
	deny permit	deny or permit.
	<source>	multicast source address
	<wildcard-bit>	address wildcard character.
	<source-host-ip>	multicast source host address.
	<2-65535>	range of multicast source host
	<destination>	multicast destination address
	<destination-host-ip>	multicast destination host address
Default	<2-255>	range of multicast destination host.
	none	
Mode	Global Mode	
Usage	Profile-list of Multicast destination control list item is controlled by specific profile-id number from 1 to 50, the command applies to configure this profile to add it into the ACL for using. Multicast destination control only needs to configure source IP address and destination IP address controlled (group IP address), the configuration mode is basically the same to ACLs, and use mask length to configure address range, and also specify a host address or all address. Remarkable, “all address” is 224.0.0.0/4 according to group IP address, not 0.0.0.0/0 in other access-list.	
Example	switch(config)# profile-id 1 deny ip any-source host-destination 224.1.1.2	

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]	
Parameter	detail	expresses if it display information in detail or not
	<Interfacename>	interface name, or interface aggregation name, such as Ethernet1/0/1, port-channel 1 or ethernet1/0/1.
	<ipaddress>	IP address
	<vlan-id>	VLAN ID
	<mac-address>	Mac address
Default	None	
Mode	Admin Mode and Global Mode	
Usage	The command displays multicast destination control rules of configuration including detail option, and access-list information applied in detail.	
Example	Switch#show ip multicast destination-control ip multicast destination-control is enabled	

multicast destination-control access-group 6000 used on interface Ethernet1/0/4

show ip multicast destination-control access-list

Command	show ip multicast destination-control access-list show ip multicast destination-control access-list <6000-7999>
Parameter	<6000-7999> access-list number.
Default	None
Mode	Admin Mode and Global Mode
Usage	The command displays destination control multicast access-list of configuration.
Example	Switch#show ip multicast destination-control access-list access-list 6000 permit ip 10.1.1.1 0.0.0.255 232.0.0.0 0.0.0.255

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>
Parameter	<1-50> profile-id
Default	None
Mode	Admin Mode and Global Mode
Usage	This command can show the configured destination control profile rule list.
Example	Switch#show l2-address-table multicast vlan 1 Vlan Address Insert Type Creator Ports -----

show ip multicast policy

Command	show ip multicast policy
Parameter	None
Default	None
Mode	Admin Mode and Global Mode
Usage	The command displays multicast policy of configuration

Example	Switch#show ip multicast policy ip multicast-policy 10.1.1.0/24 225.0.0.0/8 cos 5

show ip multicast source-control

Command	show ip multicast source-control [detail] show ip multicast source-control interface { IFNAME ethernet < Interfacename > } [detail]
Parameter	detail expresses if it displays information in detail.
	<Interfacename> interface name, such as ethernet 1/0/1 or ethernet1/0/1.
Default	None
Mode	Admin Mode and Global Mode
Usage	The command displays multicast source control rules of configuration, including detail option, and access-list information applied in detail.
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

show ip multicast source-control access-list

Command	show ip multicast source-control access-list show ip multicast source-control access-list <5000-5099>
Parameter	<5000-5099> access-list number
Default	None
Mode	Admin Mode and Global Mode
Usage	The command displays source control multicast access-list of configuration
Example	Switch#show 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

clear ip igmp snooping vlan

Command	clear ip igmp snooping vlan <1-4094> groups {A.B.C.D authentication-port [IFNAME ethernet <interface-list> port-channel < interface-name>]}

Parameter	<1-4094>	VLAN ID
	A.B.C.D	group address.
	<interface-list>	Interface name
	< interface-name>	port-channel name
Default	None	
Mode	Admin Configuration Mode	
Usage	Use show command to check the deleted group record.	
Example	Switch#clear ip igmp snooping vlan 1 groups	

clear ip igmp snooping vlan <1-4094> mrouter-port

Command	clear ip igmp snooping vlan <1-4094> mrouter-port [ethernet] IFNAME	
Parameter	<1-4094>	VLAN ID
	IFNAME	port name
Default	None	
Mode	Admin Configuration Mode	
Usage	use show command to check the deleted mrouter port of the specific VLAN. 。	
Example	Delete mrouter port in vlan 1.	
	Switch#clear ip igmp snooping vlan 1 mrouter-port	

ip igmp snooping

Command	ip igmp snooping no ip igmp snooping	
Parameter	none	
Default	IGMP Snooping is disabled by default.	
Mode	Global Mode	
Usage	Use this command to enable IGMP Snooping, that is permission every VLAN config the function of IGMP snooping. The “ no ip igmp snooping ” command disables this function.	
Example	Enable IGMP Snooping	
	Switch#config	
	Switch(config)#ip igmp snooping	
	Switch(config)#	

ip igmp snooping proxy

Command	ip igmp snooping proxy { query <cr>} no ip igmp snooping proxy { query <cr>}
Parameter	none
Default	Enable
Mode	Global Mode
Usage	Enable IGMP Snooping proxy function, the no command disables the function.
Example	Switch#config Switch(config)#no ip igmp snooping proxy Switch(config)#

ip igmp snooping vlan

Command	ip igmp snooping vlan <vlan-id> no ip igmp snooping vlan <vlan-id>
Parameter	<vlan-id> VLAN ID
Default	IGMP Snooping is disabled by default.
Mode	Global Mode
Usage	To configure IGMP Snooping on specified VLAN, the global IGMP Snooping should be first enabled. Disable IGMP Snooping on specified VLAN with the “ no ip igmp snooping vlan <vlan-id> ” command.
Example	Enable IGMP Snooping for VLAN 100 in Global Mode. Switch#config Switch(config)#ip igmp snooping vlan 100

ip igmp snooping vlan immediate-leave

Command	ip igmp snooping vlan <vlan-id> immediate-leave no ip igmp snooping vlan <vlan-id> immediate-leave
Parameter	<vlan-id> VLAN ID
Default	This function is disabled by default.
Mode	Global Mode

Usage	Enable immediate-leave function of the IGMP Snooping in specified VLAN; the“no” form of this command disables the immediate-leave function of the IGMP Snooping
Example	Enable the IGMP Snooping fast leave function for VLAN 100. Switch#config Switch(config)#ip igmp snooping vlan 100 immediate-leave

ip igmp snooping vlan <id> immediately-leave mac-based

Command	ip igmp snooping vlan <vlan-id> immediately-leave mac-based no ip igmp snooping vlan <vlan-id> immediately-leave mac-based
Parameter	<vlan-id> VLAN ID
Default	This function is disabled by default.
Mode	Global Mode
Usage	Configure this command to delete the existed igmp snooping table entries according to the source mac in leave packet when the switch which is enabled the igmp snooping function receives the leave packet. Only when the received the port, source mac and multicast group of the leave packet are the same as the port, host mac and multicast group of the existed igmp snooping table entry, the snooping table entry can be deleted. If this command is not configured, delete the existed igmp snooping table entry according to the port and multicast group of the leave packet. Configure the immediately-leave under the same vlan at the same time to make this command effective. In this time, deal with it according to the host mac of the port.
Example	Use the following configuration when delete the table entry according to the host mac of the port. Switch#config Switch(config)#ip igmp snooping vlan 12 immediately-leave Switch(config)#ip igmp snooping vlan 12 immediately-leave mac-based

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
Parameter	<vlan-id> is ID number of the VLAN, ranging is <1-4094>
Default	VLAN is not as the IGMP Snooping layer 2 general querier.
Mode	Global Mode
Usage	It is recommended to configure a layer 2 general querier on a segment. IGMP Snooping function will be enabled by this command if not enabled on this VLAN before configuring this command, IGMP Snooping function will not be disabled when disabling

the layer 2 general querier function. This command is mainly for sending general queries regularly to help switches within this segment learn mrouter ports.

Comment: There are three paths IGMP snooping learn mrouter

1 Port receives the IGMP query messages

2 Port receives multicast protocol packets, and supports DVMRP, PIM

3 Static configured port

Example

Switch(config)#ip igmp snooping vlan 1 l2-general-querier

ip igmp snooping vlan l2-general-querier-source

Command `ip igmp snooping vlan <vlan-id> l2-general-querier-source <A.B.C.D>`
no ip igmp snooping vlan <vlanid> l2-general-querier-source

Parameter `<vlan-id>` VLAN ID
`<A.B.C.D>` `<A.B.C.D>` is the source address of the query operation

Default 0.0.0.0

Mode Global Mode

Usage It is not supported on Windows 2000/XP to query with the source address as 0.0.0.0. So the layer 2 query source address configuration does not function. The client will stop sending requesting datagrams after one is sent. And after a while, it can not receive multicast datagrams.

Example Switch(config)#ip igmp snooping vlan 2 l2-general-query-source 192.168.1.2

ip igmp snooping vlan l2-general-querier-version

Command `ip igmp snooping vlan <vlanid> l2-general-querier-version <version>`

Parameter `<vlan-id>` VLAN ID
`<version>` version number, limited to <1-3>.

Default version 3

Mode Global Mode

Usage When the switch is connected to V1 and V2 capable environment, and for VLAN which has source of layer 2 query configuration, the VLAN can be queried only if the version number has been specified. This command is used to query the layer 2 version number.

Example Switch(config)#ip igmp snooping vlan 2 l2-general-querier-version 2

ip igmp snooping vlan limit

Command	ip igmp snooping vlan <vlanid> limit {group <g_limit> source <s_limit>} no ip igmp snooping vlan <vlan-id> limit	
Parameter	<vlan-id>	VLAN ID
	<g_limit>	<1-65535>, max number of groups joined
	<s_limit>	<1-65535>, max number of source entries in each group, consisting of include source and exclude source.
Default	Maximum 50 groups by default, with each group capable with 40 source entries.	
Mode	Global Mode	
Usage	When number of joined group reaches the limit, new group requesting for joining in will be rejected for preventing hostile attacks. To use this command, IGMP snooping must be enabled on VLAN. The “no” form of this command restores the default other than set to “no limit”. For the safety considerations, this command will not be configured to “no limit”. It is recommended to use default value and if layer 3 IGMP is in operation, please make this configuration in accordance with the IGMP configuration as possible.	
Example	Switch(config)#ip igmp snooping vlan 2 limit group 300	

ip igmp snooping vlan interface (ethernet | port-channel) IFNAME limit

Command	ip igmp snooping vlan <vlanid> interface (ethernet port-channel) IFNAME limit {group <g_limit> source <s_limit>} strategy (replace drop) no ip igmp snooping vlan <1-4094> interface (ethernet port-channel) IFNAME limit group source strategy	
Parameter	<vlan-id>	VLAN ID
	IFNAME	Interface name
	<g_limit>	<1-65535>, The maximum number of groups allowed joining
	<s_limit>	<1-65535>, The maximum number of source table entries in each group, including include source and exclude source.
	replace	Replace the group and source information
	drop	Drop the new group and source information
Default	There is no limitation as default.	
Mode	Global Mode	
Usage	When the number of the groups joined under the port or the number of sources in this group exceeds the limit, it will be dealt according to the configured strategy. If it is drop, drop the new group and source information; if it is replace, find a dynamic group and source from the port to conduct deleting and replacing, and then add the new group and source information. The premise of using this command is that this VLAN is enabled IGMP Snooping function. No command configures as “no limitation”.	

Example	Switch(config)#ip igmp snooping vlan 2 interface ethernet 1/0/11 limit group 300 source 200 strategy replace

ip igmp snooping vlan mrouter-port interface

Command	ip igmp snooping vlan <vlanid> mrouter-port interface [ehternet port-channel] <ifname> no ip igmp snooping vlan <vlan-id> mrouter-port interface[<ehternet> <port-channel>] <ifname>
Parameter	<vlan-id> VLAN ID IFNAME Name of interface
Default	No static mrouter port on VLAN by default.
Mode	Global Mode
Usage	When a port is a static mrouter port while also a dynamic mrouter port, it should be taken as a static mrouter port. Deleting static mrouter port can only be realized by the no command.
Example	Switch(config)#ip igmp snooping vlan 2 mrouter-port interface ethernet1/0/13

ip igmp snooping vlan mrouter-port learnpim

Command	ip igmp snooping vlan <vlanid> mrouter-port learnpim no ip igmp snooping vlan <vlan-id> mrouter-port learnpim
Parameter	<vlan-id> VLAN ID
Default	Enable
Mode	Global Mode
Usage	Enable the function that the specified VLAN learns mrouter-port (according to pim packets). After a port received pim packets, it will be set to mrouter port for implementing the automatic learning.
Example	Disable the function that vlan 100 learns mrouter-port (according to pim packets). Switch(config)#no ip igmp snooping vlan 100 mrouter-port learnpim

ip igmp snooping vlan mrpt

Command	ip igmp snooping vlan <vlanid> mrpt <value>

Parameter	no ip igmp snooping vlan <vlan-id> mrpt	
	<vlan-id>	VLAN ID, ranging between <1-4094>
	<value>	mrouter port survive period, ranging between <1-65535>seconds
Default	255s	
Mode	Global Mode	
Usage	This command validates on dynamic mrouter ports but not on mrouter port. To use this command, IGMP Snooping of this VLAN should be enabled previously.	
Example	Switch(config)#ip igmp snooping vlan 2 mrpt 100	

ip igmp snooping vlan query-interval

Command	ip igmp snooping vlan <vlanid> query-interval <value> no ip igmp snooping vlan <vlan-id> query-interval	
Parameter	<vlan-id>	VLAN ID, ranging between <1-4094>
	<value>	query interval, ranging between <1-65535>seconds
Default	125s	
Mode	Global Mode	
Usage	It is recommended to use the default settings. Please keep this configure in accordance with IGMP configuration as possible if layer 3 IGMP is running.	
Example	Switch(config)#ip igmp snooping vlan 2 query-interval 130	

ip igmp snooping vlan query-mrsp

Command	ip igmp snooping vlan <vlanid> query-mrsp <value> no ip igmp snooping vlan <vlan-id> query-mrspt	
Parameter	<vlan-id>	VLAN ID, ranging between <1-4094>
	<value>	ranging between <1-25> seconds
Default	10s	
Mode	Global Mode	
Usage	It is recommended to use the default settings. Please keep this configure in accordance with IGMP configuration as possible if layer 3 IGMP is running.	
Example	Switch(config)#ip igmp snooping vlan 2 query-mrsp 18	

ip igmp snooping vlan query-robustness

Command	ip igmp snooping vlan <vlanid> query-robustness <value> no ip igmp snooping vlan <vlan-id> query-robustness	
Parameter	<vlan-id>	VLAN ID
	<value>	ranging between <2-10>
Default	2s	
Mode	Global Mode	
Usage	It is recommended to use the default settings. Please keep this configure in accordance with IGMP configuration as possible if layer 3 IGMP is running.	
Example	Switch(config)#ip igmp snooping vlan 2 query- robustness 3	

ip igmp snooping vlan report source-address

Command	ip igmp snooping vlan <vlanid> report source-address {A.B.C.D cisco mode} no ip igmp snooping vlan <vlan-id> report source-address {cisco mode <cr>}	
Parameter	<vlan-id>	VLAN ID
	<A.B.C.D>	IP address, can be 0.0.0.0
Default	Disabled	
Mode	Global Mode	
Usage	Default configuration is recommended here. If IGMP snooping needs to be configured, the source address for forwarded IGMP messages can be 0.0.0.0. If it is required by the upstream that IGMP messages should use the same network address, the source address of IGMP messages should be configured to be the same with upstream.。	
Example	Switch(config)#ip igmp snooping vlan 2 report source-address 10.1.1.1	

ip igmp snooping vlan specific-query-mrsp

Command	ip igmp snooping vlan <vlanid> specific-query-mrsp <value> no ip igmp snooping vlan <vlan-id> specific-query-mrspt	
Parameter	<vlan-id>	specific VLAN ID, the range from 1 to 4094
	<value>	the maximum query response time, unit is second, the range from 1 to 25, default value is 1
Default	Enable	

Mode	Global Mode
Usage	After enable vlan snooping in global mode, input this command to configure the maximum query response time of the specific group.
Example	Configure/cancel the specific-query-mrsp of vlan3 as 2s. Switch(config)#ip igmp snooping vlan 3 specific-query-mrsp 2 Switch(config)#no ip igmp snooping vlan 3 specific-query-mrsp

ip igmp snooping vlan static-group

Command	ip igmp snooping vlan <vlanid> 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>						
Parameter	<table> <tr> <td><vlan-id></td><td>VLAN ID, ranging between <1-4094></td></tr> <tr> <td><A.B.C.D></td><td>address of group or source</td></tr> <tr> <td><IFNAME></td><td>Name of interface</td></tr> </table>	<vlan-id>	VLAN ID, ranging between <1-4094>	<A.B.C.D>	address of group or source	<IFNAME>	Name of interface
<vlan-id>	VLAN ID, ranging between <1-4094>						
<A.B.C.D>	address of group or source						
<IFNAME>	Name of interface						
Default	None						
Mode	Global Mode						
Usage	Configure static-group on specified port of the VLAN. The no form of the command cancels this configuration. When a group is a static while also a dynamic group, it should be taken as a static group. Deleting static group can only be realized by 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						

ip igmp snooping vlan suppression-query-time

Command	ip igmp snooping vlan <vlanid> suppression-query-time <value> no ip igmp snooping vlan <vlan-id> suppression-query-time				
Parameter	<table> <tr> <td><vlan-id></td><td>VLAN ID, ranging between <1-4094></td></tr> <tr> <td><value></td><td>ranging between<1-65535> seconds</td></tr> </table>	<vlan-id>	VLAN ID, ranging between <1-4094>	<value>	ranging between<1-65535> seconds
<vlan-id>	VLAN ID, ranging between <1-4094>				
<value>	ranging between<1-65535> seconds				
Default	255s				
Mode	Global Mode				
Usage	Configure the suppression query time. The “no ip igmp snooping vlan <vlan-id> suppression-query-time” command restores to the default value. This command can only be configured on L2 general querier. The Suppression-query-				

time refers to the period of suppression state in which the querier enters when receives query from the layer 3 IGMP in the segments.

Example

```
Switch(config)#ip igmp snooping vlan 2 suppression-query-time 270
```

show ip igmp snooping

Command	show ip igmp snooping [vlan <vlan-id>]		
Parameter	<vlan-id>	VLAN ID	
Default	none		
Mode	Admin Configuration Mode		
Usage	If no VLAN number is specified, it will show whether global IGMP Snooping switch is on, which VLAN is configured with l2-general-querier function, and if a VLAN number is specified, detailed IGMP messages for this VLAN will be shown.		
Example	1. Show IGMP Snooping summary messages 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		
	Displayed Information	Explanation	
	Global igmp snooping status	Whether the global igmp snooping switch on the switch is on	
	L3 multicasting	whether the layer 3 multicast protocol of the switch is running	
	Igmp snooping is turned on for vlan 1(querier)	which VLANs on the switch is enabled with igmp snooping function, whether they are l2-general-querier	
2.Display the IGMP Snooping summary messages of vlan1.			
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) Ethernet1/0/8 00:04:14 V2			
(192.168.0.2) Ethernet1/0/8 00:04:14 V2			

Igmp snooping vlan 1 mrouter port

Note:"!"-static mrouter port

!Ethernet1/0/2

Displayed Information	Explanation
Igmp snooping L2 general querier	Whether the VLAN enables l2-general-querier function and show whether the querier state is could-query or suppressed
Igmp snooping query-interval	Query interval of the VLAN
Igmp snooping max reponse time	Max response time of the VLAN
Igmp snooping robustness	IGMP Snooping robustness configured on the VLAN
Igmp snooping mrouter port keep-alive time	keep-alive time of dynamic mrouter of the VLAN
Igmp snooping query-suppression time	Suppression timeout of VLAN when as l2-general-querier
IGMP Snooping Connect Group Membership	Group membership of this VLAN, namely the correspondence between ports and (S,G)
Igmp snooping vlan 1 mrouter port	mrouter port of the VLAN, including both static and dynamic

clear ipv6 mld snooping vlan

Command	clear ipv6 mld snooping vlan <1-4094> groups [X:X::X:X]				
Parameter	<table><tr><td><1-4094></td><td>VLAN ID</td></tr><tr><td>[X:X::X:X]</td><td>specific group address</td></tr></table>	<1-4094>	VLAN ID	[X:X::X:X]	specific group address
<1-4094>	VLAN ID				
[X:X::X:X]	specific group address				
Default	None				
Mode	Admin Configuration Mode				
Usage	Delete the group record of the specific VLAN. Use show command to check the deleted group record				
Example	Delete all groups. Switch#clear ipv6 mld snooping vlan 1 groups				

clear ipv6 mld snooping vlan <1-4094> mrouter-port

Command	clear ipv6 mld snooping vlan <1-4094> mrouter-port [ethernet] IFNAME

Parameter	<1-4094>	VLAN ID
	IFNAME	port name
Default	None	
Mode	Admin Configuration Mode	
Usage	Delete the mrouter port of the specific VLAN. Use show command to check the deleted group record.	
Example	Delete the mrouter port in vlan 1. Switch#clear ipv6 mld snooping vlan 1 mrouter-port	

ipv6 mld snooping

Command	ipv6 mld snooping no ipv6 mld snooping
Parameter	None
Default	MLD Snooping disabled on the switch by default
Mode	Global Mode
Usage	Enable global MLD Snooping on the switch, namely allow every VLAN to be configured with MLD Snooping; the “no” form of this command will disable MLD Snooping on all the VLANs as well as the global MLD snooping
Example	Enable MLD Snooping under global mode. Switch(config)#ipv6 mld snooping

ipv6 mld snooping vlan

Command	ipv6 mld snooping vlan <vlan-id> no ipv6 mld snooping vlan <vlan-id>
Parameter	<vlan-id> VLAN ID, with a valid range of <1-4094>.
Default	MLD Snooping disabled on VLAN by default
Mode	Global Mode
Usage	Enable MLD Snooping on specified VLAN; the “no” form of this command disables MLD Snooping on specified VLAN. To configure MLD snooping on certain VLAN, the global MLD snooping should be first enabled. Disable MLD snooping on specified VLAN with the no ipv6 mld snooping vlan vid command
Example	Enable MLD snooping on VLAN 100 under global mode. Switch(config)#ipv6 mld snooping vlan 100

ipv6 mld snooping vlan immediate-leave

Command	ipv6 mld snooping vlan <vlan-id> immediate-leave no ipv6 mld snooping vlan <vlan-id> immediate-leave
Parameter	<vlan-id> VLAN ID, with valid range of <1-4094>.
Default	Disabled by default
Mode	Global Mode
Usage	Enable immediate-leave function of the MLD protocol in specified VLAN; the “no” form of this command disables the immediate-leave function of the MLD protocol Enabling the immediate-leave function of the MLD protocol will hasten the process the port leaves one multicast group, in which the specified group query of the group will not be sent and the port will be directly deleted.
Example	Enable the MLD immediate-leave function on VLAN 100. Switch(config)#ipv6 mld snooping vlan 100 immediate-leave

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
Parameter	<vlan-id> VLAN ID, with a valid range of <1-4094>
Default	VLAN is not a MLD Snooping L2 general querier by default.
Mode	Global Mode
Usage	It is recommended to configure an L2 general querier on a segment. If before configure with this command, MLD snooping is not enabled on this VLAN, this command will no be executed. When disabling the L2 general querier function, MLD snooping will not be disabled along with it. Main function of this command is sending general queries periodically to help the switches within this segment learn mrouter port. Comment: There are three ways to learn mrouter port in MLD Snooping: 1. The port which receives MLD query messages 2. The port which receives multicast protocol packets and support PIM 3. The port statically configured.
Example	Set VLAN 100 to L2 general querier. Switch(config)#ipv6 mld snooping vlan 100 l2-general-querier

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	
Parameter	<vlan-id>	VLAN ID, the valid range is <1-4094>
	<g_limit>	max number of groups joined, range: 1-65535
	<s_limit>	max number of source entries in each group, consisting of include source and exclude source, range: 1-65535
Default	Maximum 50 groups by default, with each group capable with 40 source entries.	
Mode	Global Mode	
Usage	When number of joined group reaches the limit, new group requesting for joining in will be rejected for preventing hostile attacks. To use this command, MLD snooping must be enabled on VLAN. The “no” form of this command restores the default other than set to “no limit”. For the safety considerations, this command will not be configured to “no limit”. It is recommended to use default value and if layer 3 MLD is in operation, please make this configuration in accordance with the MLD configuration as possible.	
Example	Switch(config)#ipv6 mld snooping vlan 2 limit group 300	

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>	
Parameter	<vlan-id>	VLAN ID,the valid range is<1-4094>
	<ifname>	Name of interface
Default	When a port is made static and dynamic mrouter port at the same time, it's the static mrouter properties is preferred. Deleting the static mrouter port can only be done with the “no” form of this command	
Mode	Global Mode	
Usage	Set the static mrouter port of the VLAN; the “no” form of this command cancels the configuration.	
Example	Switch(config)#ipv6 mld snooping vlan 2 mrouter-port interface ethernet1/0/13	

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	
Parameter	<vlan-id>	VLAN ID, ranging from 1 to 4094.

Default	Enable
Mode	Global Mode
Usage	Enable the function that the specified VLAN learns mrouter-port (according to pimv6 packets). After a port received pimv6 packets, it will be set to mrouter port for implementing the automatic learning.
Example	Disable the function that vlan 100 learns mrouter-port (according to pimv6 packets). Switch(config)#ipv6 mld snooping vlan 2 mrouter-port learnpim6

ipv6 mld snooping vlan mrpt

Command	ipv6 mld snooping vlan <vlan-id> mrpt <value> no ipv6 mld snooping vlan <vlan-id> mrpt	
Parameter	<vlan-id>	VLAN ID, the valid range is <1-4094>
	<value>	mrouter port keep-alive time with a valid range of <1-65535> secs.
Default	255s	
Mode	Global Mode	
Usage	Configure the keep-alive time of the mrouter port. This configuration is applicable on dynamic mrouter port, but not on static mrouter port. To use this command, MLD snooping must be enabled on the VLAN.	
Example	Switch(config)#ipv6 mld snooping vlan 2 mrpt 100	

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	
Parameter	<vlan-id>	VLAN ID, the valid range is <1-4094>
	<value>	query interval, valid range: <1-65535>secs.
Default	125s	
Mode	Global Mode	
Usage	Configure the query interval. It is recommended to use default value and if layer 3 MLD is in operation, please make this configuration in accordance with the MLD configuration as possible. 。	
Example	Switch(config)#ipv6 mld snooping vlan 2 query-interval 130	

ipv6 mld snooping vlan query-mrsp

Command	ipv6 mld snooping vlan <vlan-id> query-mrsp <value> no ipv6 mld snooping vlan <vlan-id> query-mrspt	
Parameter	<vlan-id>	VLAN ID,the valid range is<1-4094>
	<value>	the valid range is <1-25> secs .
Default	10s	
Mode	Global Mode	
Usage	Configure the maximum query response period. The “no” form of this command restores the default value.	
	It is recommended to use default value and if layer 3 MLD is in operation, please make this configuration in accordance with the MLD configuration as possible.	
Example	Switch(config)#ipv6 mld snooping vlan 2 query-mrsp 18	

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	
Parameter	<vlan-id>	VLAN ID,the valid range is <1-4094>
	<value>	the valid range is <2-10>.
Default	2s	
Mode	Global Mode	
Usage	Configure the query robustness; the “no” form of this command restores to the default value.	
	It is recommended to use default value and if layer 3 MLD is in operation, please make this configuration in accordance with the MLD configuration as possible.	
Example	Switch(config)#ipv6 mld snooping vlan 2 query- robustness 3	

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>	
Parameter	<vlan-id>	VLAN ID, range: 1-4094
	<X:X::X:X>	The address of group or source.
	<IFNAME>	Name of interface
Default	None	

Mode	Global Mode
Usage	Configure static-group on specified port of the VLAN. The no form of the command cancels this configuration. When a group is a static while also a dynamic group, it should be taken as a static group. Deleting static group can only be realized by the no form of the command.
Example	Switch(config)#ipv6 mld snooping vlan 2 static-group ff1e::15 source 2000::1 interface ethernet 1/0/1

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	
Parameter	<vlan-id>	VLAN ID, valid range: <1-4094>
	<value>	valid range: <1-65535>secs.
Default	255s	
Mode	Global Mode	
Usage	Configure the suppression query time; the “no” form of this command restores the default value. This command can only be configured on L2 general querier. The Suppression-query-time represents the period the suppression state maintains when general querier receives queries from layer 3 MLD within the segment. To use this command, the query-intervals in different switches within the same segment must be in accordance. It is recommended to use the default value.	
Example	Switch(config)#ipv6 mld snooping vlan 2 suppression-query-time 270	

show ipv6 mld snooping

Command	show ipv6 mld snooping [vlan <vlan-id>]	
Parameter	<vlan-id>	VLAN ID
Default	none	
Mode	Admin Configuration Mode	
Usage	If no VLAN number is specified, it will show whether the global MLD snooping is enabled and layer 3 multicast protocol is running, as well as on which VLAN the MLD Snooping is enabled and configured l2-general-querier. If a VLAN number is specified, the detailed MLD Snooping messages of this VLAN will be displayed.	
Example	1.Summary of the switch MLD snooping 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

Displayed Information	Explanation
Global mld snooping status	Whether or not the global MLD Snooping is enabled on the switch
L3 multicasting	Whether or not the layer 3 multicast protocol is running on the switch.
Mld snooping is turned on for vlan 1(querier)	On which VLAN of the switch is enabled MLD Snooping, if the VLAN are l2-general-querier.

2.Display the detailed MLD Snooping information of vlan1

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 Source, (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

Displayed Information	Explanation
Mld snooping L2 general querier	whether or not l2-general-querier is enabled on VLAN, the querier display status is set to could-query or suppressed
Mld snooping query-interval	Query interval time of the VLAN
Mld snooping max reponse time	Max response time of this VLAN
Mld snooping robustness	Robustness configured on the VLAN
Mld snooping mrouter port keep-alive time	Keep-alive time of the dynamic mrouter on this VLAN
Mld snooping query-suppression time	timeout of the VLAN as l2-general-querier at suppressed status.
MLD Snooping	Group membership of the VLAN, namely the

Connect Membership	Group	correspondence between the port and (S,G)
Mld snooping	vlan 1	Mrouter port of the VLAN, including both static and dynamic.
mrouter port		

multicast-vlan

Command	multicast-vlan no multicast-vlan
Parameter	none
Default	Multicast VLAN function not enabled by default.
Mode	VLAN Configuration Mode
Usage	Enable multicast VLAN function on a VLAN; the “no” form of this command disables the multicast VLAN function. The multicast VLAN function can not be enabled on Private VLAN. To disabling the multicast VLAN function of the VLAN, configuration of VLANs associated with the multicast VLAN should be deleted. Note that the default VLAN can not be configured with this command and only one multicast VLAN is allowed on a switch.
Example	<pre>Switch(config)#vlan 2 Switch(config-vlan2)# multicast-vlan</pre>

multicast-vlan association

Command	multicast-vlan association <vlan-list> no multicast-vlan association <vlan-list>
Parameter	<vlan-list> <vlan-list> the VLAN ID list associated with multicast VLAN. Each VLAN can only be associated with one multicast VLAN and the association will only succeed when every VLAN listed in the VLAN ID table exists.
Default	The multicast VLAN is not associated with any VLAN by default.
Mode	VLAN Configuration Mode
Usage	Associate several VLANs with a multicast VLAN; the “no” form of this command cancels the association relations. After a VLAN is associated with the multicast VLAN, when there comes the multicast order in the port of this VLAN, then the multicast data will be sent from the multicast VLAN to this port, so to reduce the data traffic. The VLAN associated with the multicast VLAN should not be a Private VLAN. A VLAN can only be associated with another

VLAN 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
```

multicast-vlan association interface

Command	multicast-vlan association interface (ethernet port-channel) IFNAME out-tag <tag-id> no multicast-vlan association interface (ethernet port-channel) IFNAME	
Parameter	IFNAME	The name of the ethernet port or port-channel port
	<tag-id>	Specify vlan tag of the multicast data forwarded by the associated port, only the tag of the associated port allows the multicast VLAN, the tag-id takes effect. Its range from 1 to 4094.
Default	None	
Mode	VLAN Configuration Mode	
Usage	Associate the specified port with the multicast VLAN, so the associated ports are able to receive the multicast flow. The no command cancels the association between the ports and the multicast VLAN. 1. 'associated VLAN' and 'associated port' of the multicast VLAN are absolute, they do not affect each other when happening the cross. 2. The port of the aggregation member cannot be associated, but the associated port is able to be added to port-group and cancelling the association. 3. The configured port type includes port-channel port or ethernet port and the port is only configured as ACCESS mode. 4. The port (it will be associated) cannot belong to the multicast VLAN, in the same way, the associated port cannot be divided in multicast VLAN. 5. When the associated port mode is set as non ACCESS mode, the mode cannot be changed.	
Example	<pre>Switch(config)#vlan 2 Switch(config-vlan2)# multicast-vlan association interface ethernet 1/2 Switch(config-vlan2)#multicast-vlan association interface port-channel 2 Switch(config-vlan2)#no multicast-vlan association interface ethernet 1/2 Switch(config-vlan2)#no multicast-vlan association interface port-channel 2</pre>	

multicast-vlan mode

Command	multicast-vlan mode {dynamic compatible} no multicast-vlan mode {dynamic compatible}	
Parameter	dynamic	dynamic mode

Default	compatible	compatible mode
	Neither of the two modes	
Mode	VLAN Configuration Mode	
Usage	This command is used to configure the two modes of the multicast vlan; the no command cancels this configuration.	
	When configured as dynamic mode, the mrouter port will not be added automatically any more when issuing the multicast entries; when configured as compatible mode, the report packet will be not transmitted to the mrouter port any more. When it is not configured as default, the mrouter port will be added when issuing the multicast entries and the report packet will be transmitted to the mrouter port when it is received.	
Example	Switch(config)#vlan 2	
	Switch(config-vlan2)# multicast vlan mode dynamic	

switchport association multicast-vlan

Command	switchport association multicast-vlan <vlan-id> out-tag <tag-id> no switchport association multicast-vlan <vlan-id>	
Parameter	<vlan-id>	The multicast VLAN associates with the port. Each port can only be associated with one multicast VLAN, and the association will be successful only when the multicast VLAN is existent.
	<tag-id>	Specify vlan tag of the multicast data forwarded by the associated port, only the tag of the associated port allows the multicast VLAN, the tag-id takes effect. Its range from 1 to 4094.
Default	The port is not associated with any multicast VLAN by default.	
Mode	Interface Configuration Mode	
Usage	Associate a port with the specified multicast VLAN; the no command cancels the association.	
	After a port is associated with the multicast VLAN, when there comes the multicast order in the port, then the multicast data will be sent from the multicast VLAN to this port, so to reduce the data traffic. If the associated port is set as trunk port and allows the multicast VLAN, the multicast traffic with the specified vlan tag will be forwarded. The port can only be associated with the multicast VLAN after the multicast VLAN is enabled.	
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	

2 IGMP

show ip mroute

Command	show ip mroute [<GroupAddr> [<SourceAddr>]]	
	show IPv4 software multicast route table.	
Parameter	GroupAddr	show the multicast entries relative to this Group address
	SourceAddr	show the multicast route entries relative to this source address
Default	None。	
Mode	Admin mode and global mode。	
Usage		
Example	show all entries of multicast route 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

Displayed information	Explanation
Name	the name of interface
Index	the index number of interface
State	the state of interface
The total matched ipmr active mfc entries	The total matched active IP multicast route mfc (multicast forwarding cache) entries
Unresolved ipmr entries	unresolved ip multicast route entries
Group	the destination address of the entries
Origin	the source address of the entries
Iif	ingress interface of the entries
Wrong	packets received from the wrong interface
Oif	egress interface of the entries
TTL	the value of TTL

show ipv6 mroute

Command	show ipv6 mroute [<GroupAddr> [<SourceAddr>]]	
	show IPv6 software multicast route table.	
Parameter	GroupAddr	show the multicast entries relative to this Group address
	SourceAddr	show the multicast route entries relative to this source address
Default	None。	
Mode	Admin mode and global mode。	
Usage		
Example	show all entries of IPv6 multicast route 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 lif 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

```

Displayed information	Explanation
Name	the name of interface
Index	the index number of interface
State	the state of interface
The total matched ipmr active mfc entries	The total matched active IP multicast route mfc (multicast forwarding cache) entries
Unresolved ipmr entries	unresolved ip multicast route entries
Group	the destination address of the entries
Origin	the source address of the entries
lif	ingress interface of the entries
Wrong	packets received from the wrong interface
Oif	egress interface of the entries
TTL	the value of TTL

clear ip igmp group

Command **clear ip igmp group [A.B.C.D | IFNAME]**

Delete the group record of the specific group or interface.

Parameter	A.B.C.D	the specific group address
	IFNAME	the specific interface.

Default

Mode Admin Configuration Mode

Usage Use show command to check the deleted group record.

Example	Switch#clear ip igmp group

debug igmp event

Command	debug igmp event no debug igmp event
	Enable debugging switch of IGMP event; the “ no debug igmp event ” command disenables the debugging switch
Parameter	
Default	Disabled
Mode	Admin Mode
Usage	Enable debugging switch if querying 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

debug igmp packet

Command	debug igmp packet no debug igmp packet
	Enable debugging switch of IGMP message information; the “no debug igmp packet” command disenables the debugging switch
Parameter	

Default	Disabled
Mode	Admin Mode
Usage	Enable the debugging switch if querying IGMP message information.
Example	<pre>Switch# debug igmp packet igmp packet debug is on Switch #02:17:38:58: IGMP: Send membership query on dvmrp2 for 0.0.0.0 02:17:38:58: IGMP: Received membership query on dvmrp2 from 192.168.1.11 for 0.0.0.0 02:17:39:26: IGMP: Send membership query on vlan1 for 0.0.0.0 02:17:39:26: IGMP: Received membership query on dvmrp2 from 192.168.1.11 for 0.0.0.0</pre>

ip igmp access-group

Command	ip igmp access-group {<acl_num acl_name>} no ip igmp access-group
	Configure interface to filter IGMP group; the “no ip igmp access-group” command cancels the filter condition
Parameter	{<acl_num acl_name>} is SN or name of access-list, value range of acl_num is from 1 to 99.
Default	Default no filter condition
Mode	Interface Configuration Mode
Usage	Configure interface to filter groups, permit or deny some group joining
Example	<pre>Configure interface vlan1 to permit group 224.1.1.1, 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</pre>

ip igmp immediate-leave

Command	ip igmp immediate-leave group-list {<number> <name>} no ip igmp immediate-leave
	Configure IGMP working in immediate-leave mode, that is, when the host transmits

member identity report of equivalent to leave a group, router does not transmit query, it directly confirms there is no member of this group in subnet; the “no ip igmp immediate-leave” command cancels immediate-leave mode.

Parameter	<number> is access-list SN, value is from 1 to 99.
	<name> is access-list name.
Default	Interface default and no immediate-leave group of configuration after finished product
Mode	Interface Configuration Mode
Usage	The command only can apply in only one host condition in subnet.
Example	Configure immediate-leave mode on access-group list 1 Switch (Config-if-Vlan1)#ip igmp immediate-leave group-list 1 Switch (Config-if-Vlan1)#

ip igmp join-group

Command	ip igmp join-group <A.B.C.D > no ip igmp join-group <A.B.C.D >
	Configure interface to join some IGMP group; the “no ip igmp join-group” command cancels this join
Parameter	<A.B.C.D > is group address
Default	Do not join
Mode	Interface Configuration Mode
Usage	When the switch is the HOST, the command configures HOST to join some group; that is, if configuring the interface join-group 224.1.1.1, it will transmit IGMP member report including group 224.1.1.1 when the switch receives IGMP group query transmitted by other switches. Carefully, it is the difference between the command and ip igmp static-group command.
Example	Configure join-group 224.1.1.1 on interface vlan1. Switch (config)#interface vlan 1 Switch(Config-If-Vlan1)#ip igmp join-group 224.1.1.1

ip igmp last-member-query-interval

Command	ip igmp last-member-query-interval <interval>

no ip igmp last-member-query-interval

Configure interval of specified group query transmitting on interface; the “no ip igmp last-member-query-interval” command cancels the value of user manual configuration, and restores default value.

Parameter	<interval>	is interval of specified group query, range from 1000ms to 25500ms; the value is integer times of 1000ms, namely if input value is not integer times of 1000ms, the system automatically changes to integer times of 1000ms.
Default	1000ms	
Mode	Interface Configuration Mode	
Usage	It can configure interfaces to filter groups, allowing or rejecting the addition of certain groups.	
Example	Configure interface vlan1 IGMP last-member-query-interval to 2000. Switch (config)#int vlan 1 Switch (Config-if-vlan1)#ip igmp last-member-query-interval 2000	

ip igmp limit

Command	ip igmp limit <state-count> no ip igmp limit	
	Configure limit IGMP state-count on interface; the “no ip igmp limit” command cancels the value of user manual configuration, and restores default value.	
Parameter	<state-count>	is maximum IGMP state reserved by interface, range from 1 to 65000
Default	0, no limit.	
Mode	Interface Configuration Mode	
Usage	After configuring maximum state state-count, interface only saves states which are not more than state-count groups and sources. If it reaches upper limit of state-count, it does not deal with when receiving related new group member identity report. If it has saved some IGMP group states before configuring the command, it deletes all of the states, and then immediately transmits IGMP general query to collect the member identity report which is not more than state-count group. Static state and static source are not in the limit	
Example	Configure interface vlan1 IGMP limit to 4000. Switch (config)#int vlan 1 Switch (Config-if-vlan1)#ip igmp limit 4000	

ip igmp query-interval

Command	ip igmp query-interval <time_val> no ip igmp query-interval	
	Configure interval of periodically transmitted IGMP query information; the “no ip igmp query-interval” command restores default value.	
Parameter	<time_val>	is interval of periodically transmitted IGMP query information, value range from 1s to 65535s.
Default	Default interval of periodically transmitted IGMP query information to 125s.	
Mode	Interface Configuration Mode	
Usage	Periodically transmitting IGMP query information on interface when some interface enables some group multicast protocol. The command applies to configure this query period time.	
Example	Configure interval of periodically transmitted IGMP query message to 10s Switch (config)#interface vlan 1 Switch(Config-If-Vlan1)#ip igmp query-interval 10	

ip igmp query-max-response-time

Command	ip igmp query-max-response-time <time_val> no ip igmp query-max-response-time	
	Configure IGMP query-max-response-time of interface; the “no ip igmp query-max-response-time” command restores default value.	
Parameter	<time_val>	is IGMP query-max-response-time of interface, value range from 1s to 25s
Default	10s。	
Mode	Interface Configuration Mode	
Usage	After the switch receives a query message, the host will configure a timer for its affiliated every multicast group, the value of timer is selected random from 0 to maximum response time, the host will transmit member report message of the multicast group. Reasonable configuring maximum response time, it can make host quickly response query message. The router can also quickly grasp the status of multicast group member.	
Example	configure the maximum period responding to the IGMP query messages to 20s Switch (config)#interface vlan 1	

```
Switch(Config-If-Vlan1)#ip igmp query-max-response-time 20
```

ip igmp query-timeout

Command	ip igmp query-timeout <time_val> no ip igmp query-timeout	
	Configure IGMP query timeout of interface; the "no ip igmp query-timeout" command restores default value.	
Parameter	<time_val>	is IGMP query-timeout, value range from 60s to 300s.
Default	255s	
Mode	Interface Configuration Mode	
Usage	When multi-running IGMP switches are exist on sharing network, a switch will be voted as query processor on the sharing network, and other switches will be a timer monitoring the state of query processor; It still does not receive query message transmitting by query processor over query time-out, thus it re-votes another switch as new query processor.	
Example	Configure timeout of IGMP query message on interface to 100s. Switch (config)#interface vlan 1 Switch(Config-If-Vlan1)#ip igmp query-timeout 100	

ip igmp robust-variable

Command	ip igmp robust-variable <value> no ip igmp robust-variable	
	Configure the robust variable value, the "no ip igmp robust-variable" command restores default value.	
Parameter	value	range from 2 to 7.
Default	value: 2	
Mode	Interface Configuration Mode	
Usage	It is recommended using the default value. Robustness Variable: Robustness variables allow for adjustment based on expected packet loss on the link. If the expected message loss situation worsens, then the value of the robustness variable can also increase. IGMP/MLD allows at most Robustness Variable-1 packets to be lost without being affected. The value of the robustness variable cannot be 0 and	

should not be 1. The default value is 2.

Example

```
Switch (config-if-vlan1)#ip igmp robust-variable 3
```

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>]

Configure interface to join some IGMP static group; the “no ip igmp static-group” command cancels this join.

Parameter

<A.B.C.D> is group address;

source <A.B.C.D> expresses SSM source address of configuration.

Default

Do not join static group

Mode

Interface Configuration Mode

Usage

When configuring some interface to join some static group, it will receives about the multicast packet of the static group whether the interface has a real receiver or not; that is, if configuring the interface to join static group 224.1.1.1, the interface always receives about multicast packet about group 224.1.1.1 whether the interface has a receiver or not. Carefully, it is the difference between the command and ip igmp join-group command.

Example

```
Configure static-group 224.1.1.1 on interface vlan1.  
Switch (config)#interface vlan 1  
Switch(Config-If-Vlan1)#ip igmp static-group 224.1.1.1
```

ip igmp version

Command

ip igmp version <version>
no ip igmp version

Configure IGMP version on interface; the “no ip igmp version” command restores default value.

Parameter

<version> is IGMP version of configuration, currently supporting version 1, 2 and 3.

Default

version 2

Mode	Interface Configuration Mode
Usage	The command mainly applies to supply upward compatibility of the different version; it is not communicated between version 1 and version 2, therefore it must configure to the same version IGMP in the same network. When other routers which are not upgraded to IGMPv3 on interface-connected subnet need to join member identity collection of subnet IGMP together, the interface is configured to corresponding version.
Example	Configure IGMP on interface to version 3. Switch (config)#interface vlan 1 Switch(Config-If-Vlan1)#ip igmp version 1

show ip igmp groups

Command	show ip igmp groups [<A.B.C.D>] [detail]	
	Display IGMP group information	
Parameter	< A.B.C.D >	is group address, namely querying specified group information;
	detail	expresses group information in detail
Default	Do not display	
Mode	Admin Mode。	
Usage		
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# Displayed Information Group Address Interface Uptime Expires Last Reporter Explanations Multicast group IP address Interface affiliated with multicast group Multicast group uptime Multicast group expire time Last reporter to the host of 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 Present, 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

Displayed Information	Explanations
Group	Mutlicast group IP address
Interface	Interface affiliated with Mutlicast group
Flags	Group property flag
Uptime	Mutlicast group uptime
Group Mode	Group mode, including INCLUDE and EXCLUDE. Group V3 will be available, group V1 and group V2 are regards as EXCLUDE mode.
Exptime	Mutlicast group expire time
Last Reporter	Last reporter to the host of the Mutlicast group
Source Address	Source address of this group
V3 Exp	Source expire time
Fwd	If the data of the source is forwarded or not.
Flags	Source property flag

show ip igmp interface

Command **show ip igmp interface {vlan <vlan_id>|<ifname>}**

Display related IGMP information on interface.

Parameter **<ifname>** is interface name, namely displaying IGMP information of

	specified interface.
Default	Do not display
Mode	Admin Mode。
Usage	
Example	Display interface vlan1 IGMP message on Ethernet. 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

3 PIM-DM

debug pim timer sat

Command	debug pim timer sat no debug pim timer sat
	Enable debug switch of PIM-DM source activity timer information in detail; the “no debug pim timer sat” command disenables the debug switch.
Parameter	
Default	None
Mode	Admin Mode
Usage	Enable the switch, and display source activity timer information in detail.
Example	Switch # debug pim timer sat Other debug switches in PIM-DM are common in PIM-SM, including debug pim event, debug pim packet, debug pim nexthop, debug pim nsm, debug pim mfc, debug pim mib, debug pim timer, debug pim state

debug pim timer srt

Command	debug pim timer srt no debug pim timer srt
Parameter	Enable debug switch of PIM-DM state-refresh timer information in detail; the “no debug pim timer srt” command disables the debug switch.
Default	Disabled.
Mode	Admin Mode
Usage	Enable the switch, and display PIM-DM state-refresh timer information in detail.
Example	Switch # debug pim timer srt Other debug switches in PIM-DM are common in PIM-SM, including debug pim event, debug pim packet, debug pim nexthop, debug pim nsm, debug pim mfc, debug pim mib, debug pim timer, debug pim state

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>]
Parameter	To configure static multicast entry. The no command will delete some static multicast entries or some egress interfaces.
Default	<A.B.C.D> are the source address and group address of multicast. <A.B.C.D> <ifname> the first one is ingress interface, follow is egress interface. <.ifname>
Mode	Global Mode.
Usage	The <ifname> should be valid VLAN interfaces. The multicast data flow will not be forwarded unless PIM is configured on the egress interface and the interface is UP. If the state of the interface is not UP, or PIM is not configured, or RPF is not valid, the multicast data flow will not be forwarded. To removed the specified multicast routing entry. If all the egress interfaces are specified, or no interfaces are specified, the specified multicast routing entry will be removed. Otherwise the multicast routing entry for the specified interface will be removed.

Example	Switch(config)#ip mroute 10.1.1.1 225.1.1.1 v10 v20 v30

ip pim bsr-border

Command	ip pim bsr-border no ip pim bsr-border
Parameter	To configure or delete PIM BSR-BORDER interface.
Default	Non-BSR-BORDER.
Mode	Interface Configuration Mode。
Usage	To configure the interface as the BSR-BORDER. If configured, BSR related messages will not receive from or sent to the specified interface. All the networks connected to the interface will be considered as directly connected.
Example	Switch(Config-if-Vlan1)#no ip pim bsr-border

ip pim dense-mode

Command	ip pim dense-mode no ip pim dense-mode
Parameter	Enable PIM-DM protocol on interface; the “no ip pim dense-mode” command disables PIM-DM protocol on interface.
Default	Disable PIM-DM protocol.
Mode	Interface Configuration Mode。
Usage	The command will be taken effect, executing ip multicast-routing in Global Mode. Don’t support multicast protocol mutual operation, namely can’t synchronously enable dense mode and sparse mode in one switch.
Example	Enable PIM-DM protocol on interface vlan1. Switch(config)#ip pim multicast-routing

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip pim dense-mode
```

ip pim dr-priority

Command	ip pim dr-priority <priority> no ip pim dr-priority	
	Configure, disable or change the interface's DR priority. The neighboring nodes in the same net segment select the DR in their net segment according to hello packets. The "no ip pim dr-priority" command restores the default value.	
Parameter	<priority>	is priority
Default	1	
Mode	Interface Configuration Mode。	
Usage	Range from 0 to 4294967294, the higher value has more priority.	
Example	Configure VLAN's DR priority to 100 Switch(config)# interface vlan 1 Switch(Config-if-Vlan1)#ip pim dr-priority 100 Switch (Config-if-Vlan1)#	

ip pim exclude-genid

Command	ip pim exclude-genid no ip pim exclude-genid	
	This command makes the Hello packets sent by PIM SM do not include GenId option. The "no ip pim exclude-genid" command restores the default value	
Parameter		
Default	The Hello packets include GenId option.	
Mode	Interface Configuration Mode。	
Usage	This command is used to interact with older Cisco IOS version.	
Example	Configure the Hello packets sent by the switch do not include GenId option. Switch (Config-if-Vlan1)#ip pim exclude-genid Switch (Config-if-Vlan1)#	

ip pim hello-holdtime

Command	ip pim hello-holdtime <value> no ip pim hello-holdtime
	Configure or disable the Holdtime option in the Hello packets, this value is to describe neighbore holdtime, if the switch hasn't received the neighbore hello packets when the holdtime is over, this neighbore is deleted. The "no ip pim hello-holdtime" command cancels configured holdtime value and restores default value.
Parameter	<vaule> is the value of holdtime. Range <1-65535>。
Default	The default value of Holdtime is 3.5*Hello_interval, Hello_interval's default value is 30s, so Holdtime's default value is 105s
Mode	Interface Configuration Mode。
Usage	If this value is not configured, hellotime's default value is 3.5*Hello_interval. If the configured holdtime is less than the current hello_interval, this configuration is denied. Every time hello_interval is updated, the Hello_holdtime will update according to the following rules: If hello_holdtime is not configured or hello_holdtime is configured but less than current hello_interval, hello_holdtime is modified to 3.5*hello_interval, otherwise the configured value is maintained.
Example	Configure vlan1's Hello Holdtime Switch (config)# interface vlan1 Switch (Config -if-Vlan1)#ip pim hello-holdtime 10 Switch (Config -if-Vlan1)#

ip pim hello-interval

Command	ip pim hello-interval < interval> no ip pim hello-interval
	Configure interface PIM-DM hello message interval; the "no ip pim hello-interval" restores default value.
Parameter	< interval> is interval of periodically transmitted PIM-DM hello message, value range from 1s to 18724s.
Default	Default interval of periodically transmitted PIM-DM hello message as 30s.
Mode	Interface Configuration Mode。
Usage	Hello message makes PIM-DM switch mutual location, and ensures neighborship. PIM-

DM switch announces existence itself by periodically transmitting hello messages to neighbors. If it doesn't receive hello messages from neighbors in regulation time, it confirms that the neighbors were lost. Configuration time is not more than neighbor overtime.

Example

```
Configure PIM-DM hello interval on interface vlan1.
Switch(config)#interface vlan1
Switch(Config-if-Vlan1)#ip pim hello-interval 20
```

ip pim multicast-routing

Command

ip pim multicast-routing
no ip pim multicast-routing

Globally enable PIM-DM protocol; the “**no ip pim multicast-routing**” command disenables PIM-DM protocol.

Parameter

Default

Disabled PIM-SM

Mode

Interface Configuration Mode。

Usage

Enable PIM-SM globally. The interface must enable PIM-SM to have PIM-SM work

Example

```
Enable PIM-SM globally
Switch (config)#ip pim multicast-routing
Switch (config)#
```

ip pim neighbor-filter

Command

ip pim neighbor-filter <list-number>
no ip pim neighbor-filter <list-number>

Configure the neighbore access-list. If filtered by the lists and connections with neighbors are created, this connections are cut off immediately. If no connection is created, this connction can't be created.

Parameter

Default

<list-number> is the simple access-list number, it ranges from 1 to 99
 No neighbor filter configuration.

Mode	Interface Configuration Mode。
Usage	ACL's default is DENY. If configuring access-list 1,access-list 1's default is deny. In the following example, if “permit any-source” is not configured, deny 10.1.4.10 255.255.255.0 is the same as deny any-source.
Example	Configure VLAN's filtering rules of pim neighbors. <pre>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 10.1.4.10 255.255.255.0 Switch (config)#access-list 2 permit any-source Switch (config)#show ip pim neighbor Switch (config)#</pre>

ip pim scope-border

Command	ip pim scope-border [<1-99 > <acl_name>] no ip pim scope-border
	To configure or delete management border of PIM.
Parameter	<1-99 > is the ACL number for the management border. <acl_name> is the ACL name for the management border.
Default	Not management border. If no ACL is specified, the default management border will be used.
Mode	Interface Configuration Mode。
Usage	To configure the management border and the ACL for the PIM protocol. The multicast data flow will not be forwarded to the SCOPE-BORDER.
Example	Switch(Config-if-Vlan2)#ip pim scope-border 3

ip pim state-refresh origination-interval

Command	ip pim state-refresh origination-interval <interval> no ip pim state-refresh origination-interval
	Configure transmission interval of state-refresh message. The “no ip pim state-refresh origination-interval” command restores default value.

Parameter	<interval>	packet transmission interval value is from 4s to 100s.
Default	60s。	
Mode	Global Mode.	
Usage	The first-hop router periodically transmits stat-refresh messages to maintain PIM-DM list items of all the downstream routers. The command can modify origination interval of state-refresh messages. Usually do not modify relevant timer interval.	
Example	Configure transmission interval of state-refresh message to 90s. Switch (config)#ip pim state-refresh origination-interval 90	

show ip pim interface

Command	show ip pim interface	
	Display PIM interface information	
Parameter		
Default	None	
Mode	Admin Mode。	
Usage	Display PIM interface information	
Example	Switch (config)#show ip pim interface <pre> Address Interface VIF index 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 </pre> Displayed Information Address Interface VIF index Ver/Mode Nbr Count DR Prior DR Explanations Interface address Interface name Interface index Pim version and mode,usually v2,sparse mode displays S,dense mode displays D The interface's neighbor count Dr priority The interface's DR address	

show ip pim mroute dense-mode

Command	show ip pim mroute dense-mode [group <A.B.C.D>] [source <A.B.C.D>]	
	Display PIM-DM message forwarding items.	
Parameter	group <A.B.C.D>	displays forwarding items relevant to this multicast address.
	source <A.B.C.D>	displays forwarding items relevant to this source.
Default	Do not display (Off).	
Mode	Admin Mode.	
Usage	The command shows PIM-DM multicast forwarding items, namely forwarding items of forward multicast packet in system FIB table.	
Example	Display all of PIM-DM message forwarding items. 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.....	
	Displayed Information (*,226.0.0.1) (192.168.1.12, 226.0.0.1) RPF nbr RPF idx Upstream State	Explanations (*,G) Forwarding item (S,G) Forwarding item Backward path neighbor, upstream neighbor of source direction in DM, 0.0.0.0 expresses the switch is the first hop. Interface located in RPF neighbor Upstream direction, including FORWARDING(forwarding upstream data), PRUNED(Upstream stops forwarding data), ACKPENDING(waiting for upstream

	response, forwarding upstream data)
Origin State	The two states: ORIGINATOR(on transmit state-refresh state), NON_ORIGINATOR(on non_transmit state-refresh state)
Local	Local position joins interface, the interface receives IGMP Join
Pruned	PIM prunes interface, the interface receives Prune messages
Asserted	Asserted state
Outgoing	Multicast data finally exported from interface is index number, index is 2 in this case. It can check interface information in detail by commanding show ip pim interface

show ip pim neighbor

Command **show ip pim neighbor**

Display router neighbors

Parameter
Default

Mode Admin Mode。

Usage Display multicast router neighbors maintained by the 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 /	

Displayed Information

Explanations

Neighbor Address

Neighbor address

Interface

Neighbor interface

Uptime/Expires

Running time /overtime

Ver

Pim version ,v2 usually

DR Priority/Mode	DR priority in the hello messages from the neighbor and if the neighbor is the interface's DP.

show ip pim nexthop

Command **show ip pim nexthop**

Display the PIM buffered nexthop router in the unicast route table

Parameter

Default None

Mode Admin Mode.

Usage Display the PIM buffered nexthop router information.

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

Displayed Information

Destination

Type

Nexthop Num

Nexthop Addr

Nexthop Ifindex

Nexthop Name

Metric

Pref

Refcnt

Explanations

Destination of next item

N: created nexthop, RP direction and S direction are not determined . R: RP direction S: source direction U: can't reach

Nexthop number

Nexthop address

Nexthop interface index

Nexthop name

Metric Metric to nexthop

Preference Route preference

Reference count

4 PIM-SM

clear ip pim bsr rp-set

Command	clear ip pim bsr rp-set *
Parameter	Clear all RP.
Default	
Mode	Admin Mode
Usage	Clear all RP rapidly.
Example	Switch# clear ip pim bsr rp-set *

debug pim event

Command	debug pim event no debug pim event
Parameter	Enable or Disable pim event debug switch
Default	Disabled
Mode	Admin Mode
Usage	Enable pim event debug switch and display events information about pim operation.
Example	Switch# debug pim event Switch#

debug pim mfc

Command	debug pim mfc no debug pim mfc
Parameter	Enable or Disable pim mfc debug switch
Default	Disabled
Mode	Admin Mode
Usage	Enable pim mfc debug switch and display generated and transmitted multicast id's information.
Example	Switch# debug pim mfc

debug pim mib

Command	debug pim mib no debug pim mib
Parameter	Enable or Disable PIM MIB debug switch
Default	Disabled
Mode	Admin Mode
Usage	Inspect PIM MIB information by PIM MIB debug switch. It's not available now and it's for the future extension.
Example	Switch# debug pim mib Switch#

debug pim nexthop

Command	debug pim nexthop no debug pim nexthop
Parameter	Enable or Disable pim nexthop debug switch
Default	Disabled
Mode	Admin Mode
Usage	Inspect PIM NEXTHOP changing information by the pim nexthop switch.
Example	Switch# debug pim nexthop Switch#

debug pim nsm

Command	debug pim nsm no debug pim nsm
Parameter	Enable or Disable pim debug switch communicating with Network Services
Default	Disabled
Mode	Admin Mode
Usage	Inspect the communicating information between PIM and Network Services by this switch.
Example	Switch# debug pim nsm Switch#

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	
Parameter	Enable or Disable pim debug switch	
	in	display only received pim packets
	out	display only transmitted pim packets
	None	display both
Default	Disabled	
Mode	Admin Mode	
Usage	Inspect the received and transmitted pim packets by this switch.	
Example	Switch# debug pim packet in Switch#	

debug pim state

Command	debug pim state no debug pim state	
Parameter	Enable or Disable pim debug switch	
Default	Disabled	
Mode	Admin Mode	
Usage	Inspect the changing information about pim state by this switch.	

Example

```
Switch# debug pim state
Switch#
```

debug pim packet

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

Enable or Disable each pim timer

Parameter

Default

Disabled

Mode

Admin Mode

Usage

Enable the specified timer's debug information.

Example

Switch# debug pim timer assert
 Switch#

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>]

To configure static multicast entry. The no command will delete some static multicast entries or some egress interfaces.

Parameter

<A.B.C.D> are the source address and group address of multicast.
 <A.B.C.D>

<ifname> the first one is ingress interface, follow is egress interface.
 <.ifname>

Default

To delete this static multicast entry, if the command isn't included interface parameter.

Mode

Global Mode

Usage

The <ifname> should be valid VLAN interfaces. The multicast data flow will not be forwarded unless PIM is configured on the egress interface and the interface is UP. If the state of the interface is not UP, or PIM is not configured, or RPF is not valid, the multicast data flow will not be forwarded. To removed the specified multicast routing entry. If all the egress interfaces are specified, or no interfaces are specified, the specified multicast routing entry will be removed. Otherwise the multicast routing entry for the specified interface will be removed.

Example

Switch(config)#ip mroute 10.1.1.1 225.1.1.1 v10 v20 v30

ip multicast unresolved-cache aging-time

Command	ip multicast unresolved-cache aging-time <value> no ip multicast unresolved-cache aging-time	
	Configure the cache time of the kernel multicast route, the no command restores the default value.	
Parameter	< value>	is the configured cache time, ranging between 1 and 20s.
Default	10s。	
Mode	Global Mode	
Usage	Configure the cache time of multicast route entry in kernel.	
Example	Switch(config)# ip multicast unresolved-cache aging-time 18	

ip pim accept-register

Command	ip pim accept-register list <list-number> no ip pim accept-register	
	Filter the specified multicast group and multicast address.	
Parameter	<list-number>	is the access-list number, it ranges from 100 to 199.
Default	Permit the multicast registers from any sources to any groups.	
Mode	Global Mode	
Usage	This command is used to configure the access-list filtering the PIM REGISTER packets.The addresses of the access-list respectively indicate the filtered multicast sources and multicast groups' information. For the source-group combinations that match DENY, PIM sends REGISTER-STOP immediately and does not create group records when receiving REGISTER packets. Unlike other access-list, when the access-list is configured, the default value is PERMIT.	
Example	Configure the filtered register message's rule to myfilter. 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)#	

ip pim bsr-border

Command	ip pim bsr-border

no ip pim bsr-border

	To configure or delete PIM BSR-BORDER interface.
Parameter	
Default	Non-BSR-BORDER.
Mode	Interface Configuration Mode。
Usage	To configure the interface as the BSR-BORDER. If configured, BSR related messages will not receive from or sent to the specified interface. All the networks connected to the interface will be considered as directly connected.
Example	Switch(Config-if-Vlan1)#no ip pim bsr-border

ip pim bsr-candidate

Command	ip pim bsr-candidate {vlan <vlan-id> <ifname>} [hash-mask-length] [priority] no ip pim bsr-candidate	
	This command is the candidate BSR configure command in global mode and is used to configure PIM-SM information about candidate BSR in order to compete with other candidate BSRs for the BSR router. The command "no ip pim bsr-candidate" disables the candidate BSR.	
Parameter	vlan-id	VLAN ID
	ifname	is the specified interface's name
	[hash-mask-length]	is the specified hash mask length. It's used for the RP enable selection and ranges from 0 to 32
	[priority]	is the candidate BSR priority and ranges from 0 to 255. If this parameter is not configured, the default priority value is 0
Default	This switch is not a candidate BSR router.	
Mode	Global Mode.	
Usage	This command is the candidate BSR configure command in global mode and is used to configure PIM-SM information about candidate BSR in order to compete with other candidate BSRs for the BSR router. Only this command is configured, this switch is the BSR candidate router.	
Example	Globally configure the interface vlan1 as the candidate BSR-message transmitting	

```

interface.
Switch (config)# ip pim bsr-candidate vlan1 30 10
Switch (config)#

```

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>]	
	Configure the register packet's checksum of the group specified by myfilter to use the whole packet's length.	
Parameter	<simple-acl>	<1-99> Simple access list
Default	Compute the checksum according to the register packet's head length, default: 8	
Mode	Global Mode	
Usage	This command is used to interact with older Cisco IOS version.	
Example	Configure the register packet's checksum of the group specified by myfilter to use the whole packet's length. Switch (config)#ip pim cisco-register-checksum group-list 23 Switch (config)#	

ip pim dr-priority

Command	ip pim dr-priority <priority> no ip pim dr-priority	
	Configure, disable or change the interface's DR priority. The neighboring nodes in the same net segment select the DR in their net segment according to hello packets. The "no ip pim dr-priority" command restores the default value.	
Parameter	<priority>	is priority
Default	1	
Mode	Interface Configuration Mode	
Usage	Range from 0 to 4294967294, the higher value has more priority.	
Example	Configure VLAN's DR priority to 100 Switch (config)# interface vlan 1 Switch (Config-if-Vlan1)ip pim dr-priority 100 Switch (Config -if-Vlan1)#	

ip pim exclude-genid

Command	ip pim exclude-genid no ip pim exclude-genid
	This command makes the Hello packets sent by PIM SM do not include GenId option. The "no ipv6 pim exclude-genid" command restores the default value
Parameter	
Default	The Hello packets include GenId option.
Mode	Interface Configuration Mode
Usage	This command is used to interact with older Cisco IOS version.
Example	Configure the Hello packets sent by the switch do not include GenId option. Switch (Config-if-Vlan1)#ip pim exclude-genid Switch (Config-if-Vlan1)#

ip pim hello-holdtime

Command	ip pim hello-holdtime <value> no ip pim hello-holdtime
	Configure or disable the Holdtime option in the Hello packets, this value is to describe neighbor holdtime, if the switch hasn't received the neighbor hello packets when the holdtime is over, this neighbor is deleted. The "no ip pim hello-holdtime" command cancels configured holdtime value and restores default value.
Parameter	<vaule> is the value of holdtime. Range <1-65535>.
Default	The default value of Holdtime is 3.5*Hello_interval, Hello_interval's default value is 30s, so Hold time's default value is 105s.
Mode	Interface Configuration Mode
Usage	If this value is not configured, hellotime's default value is 3.5*Hello_interval. If the configured holdtime is less than the current hello_interval, this configuration is denied. Every time hello_interval is updated, the Hello_holdtime will update according to the

following rules: If hello_holdtime is not configured or hello_holdtime is configured but less than current hello_interval, hello_holdtime is modified to 3.5*hello_interval, otherwise the configured value is maintained.

Example	Configure vlan1's Hello Holdtime Switch (config)# interface vlan1 Switch (Config-if-Vlan1)#ip pim hello-holdtime 10 Switch (Config-if-Vlan1)#

ip pim hello-interval

Command	ip pim hello-interval <interval> no ip pim hello-interval
	Configure the interface's hello_interval of pim hello packets. The "no ip pim hello-interval" command restores the default value.
Parameter	<interval> is the hello_interval of periodically transmitted pim hello packets', ranges from 1 to 18724s.
Default	The default periodically transmitted pim hello packets' hello_interval is 30s.
Mode	Interface Configuration Mode
Usage	Hello messages make pim switches oriented each other and determine neighbor relationship. Pim switch announce the existence of itself by periodically transmitting hello messages to neighbors. If no hello messages from neighbors are received in the certain time, the neighbor is considered lost. This value can't be greater than neighbor overtime.
Example	Configure VLAN's pim-sm hello interval Switch (config)#interface vlan 1 Switch (Config-If-Vlan1)#ip pim hello-interval 20 Switch (Config-If-Vlan1)#

ip pim ignore-rp-set-priority

Command	ip pim ignore-rp-set-priority no ip pim ignore-rp-set-priority
	When RP selection is carried out, this command configures the switch to enable Hashing regulation and ignore RP priority. This command is used to interact with older Cisco IOS versions.
Parameter	
Default	Disabled

Mode	Global Mode
Usage	When selecting RP, Pim usually will select according to RP priority. When this command is configured, pim will not select according to RP priority. Unless there are older routers in the net, this command is not recommended.
Example	Switch (config)#ip pim ignore-rp-set-priority Switch (config)#

ip pim jp-timer

Command	ip pim jp-timer <value> no ip pim jp-timer
	Configure to add JP timer. The “no ip pim jp-timer” command restores the default value.
Parameter	<value> ranges from 10 to 65535s
Default	60s
Mode	Global Mode
Usage	Configure the interval of JOIN-PRUNE packets sent by PIM periodically, the default value is 60s. The default value is recommended if no special reasons.
Example	Configure the interval of timer Switch (config)#ip pim jp-timer 59 Switch (config)#

ip pim multicast-routing

Command	ip pim multicast-routing no ip pim multicast-routing
	Enable PIM-SM globally. The “no ip pim multicast-routing” command disables PIM-SM globally.
Parameter	
Default	Disabled PIM-SM

Mode	Global Mode
Usage	Enable PIM-SM globally. The interface must enable PIM-SM to have PIM-SM work
Example	Enable PIM-SM globally Switch (config)#ip pim multicast-routing Switch (config)#

ip pim neighbor-filter

Command	ip pim neighbor-filter <list-number> no ip pim neighbor-filter <list-number>
	Configure the neighbor access-list. If filtered by the lists and connections with neighbors are created, this connections are cut off immediately. If no connection is created, this connection can't be created.
Parameter	<list-number> is the simple access-list number, it ranges from 1 to 99
Default	No neighbor filter configuration.
Mode	Interface Configuration Mode
Usage	ACL's default is DENY. If configuring access-list 1, access-list 1's default is deny. In the following example, if "permit any" is not configured, deny 10.1.4.10 255.255.255.0 is the same as deny any.
Example	Configure VLAN's filtering rules of pim neighbors. 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 10.1.4.10 255.255.255.0 Switch (config)#access-list 2 permit any-source Switch (config)#show ip pim neighbor Switch (config)#

ip pim register-rate-limit

Command	ip pim register-rate-limit <limit> no ip pim register-rate-limit
	This command is used to configure the speedrate of DR sending register packets;

the unit is packet/second. The “no ip pim Register-rate-limit” command restores the default value. This configured speedrate is each (S, G) state's ,not the whole system's.

Parameter	<limit>	ranges from 1 to 65535.
Default	No limit for sending speed	
Mode	Global Mode	
Usage	This configuration is to prevent the attack to DR, limiting sending REGISTER packets.	
Example	Configure the speedrate of DR sending register packets to 59p/s. Switch (config)#ip pim register-rate-limit 59 Switch (config)#	

ip pim register-rp-reachability

Command	ip pim register-rp-reachability no ip pim register-rp-reachability	
	This command makes DR check the RP reachability in the process of registration.	
Parameter		
Default	Do not check	
Mode	Global Mode	
Usage	This command configures DR whether or not to check the RP reachability.	
Example	Configure DR to check the RP reachability. Switch (config)#ip pim register-rp-reachability Switch (config)#	

ip pim register-source

Command	ip pim register-source {<A.B.C.D> <ifname> vlan <vlan-id>}

no ip pim register-source

This command is to configure the source address of register packets sent by DR to overwrite default source address. This default source address is usually the RPF neighbor of source host direction.

Parameter	<ifname>	is the interface name
	<vlan-id>	is VLAN ID
Default	<A.B.C.D>	is the configured source IP addresses.
	Do not check	
Mode	Global Mode	
Usage	The “no ip pim register-source” command restores the default value, no more parameter is needed. Configured address must be reachable to Register-Stop messages sent by RP. It’s usually a circle address, but it can be other physical addresses. This address must be announcable through unicast router protocols of DR.	
Example	Configure the source address sent by DR. Switch (config)#ip pim register-source 10.1.1.1 Switch (config)#	

ip pim register-suppression

Command	ip pim register-suppression <value> no ip pim register-suppression	
	This command is to configure the value of register suppression timer, the unit is second. The “no ip pim register-suppression” command restores the default value.	
Parameter	<value>	is the timer’s value; it ranges from 10 to 65535s.
Default	60s	
Mode	Global Mode	
Usage	If this value is configured at DR, it’s the value of register suppression timer; the bigger one of the default register keep-alive time of RP (210s) and the sum of triple register suppression time and 5. If configure this value on RP without the command “ip pim rp-register-kat”, this command may modify the RP register keep-alive time.	
Example	Configure the value of register suppression timer to 10s. Switch (config)#ip pim register-suppression 10 Switch (config)#	

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>]	
Parameter	This command is to configure static RP globally or in a multicast address range. The “no ip pim rp-address <A.B.C.D> [<A.B.C.D/M> <all>]” command cancels static RP.	
	<A.B.C.D>	is the RP address
	<A.B.C.D/M>	the scope of the specified RP address
Default	<all>	is all the range
	This switch is not a RP static router.	
Mode	Global Mode	
Usage	This command is to configure static RP globally or in a multicast address range and configure PIM-SM static RP information. Attention, when computing rp, BSR RP is selected first. If it doesn't succeed, static RP is selected.	
Example	Configure vlan1 as candidate RP announcing sending interface globally. Switch (config)# ip pim rp-address 10.1.1.1 238.0.0.0/8 Switch (config)#	

ip pim rp-candidate

Command	ip pim rp-candidate {vlan<vlan-id> loopback<index> <ifname>} [<A.B.C.D/M>] [<priority>] no ip pim rp-candidate	
Parameter	This command is the candidate RP global configure command, it is used to configure PIM-SM candidate RP information in order to compete RP router with other candidate RPs. The “no ip pim rp-candidate” command cancels the candidate RP.	
	vlan-id	is vlan ID
	<index>	indexing the Loopback interface
	ifname	is the name of the specified interface
	A.B.C.D/M	is the ip prefix and mask
	<priority>	is the RP selection priority, it ranges from 0 to 255, the default value is 192, the lower value has more priority
Default	This switch is not a RP static router.	
Mode	Global Mode	
Usage	This command is the candidate RP global configure command, it is used to configure PIM-SM candidate RP information in order to compete RP router with other candidate	

RPs. Only this command is configured, this switch is the RP candidate router.

Example	Configure vlan1 as the sending interface of candidate RP announcing sending messages Switch (config)# ip pim rp-candidate vlan1 100 Switch (config)#

ip pim rp-register-kat

Command	ip pim rp-register-kat <vaule> no ip pim rp-register-kat
	This command is to configure the KAT (KeepAlive Timer) value of the RP (S, G) items, the unit is second. The "no ip pim rp-register-kat" command restores the default value.
Parameter	<value> is the timer value; it ranges from 1 to 65535s.
Default	185s
Mode	Global Mode
Usage	This command is to configure the RP's keep alive time, during the keep alive time RP's (S, G) item will not be deleted because it hasn't received REGISTER packets. If no new REGISTER packet is received when the keep alive time is over, this item will be obsolete.
Example	Configure the kat value of RP's (S, G) item to 180s Switch (config)#ip pim rp-register-kat 180 Switch (config)#

ip pim scope-border

Command	ip pim scope-border [<1-99 > <acl_name>] no ip pim scope-border
	To configure or delete management border of PIM.
Parameter	<1-99 > is the ACL number for the management border.
	<acl_name> is the ACL name for the management border.
Default	Not management border. If no ACL is specified, the default management border will be used.
Mode	Interface Configuration Mode.
Usage	To configure the management border and the ACL for the PIM protocol. The multicast data flow will not be forwarded to the SCOPE-BORDER.

Example	Switch(Config-if-Vlan2)#ip pim scope-border 3

ip pim sparse-mode

Command	ip pim sparse-mode [passive] no ip pim sparse-mode [passive]
	Enable PIM-SM on the interface; the "no ip pim sparse-mode [passive]" command disables PIM-SM.
Parameter	[passive] means to disable PIM-SM (that's PIM-SM doesn't receive any packets) and only enable IGMP (receive and transmit IGMP packets).
Default	Do not enable PIM-SM
Mode	Interface Configuration Mode
Usage	Enable PIM-SM on the interface.
Example	Enable PIM-SM on the interface vlan1. Switch(config)#interface vlan 1 Switch(Config-If-Vlan1)#ip pim sparse-mode Switch(Config-If-Vlan1)#

show ip pim bsr-router

Command	show ip pim bsr-router
	Display BSR address
Parameter	
Default	None
Mode	Admin Mode.
Usage	Display the BSR information maintained by the PIM.
Example	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)	
Displayed Information	Explanations
BSR address	Bsr-router Address
Priority	Bsr-router Priority
Hash mask length	Bsr-router hash mask length
State	The current state of this candidate
BSR, Elected BSR is selected BSR	

show ip pim interface

Command **show ip pim interface**

Display PIM interface information

Parameter

Default

None

Mode

Admin Mode and Global Mode

Usage

Display 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

Displayed Information

Explanations

Address

Interface address

Interface

Interface name

VIF index

Interface index

Ver/Mode

Pim version and mode,usually v2,sparse mode displays S,dense mode displays D

Nbr Count

The interface's neighbor count

DR Prior

Dr priority

DR

The interface's DR address

show ip pim mroute sparse-mode

Command **show ip pim mroute sparse-mode [group <A.B.C.D>] [source <A.B.C.D>]**

	Display the multicast route table of PIM-SM.																			
Parameter	group <A.B.C.D>	Display redistributed items that related to this multicast address																		
Default	source <A.B.C.D> None	Display redistributed items that related to this source																		
Mode	Admin Mode and Global Mode																			
Usage	Display the BSP routers in the network 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..... <table><tr><th>Displayed Information</th><th>Explanations</th></tr><tr><td>Entries</td><td>The counts of each item</td></tr><tr><td>RP</td><td>Share tree’s RP address</td></tr><tr><td>RPF nbr</td><td>RP direction or upneighbor of source direction.</td></tr><tr><td>RPF idx</td><td>RPF nbr interface</td></tr><tr><td>Upstream State</td><td>Upstream State, there are two state of Joined(join the tree, expect to receive data from upstream) and Not Joined(quit the tree, not expect to receive data from upstream), and more options such as RPT Not Joined, Pruned, Not Pruned are available for (S,G,rpt.)</td></tr><tr><td>Local</td><td>Local join interface, this interface receive IGMPJoin</td></tr><tr><td>Joined</td><td>PIM join interface, this interface receive J/P messages</td></tr><tr><td>Asserted</td><td>Asserted state</td></tr></table>		Displayed Information	Explanations	Entries	The counts of each item	RP	Share tree’s RP address	RPF nbr	RP direction or upneighbor of source direction.	RPF idx	RPF nbr interface	Upstream State	Upstream State, there are two state of Joined(join the tree, expect to receive data from upstream) and Not Joined(quit the tree, not expect to receive data from upstream), and more options such as RPT Not Joined, Pruned, Not Pruned are available for (S,G,rpt.)	Local	Local join interface, this interface receive IGMPJoin	Joined	PIM join interface, this interface receive J/P messages	Asserted	Asserted state
Displayed Information	Explanations																			
Entries	The counts of each item																			
RP	Share tree’s RP address																			
RPF nbr	RP direction or upneighbor of source direction.																			
RPF idx	RPF nbr interface																			
Upstream State	Upstream State, there are two state of Joined(join the tree, expect to receive data from upstream) and Not Joined(quit the tree, not expect to receive data from upstream), and more options such as RPT Not Joined, Pruned, Not Pruned are available for (S,G,rpt.)																			
Local	Local join interface, this interface receive IGMPJoin																			
Joined	PIM join interface, this interface receive J/P messages																			
Asserted	Asserted state																			

Outgoing	Final outgoing of multicast data, in this example, the index of the outgoing interface is 2. Command “show ip pim interface” can query interface information.

show ip pim neighbor

Command **show ip pim neighbor**

Display router neighbors

Parameter

Default

None

Mode

Admin Mode and Global Mode

Usage

Display multicast router neighbors maintained by the PIM

Example

```
s1(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 /
```

Displayed Information

Neighbor Address

Interface

Uptime/Expires

Ver

DR Priority/Mode

Explanations

Neighbor address

Neighbor interface

Running time /overtime

Pim version ,v2 usually

DR priority in the hello messages from

the neighbor and if the neighbor is the interface's DP.

show ip pim nexthop

Command **show ip pim nexthop**

Display the PIM buffered nexthop router in the unicast route table

Parameter

Default

None

Mode

Admin Mode and Global Mode

Usage

Display the PIM buffered nexthop router information.

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

Displayed Information

Destination

Type

Nexthop Num

Nexthop Addr

Nexthop Ifindex

Nexthop Name

Metric

Pref

Refcnt

Explanations

Destination of next item

N: created nexthop, RP direction and S direction are not determined . R: RP direction S: source direction U: can't reach

Nexthop number

Nexthop address

Nexthop interface index

Nexthop name

Metric Metric to nexthop

Preference Route preference

Reference count

show ip pim rp-hash

Command	show ip pim rp-hash <A.B.C.D>	
	Display the RP address of A.B.C.D's merge point	
Parameter	<A.B.C.D>	Group address
Default	None	
Mode	Admin Mode and Global Mode	
Usage	Display the RP address corresponding to the specified group address	
Example	testS2(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	
	Displayed Information	Explanations
	RP	Queried group's RP
	Info source	The source of Bootstrap information

show ip pim rp mapping

Command	show ip pim rp mapping	
	Display Group-to-RP Mapping and RP.	
Parameter		
Default	None	
Mode	Admin Mode and Global Mode	
Usage	Display the current RP and mapping relationship.	
Example	testS2(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	

Displayed Information	Explanations
Group(s)	Group address range of RP
Info source	Source of Bootstrap messages
Priority	Priority of Bootstrap messages

5 PIM-SSM

ip multicast ssm

Command	ip multicast ssm {default range <access-list-number >} no ip multicast ssm	
	Configure the range of pim ssm multicast address. The “no ip multicast ssm” command deletes configured pim ssm multicast group.	
Parameter	default	indicates the default range of pim ssm multicast group is 232/8.
	<access-list-number >	is the applying access-list number; it ranges from 1 to 99.
Default	Do not configure the range of pim ssm group address.	
Mode	Global Mode.	
Usage	1. Only this command is configured, pim ssm can be available. 2. Before configuring this command, make sure ip pim multicasting succeed. This command can't work with DVMRP. 3. Access-list can't used the lists created by ip access-list, but the lists created by access-list. 4. Users can execute this command first and then configure the corresponding acl; or delete corresponding acl in the bondage. After the bondage, only command no ip pim ssm can release the bondage. 5 .If ssm is needed, this command should be configured at the related edge route. For example, the local switch with IGMP (must) and multicast source DR or RP (at least one of the two) configure this command, the middle switch need only enable PIM-SM.	
Example	Configure the switch to enable PIM-SSM, the group's range is what is specified by access-list 23. Switch (config)#ip multicast ssm range 23	

6 PIM-DM6

debug ipv6 pim timer sat

Command	debug ipv6 pim timer sat no debug ipv6 pim timer sat
	Enable debug switch of PIM-DM source activity timer information in detail; the " no debug ipv6 pim timer sat " command disenables the debug switch.
Parameter	None
Default	Disabled
Mode	Admin Mode
Usage	Enable the switch, and display source activity timer information in detail.
Example	Switch # debug ipv6 pim timer sat

debug ipv6 pim timer srt

Command	debug ipv6 pim timer srt no debug ipv6 pim timer srt
	Enable debug switch of PIM-DM state-refresh timer information in detail; the " no debug ipv6 pim timer srt " command disenables the debug switch.
Parameter	
Default	Disabled.
Mode	Admin Mode
Usage	Enable the switch, and display PIM-DM state-refresh timer information in detail.
Example	Switch # debug ipv6 pim timer srt

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>]	
	To configure static multicast entry. The no command will delete some static multicast entries or some egress interfaces.	
Parameter	<X:X::X:X>	are the source address and group address of multicast.
	<X:X::X:X>	IPv6 group address
	<ifname> <.ifname>	the first one is ingress interface, follow is egress interface.
Default	None	
Mode	Global Mode.	
Usage	The <ifname> should be valid VLAN interfaces. The multicast data flow will not be forwarded unless PIM is configured on the egress interface and the interface is UP. If the state of the interface is not UP, or PIM is not configured, or RPF is not valid, the multicast data flow will not be forwarded. To removed the specified multicast routing entry. If all the egress interfaces are specified, or no interfaces are specified, the specified multicast routing entry will be removed. Otherwise the multicast routing entry for the specified interface will be removed.	
Example	Switch(config)# ipv6 mroute 2106::2 ff16::1 vlan10 vlan20	

ipv6 pim bsr-border

Command	ipv6 pim bsr-border no ipv6 pim bsr-border	
	To configure or delete PIM6 BSR-BORDER interface.	
Parameter	None	
Default	Non-BSR-BORDER.	
Mode	Interface Configuration Mode。	
Usage	To configure the interface as the BSR-BORDER. If configured, BSR related messages will not receive from or sent to the specified interface. All the networks connected to the interface will be considered as directly connected.	
Example	Switch(Config-if-Vlan1)#ipv6 pim bsr-border	

ipv6 pim dense-mode

Command	ipv6 pim dense-mode no ipv6 pim dense-mode
	Enable PIM-DM protocol on interface; the “ no ipv6 pim dense-mode ” command disables PIM-DM protocol on interface.
Parameter	
Default	Disable PIM-DM protocol.
Mode	Interface Configuration Mode。
Usage	The command will be taken effect, executing ipv6 multicast-routing in Global Mode. Don't support multicast protocol mutual operation, namely can't synchronously enable dense mode and sparse mode in one switch. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully
Example	Enable PIM-DM protocol on interface vlan1. Switch(config)#ipv6 pim multicast-routing Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ipv6 pim dense-mode

ipv6 pim dr-priority

Command	ipv6 pim dr-priority <priority> no ipv6 pim dr-priority
	Configure, disable or change the interface's DR priority. The neighboring nodes in the same net segment select the DR in their net segment according to hello packets. The “no ipv6 pim dr-priority” command restores the default value.
Parameter	<priority> priority, value range from 0 to 4294967294
Default	1
Mode	Interface Configuration Mode。
Usage	Value range is from 0 to 4294967294, the bigger value, the more priority. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example	Switch (config)# interface vlan 1 Switch(Config-if-Vlan1)ipv6 pim dr-priority 100

ipv6 pim exclude-genid

Command	ipv6 pim exclude-genid no ipv6 pim exclude-genid
	This command makes the Hello packets sent by PIM SM do not include Genid option. The “ no ipv6 pim exclude-genid ” command restores the default value
Parameter	None
Default	Hello message includes Genid option
Mode	Interface Configuration Mode。
Usage	The command is used to interactive with old Cisco IOS Version.The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.
Example	Configure hello messages transmitted by switch to exclude Genid option. Switch(Config-if-Vlan1)#ipv6 pim exclude-genid

ipv6 pim hello-holdtime

Command	ipv6 pim hello-holdtime <value> no ipv6 pim hello-holdtime
	Configure or disable the Holdtime option in the Hello packets, this value is to describe neighbore holdtime, if the switch hasn't received the neighbore hello packets when the holdtime is over, this neighbore is deleted. The “no ip pim hello-holdtime” command cancels configured holdtime value and restores default value.
Parameter	<vaule> is configure time of holdtime.
Default	The default value of Holdtime is 3.5*Hello_interval, Hello_interval's default value is 30s, so Holdtime's default value is 105s
Mode	Interface Configuration Mode。
Usage	If no setting, hello time will default current 3.5 times of Hello_interval. If setting hello

time is less than current hello_interval, this setting will be declined. When updating hello_interval every time, hello_holdtime will be also update based on these rules below: if hello_holdtime does not be configured, or if hello_holdtime configured is less than current hello_interval, hello_holdtime will be modified to 3.5 times Hello_interval, otherwise, keeps configured value. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example

```
Configure hello holdtime setting on interface vlan1 to 10.
Switch (config)# interface vlan1
Switch (Config-if-Vlan1)#ipv6 pim hello-holdtime 10
```

ipv6 pim hello-interval

Command

ipv6 pim hello-interval < interval>
no ipv6 pim hello-interval

Configure interface PIM-DM hello message interval; the “no ipv6 pim hello-interval” restores default value.

Parameter

< interval> is interval of periodically transmitted PIM-DM hello message, value range from 1s to 18724s.

Default

Default interval of periodically transmitted PIM-DM hello message as 30s.

Mode

Interface Configuration Mode。

Usage

Hello message makes PIM-DM switch mutual location, and ensures neighbor ship. PIM-DM switch announces existence itself by periodically transmitting hello messages to neighbors. If it doesn't receive hello messages from neighbors in regulation time, it confirms that the neighbors were lost. Configuration time is not more than neighbor overtime. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example

```
Configure PIM-DM hello interval on interface vlan1
Switch (config)#interface vlan1
Switch(Config-if-Vlan1)#ipv6 pim hello-interval 20
```

ipv6 pim multicast-routing

Command

ipv6 pim multicast-routing
no ipv6 pim multicast-routing

Globally enable PIM-DM protocol; the “no ipv6 pim multicast-routing” command disables PIM-DM protocol.

Parameter	
Default	Disabled PIM-SM
Mode	Interface Configuration Mode。
Usage	Ipv6 pim can enable only after executing this command.
Example	Globally enable PIM-DM protocol Switch (config)#ipv6 pim multicast-routing

ipv6 pim neighbor-filter

Command	ipv6 pim neighbor-filter <access-list-name> no ipv6 pim neighbor-filter <access-list-name>
	Configure neighbor access-list. If filtered by list and connected the neighbor, the connection immediately was broken. If no connection, the connection can be established.
Parameter	<access-list-name> is an applied access-list name
Default	No neighbor filter configuration.
Mode	Interface Configuration Mode。
Usage	If it is not necessary for partner to establish neighbor ship, the command can filter pim message of partner. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.
Example	Configure access-list of pim neighbor on interface vlan1 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

ipv6 pim scope-border

Command	ipv6 pim scope-border [<500-599> <acl_name>] no ipv6 pim scope-border

	To configure or delete management border of PIM6.	
Parameter	<500-599>	is the ACL number for the management border.
	<acl_name>	is the ACL name for the management border.
Default	Not management border. If no ACL is specified, the default management border will be used.	
Mode	Interface Configuration Mode。	
Usage	To configure the management border and the ACL for the IPV6 PIM protocol. The multicast data flow will not be forwarded to the SCOPE-BORDER.	
Example	Switch(Config-if-Vlan2)#ipv6 pim scope-border 503	

ipv6 pim state-refresh origination-interval

Command	ipv6 pim state-refresh origination-interval <interval> no ipv6 pim state-refresh origination-interval	
	Configure transmission interval of state-refresh message. The “no ipv6 pim state-refresh origination-interval” command restores default value.	
Parameter	<interval>	packet transmission interval value is from 4s to 100s.
Default	60s。	
Mode	Global Mode.	
Usage	The first-hop router periodically transmits stat-refresh messages to maintain PIM-DM list ltems of all the downstream routers. The command can modify origination interval of state-refresh messages. Usually do not modify relevant timer interval. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.	
Example	Configure transmission interval of state-refresh message on interface vlan1 to 90s. Switch (Config-if-Vlan1)#ipv6 pim state-refresh origination-interval 90	

show ipv6 pim interface

Command	show ipv6 pim interface [detail]

	Display PIM interface information	
Parameter		
Default	None	
Mode	Any Mode.	
Usage	Display PIM interface information	
Example	<pre>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</pre>	
	Displayed Information	Explanations
	Address	Interface address
	Interface	Interface name
	VIF index	Interface index
	Ver/Mode	Pim version and mode,usually v2,sparse mode displays S,dense mode displays D
	Nbr Count	The interface's neighbor count
	DR Prior	Dr priority
	DR	The interface's DR address

show ipv6 pim mroute dense-mode

Command	show ip pim mroute dense-mode [group <X:X::X:X>] [source <X:X::X:X>]	
	Display PIM-DM message forwarding items.	
Parameter	group <X:X::X:X>	displays forwarding items relevant to this multicast address.
	source <X:X::X:X>	displays forwarding items relevant to this source.
Default	Do not display.	
Mode	Admin Mode	
Usage	The command shows PIM-DM multicast forwarding items, namely forwarding items of	

forward multicast packet in system FIB table.

Example

Display all of PIM-DM message forwarding items.
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.....

Displayed Information

(* , ff1e::15)

(2000:10:1:12::11, ff1e::15)

RPF nbr

RPF idx

Upstream State

Origin State

Local

Pruned

Explanations

(* ,G) Forwarding item

(S,G) Forwarding item

Backward path neighbor, upstream neighbor of source direction in DM, 0.0.0.0 expresses the switch is the first hop.

Interface located in RPF neighbor

Upstream direction, including FORWARDING(forwarding upstream data), PRUNED(Upstream stops forwarding data), ACKPENDING(waiting for upstream response, forwarding upstream data)

The two states: ORIGINATOR(on transmit state-refresh state), NON_ORIGINATOR(on non_transmit state-refresh state)

Local position joins interface, the interface receives IGMP Join

PIM prunes interface, the interface receives Prune messages

Asserted Outgoing	Asserted state Multicast data finally exported from interface is index number, index is 2 in this case. It can check interface information in detail by commanding show ip pim interface

show ipv6 pim neighbor

Command **show ipv6 pim neighbor**

Display router neighbors

**Parameter
Default**

Mode Admin and configuration Mode

Usage Display multicast router neighbors maintained by the 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:face Vlan1 00:00:13/00:01:32 v2 1 /

Displayed Information	Explanations
Neighbor Address	Neighbor address
Interface	Neighbor interface
Uptime/Expires	Running time /overtime
Ver	Pim version ,v2 usually
DR Priority/Mode	DR priority in the hello messages from the neighbor and if the neighbor is the interface's DP.

show ipv6 pim nexthop

Command **show ip pim nexthop**

	Display the PIM buffered nexthop router in the unicast route table																					
Parameter																						
Default	None																					
Mode	Admin and configuration Mode																					
Usage	Display the PIM buffered nexthop router information.																					
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 <table><tr><td>Displayed Information</td><td>Explanations</td></tr><tr><td>Destination</td><td>Destination of next item</td></tr><tr><td>Type</td><td>N: created nexthop, RP direction and S direction are not determined . R: RP direction S: source direction U: can't reach</td></tr><tr><td>Nexthop Num</td><td>Nexthop number</td></tr><tr><td>Nexthop Addr</td><td>Nexthop address</td></tr><tr><td>Nexthop Ifindex</td><td>Nexthop interface index</td></tr><tr><td>Nexthop Name</td><td>Nexthop name</td></tr><tr><td>Metric</td><td>Metric Metric to nexthop</td></tr><tr><td>Pref</td><td>Preference Route preference</td></tr><tr><td>Refcnt</td><td>Reference count</td></tr></table>		Displayed Information	Explanations	Destination	Destination of next item	Type	N: created nexthop, RP direction and S direction are not determined . R: RP direction S: source direction U: can't reach	Nexthop Num	Nexthop number	Nexthop Addr	Nexthop address	Nexthop Ifindex	Nexthop interface index	Nexthop Name	Nexthop name	Metric	Metric Metric to nexthop	Pref	Preference Route preference	Refcnt	Reference count
Displayed Information	Explanations																					
Destination	Destination of next item																					
Type	N: created nexthop, RP direction and S direction are not determined . R: RP direction S: source direction U: can't reach																					
Nexthop Num	Nexthop number																					
Nexthop Addr	Nexthop address																					
Nexthop Ifindex	Nexthop interface index																					
Nexthop Name	Nexthop name																					
Metric	Metric Metric to nexthop																					
Pref	Preference Route preference																					
Refcnt	Reference count																					

7 PIM-SM6

clear ipv6 pim bsr rp-set

Command	clear ipv6 pim bsr rp-set *
	Clear all RP.
Parameter	
Default	
Mode	Admin Configuration Mode

Usage	Clear all RP rapidly.

Example	Switch# clear ipv6 pim bsr rp-set *

debug ipv6 pim event

Command	debug ipv6 pim event no debug ipv6 pim event

Parameter	Enable or Disable pim event debug switch

Default	Disabled

Mode	Admin Mode

Usage	Enable pim event debug switch and display events information about pim operation.

Example	Switch# debug ipv6 pim event Switch#

debug ipv6 pim mfc

Command	debug ipv6 pim mfc (in out) no debug ipv6 pim mfc (in out)

Parameter	Enable or Disable pim mfc debug switch

Default	Disabled

Mode	Admin Mode
Usage	Enable pim mfc debug switch and display generated and transmitted multicast id's information.
Example	Switch# debug ipv6 pim mfc

debug ipv6 pim mib

Command	debug ipv6 pim mib no debug ipv6 pim mib
Parameter	Enable or Disable PIM MIB debug switch
Default	Disabled
Mode	Admin Mode
Usage	Inspect PIM MIB information by PIM MIB debug switch. It's not available now and it's for the future extension.
Example	Switch# debug ipv6 pim mib Switch#

debug ipv6 pim nexthop

Command	debug ipv6 pim nexthop no debug ipv6 pim nexthop
Parameter	Enable or Disable pim nexthop debug switch

Default	Disabled
Mode	Admin Mode
Usage	Inspect PIM NEXTHOP changing information by the pim nexthop switch.
Example	Switch# debug ipv6 pim nexthop Switch#

debug ipv6 pim nsm

Command	debug ipv6 pim nsm no debug ipv6 pim nsm
Parameter	Enable or Disable pim debug switch communicating with Network Services
Default	Disabled
Mode	Admin Mode
Usage	Inspect the communicating information between PIM and Network Services by this switch.
Example	Switch# debug ipv6 pim nsm Switch#

debug ipv6 pim packet

Command	debug ipv6 pim packet [in out]

no debug ipv6 pim packet [in|out|]

Parameter	Enable or Disable pim debug switch	
	in	display only received pim packets
	out	display only transmitted pim packets
Default	None	display both
	Disabled	
Mode	Admin Mode	
Usage	Inspect the received and transmitted pim packets by this switch.	
Example	Switch# debug ipv6 pim packet in Switch#	

debug ipv6 pim state

Command	debug ipv6 pim state no debug ipv6 pim state	
Parameter	Enable or Disable pim debug switch	
Default	Disabled	
Mode	Admin Mode	
Usage	Inspect the changing information about pim state by this switch.	
Example	Switch# debug ipv6 pim state Switch#	

debug ipv6 pim packet

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

Enable or Disable each pim timer

Parameter	
Default	Disabled
Mode	Admin Mode
Usage	Enable the specified timer's debug information.
Example	Switch# debug ipv6 pim timer assert Switch#

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>]
	To configure static multicast entry. The no command will delete some static multicast entries or some egress interfaces.
Parameter	<X:X::X:X> are the source address and group address of multicast. <X:X::X:X>
	<ifname> <.ifname> the first one is ingress interface, follow is egress interface.
Default	To delete this static multicast entry, if the command isn't included interface parameter.
Mode	Global Mode
Usage	The <ifname> should be valid VLAN interfaces. The multicast data flow will not be forwarded unless PIM is configured on the egress interface and the interface is UP. If the state of the interface is not UP, or PIM is not configured, or RPF is not valid, the multicast data flow will not be forwarded. To removed the specified multicast routing entry. If all the egress interfaces are specified, or no interfaces are specified, the specified multicast routing entry will be removed. Otherwise the multicast routing entry for the specified interface will be removed.
Example	Switch(config)#ipv6 mroute 10.1.1.1 225.1.1.1 v10 v20 v30

ipv6 multicast unresolved-cache aging-time

Command	ipv6 multicast unresolved-cache aging-time <value> no ipv6 multicast unresolved-cache aging-time
	Configure the cache time of the kernel multicast route, the no command restores the default value.

Parameter	< value>	is the configured cache time, ranging between 1 and 20s.
Default	20s。	
Mode	Global Mode	
Usage	Configure the cache time of multicast route entry in kernel.	
Example	Switch(config)# ipv6 multicast unresolved-cache aging-time 18	

ipv6 pim accept-register

Command	ipv6 pim accept-register list <access-list-name> no ipv6 pim accept-register	
	Filter the specified multicast group and multicast address.	
Parameter	<access-list-name>	is the access-list number, it ranges from 100 to 199.
Default	Permit the multicast registers from any sources to any groups.	
Mode	Global Mode	
Usage	This command is used to configure the access-list filtering the PIM REGISTER packets. The addresses of the access-list respectively indicate the filtered multicast sources and multicast groups' information. For the source-group combinations that match DENY, PIM sends REGISTER-STOP immediately and does not create group records when receiving REGISTER packets. Unlike other access-list, when the access-list is configured, the default value is PERMIT.	
Example	Configure the filtered register message's rule to myfilter. <pre>Switch(config)#ipv6 pim accept-register list myfilter Switch(config)#ipv6 access-list standard myfilter Switch(config_IPv6_Std-Nacl-myfilter)#permit fflc::10/128</pre>	

ipv6 pim bsr-border

Command	ipv6 pim bsr-border no ipv6 pim bsr-border	
	To configure or delete PIM BSR-BORDER interface.	
Parameter		
Default	Non-BSR-BORDER.	
Mode	Interface Configuration Mode。	

Usage	To configure the interface as the BSR-BORDER. If configured, BSR related messages will not receive from or sent to the specified interface. All the networks connected to the interface will be considered as directly connected.
Example	Switch(Config-if-Vlan1)#ipv6 pim bsr-border

ipv6 pim bsr-candidate

Command	ipv6 pim bsr-candidate {vlan <vlan-id> <ifname>} [hash-mask-length] [priority] no ipv6 pim bsr-candidate	
	This command is the candidate BSR configure command in global mode and is used to configure PIM-SM information about candidate BSR in order to compete the BSR router with other candidate BSRs. The command “no ipv6 pim bsr-candidate {vlan <vlan_id> tunnel <tunnel-id> <ifname>} [<hash-mask-length>] [<priority>]”command disables the candidate BSR.	
Parameter	vlan-id	is VLAN ID ,the value ranges from 1 to 4094;
	ifname	is the specified interface’s name
	[hash-mask-length]	is the specified hash mask length. It’s used for the RP enable selection and ranges from 0 to 32
	[priority]	is the candidate BSR priority and ranges from 0 to 255. If this parameter is not configured, the default priority value is 0
Default	This switch is not a candidate BSR router.	
Mode	Global Mode.	
Usage	This command is the candidate BSR configure command in global mode and is used to configure PIM-SM information about candidate BSR in order to compete with other candidate BSRs for the BSR router. Only this command is configured, this switch is the BSR candidate router.	
Example	Globally configure the interface vlan1 as the candidate BSR-message transmitting interface. <pre>Switch (config)# ipv6 pim bsr-candidate vlan1 30 10 Switch (config)#</pre>	

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>]

	Configure the register packet's checksum of the group specified by myfilter to use the whole packet's length.
Parameter	<access-list name> is the applying simple access-list.
Default	Compute the checksum according to the register packet's head length, default: 8
Mode	Global Mode
Usage	This command is used to interact with older Cisco IOS version.
Example	Configure the register packet's checksum of the group specified by myfilter to use the whole packet's length. <pre>Switch(config)#ipv6 pim cisco-register-checksum group-list myfilter Switch(config)#ipv6 access-list standard myfilter Switch(config_IPv6_Std-Nacl-myfilter)#permit ffe::10/128</pre>

ipv6 pim dr-priority

Command	ipv6 pim dr-priority <priority> no ipv6 pim dr-priority
	Configure, disable or change the interface's DR priority. The neighboring nodes in the same net segment select the DR in their net segment according to hello packets. The "no ipv6 pim dr-priority" command restores the default value.
Parameter	<priority> priority, it ranges from 0 to 4294967294
Default	1
Mode	Interface Configuration Mode
Usage	Range from 0 to 4294967294, the higher value has more priority. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.
Example	<pre>Switch (config)# interface vlan 1 Switch(Config-if-Vlan1)ipv6 pim dr-priority 100</pre>

ipv6 pim exclude-genid

Command	ipv6 pim exclude-genid no ipv6 pim exclude-genid
	This command makes the Hello packets sent by PIM SM do not include GenId option. The "no ipv6 pim exclude-genid" command restores the default value
Parameter	

Default	The Hello packets include GenId option.
Mode	Interface Configuration Mode
Usage	This command is used to interact with older Cisco IOS version. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.
Example	Configure the Hello packets sent by the switch do not include GenId option. Switch(Config-if-Vlan1)#ipv6 pim exclude-genid

ipv6 pim hello-holdtime

Command	ipv6 pim hello-holdtime <value> no ipv6 pim hello-holdtime
	Configure or disable the Holdtime option in the Hello packets, this value is to describe neighbor holdtime, if the switch hasn't received the neighbor hello packets when the holdtime is over, this neighbor is deleted. The "no ipv6 pim hello-holdtime" command cancels configured holdtime value and restores default value.
Parameter	<vaule> is the value of holdtime. Range <1-65535>.
Default	The default value of Holdtime is 3.5*Hello_interval, Hello_interval's default value is 30s, so Hold time's default value is 105s.
Mode	Interface Configuration Mode
Usage	If this value is not configured, hellotime's default value is 3.5*Hello_interval. If the configured holdtime is less than the current hello_interval, this configuration is denied. Every time hello_interval is updated, the Hello_holdtime will update according to the following rules: If hello_holdtime is not configured or hello_holdtime is configured but less than current hello_interval, hello_holdtime is modified to 3.5*hello_interval, otherwise the configured value is maintained. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.
Example	Configure vlan1's Hello Holdtime Switch (config)# interface vlan1 Switch (Config-if-Vlan1)#ipv6 pim hello-holdtime 10

ipv6 pim hello-interval

Command	ipv6 pim hello-interval <interval>

no ipv6 pim hello-interval

Configure the interface's hello_interval of pim hello packets. The "no ipv6 pim hello-interval" command restores the default value.

Parameter	<interval> is the hello_interval of periodically transmitted pim hello packets', ranges from 1 to 18724s.
Default	The default periodically transmitted pim hello packets' hello_interval is 30s.
Mode	Interface Configuration Mode
Usage	Hello messages make pim switches oriented each other and determine neighbor relationship. Pim switch announce the existence of itself by periodically transmitting hello messages to neighbors. If no hello messages from neighbors are received in the certain time, the neighbor is considered lost. This value can't be greater than neighbor overtime. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully
Example	Configure VLAN's pim-sm hello interval Switch (config)#interface vlan 1 Switch (Config-If-Vlan1)#ipv6 pim hello-interval 20 Switch (Config-If-Vlan1)#

ipv6 pim ignore-rp-set-priority

Command	ipv6 pim ignore-rp-set-priority no ipv6 pim ignore-rp-set-priority
	When RP selection is carried out, this command configures the switch to enable Hashing regulation and ignore RP priority. This command is used to interact with older Cisco IOS versions.
Parameter	
Default	Disabled
Mode	Global Mode
Usage	When selecting RP, Pim usually will select according to RP priority. When this command is configured, pim will not select according to RP priority. Unless there are older routers in the net, this command is not recommended.
Example	Switch (config)#ipv6 pim ignore-rp-set-priority Switch (config)#

ipv6 pim jp-timer

Command	ipv6 pim jp-timer <value> no ipv6 pim jp-timer	
	Configure to add JP timer. The “no ipv6 pim jp-timer” command restores the default value.	
Parameter	<value>	ranges from 10 to 65535s
Default	60s	
Mode	Global Mode	
Usage	Configure the interval of transmitting J/P messages to 59s.	
Example	Switch (config)#ip pim jp-timer 59 Switch (config)#	

ipv6 pim multicast-routing

Command	ipv6 pim multicast-routing no ipv6 pim multicast-routing	
	Enable PIM-SM globally. The “no ipv6 pim multicast-routing” command disables PIM-SM globally.	
Parameter		
Default	Disabled PIM-SM	
Mode	Global Mode	
Usage	Enable PIM-SM globally. The interface must enable PIM-SM to have PIM-SM work	
Example	Enable PIM-SM globally Switch (config)#ipv6 pim multicast-routing Switch (config)#	

ipv6 pim neighbor-filter

Command	ipv6 pim neighbor-filter <access-list-name> no ipv6 pim neighbor-filter <access-list-name>	
	Configure the neighbor access-list. If filtered by the lists and connections with	

neighbors are created, this connections are cut off immediately. If no connection is created, this connection can't be created.

Parameter	<access-list-name> is the applying access-list' name
Default	No neighbor filter configuration.
Mode	Interface Configuration Mode
Usage	ACL's default is DENY. If configuring access-list 1, access-list 1's default is deny. In the following example, if "permit any" is not configured, deny fe80:20e:cff:fe01:facc is the same as deny any. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.
Example	Configure VLAN's pim neighbor access-list. 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/128 Switch(config)#ipv6 access-list standard myfilter Switch(config_IPv6_Std-Nacl-myfilter)#permit any

ipv6 pim register-rate-limit

Command	ipv6 pim register-rate-limit <limit> no ipv6 pim register-rate-limit
	This command is used to configure the speedrate of DR sending register packets; the unit is packet/second. The "no ipv6 pim Register-rate-limit" command restores the default value. This configured speedrate is each (S, G) state's ,not the whole system's.
Parameter	<limit> ranges from 1 to 65535.
Default	No limit for sending speed
Mode	Global Mode
Usage	This configuration is to prevent the attack to DR, limiting sending REGISTER packets.
Example	Configure the speedrate of DR sending register packets to 59p/s. Switch (config)#ipv6 pim register-rate-limit 59 Switch (config)#

ipv6 pim register-rp-reachability

Command	ipv6 pim register-rp-reachability no ipv6 pim register-rp-reachability
Parameter	This command makes DR check the RP reachability in the process of registration.
Default	Do not check
Mode	Global Mode
Usage	This command configures DR whether or not to check the RP reachability.
Example	Configure the router to check the RP reachability before sending register packets. Switch(config)# ipv6 pim Register-rp-reachability

ipv6 pim register-source

Command	ipv6 pim register-source {<source-address> <ifname> vlan <vlan-id>} no ipv6 pim register-source						
Parameter	This command is to configure the source address of register packets sent by DR to overwrite default source address. This default source address is usually the RPF neighbor of source host direction. <table><tr><td><ifname></td><td>is the interface name that will be the register packets source.</td></tr><tr><td><vlan-id></td><td>is VLAN ID</td></tr><tr><td><source-address></td><td>is the interface address will be the register packets source. In the format of hex without prefix length.</td></tr></table>	<ifname>	is the interface name that will be the register packets source.	<vlan-id>	is VLAN ID	<source-address>	is the interface address will be the register packets source. In the format of hex without prefix length.
<ifname>	is the interface name that will be the register packets source.						
<vlan-id>	is VLAN ID						
<source-address>	is the interface address will be the register packets source. In the format of hex without prefix length.						
Default	Do not check						
Mode	Global Mode						
Usage	The “ no ipv6 pim register-source ” command restores the default value, no more parameter is needed. Configured address must be reachable to Register-Stop messages sent by RP. It’s usually a circle address, but it can be other physical addresses. This address must be announcable through unicast router protocols of DR.						
Example	Configure the source address of the sent register packets to vlan1’s address Switch (config)#ipv6 pim register-source vlan 1 Switch (config)#						

ipv6 pim register-suppression

Command	ipv6 pim register-suppression <value> no ipv6 pim register-suppression	
	This command is to configure the value of register suppression timer, the unit is second. The “no ipv6 pim register-suppression” command restores the default value.	
Parameter	<value>	is the timer’s value; it ranges from 10 to 65535s.
Default	60s	
Mode	Global Mode	
Usage	If this value is configured at DR, it’s the value of register suppression timer; if this value is configured at RP and ipv6 pim rp-register-kat is not used at RP, this command modifies Keepalive-period value. The “no ipv6 pim register-suppression” command restores the default value.	
Example	Configure the value of register suppression timer to 30s. Switch (config)#ipv6 pim register-suppression 30 Switch (config)#	

ipv6 pim rp-address

Command	ipv6 pim rp- address <rp-address> [<group-range>] no ipv6 pim rp-address <rp-address> [all]<group-range>]	
	This command is to configure static RP globally or in a multicast address range. The “no ipv6 pim rp-address” command cancels static RP.	
Parameter	<rp-address>	is the RP address, the format is X:X::X:X , ipv6 address
	<group-range>	is the expected RP, the format is X:X::X:X/M , ipv6 address and prefix length all the ranges
	<all>	is all the range
Default	This switch is not a RP static router.	
Mode	Global Mode	
Usage	This command is to configure static RP globally or in a multicast address range.	
Example	Configure 2000:112::8 as RP address globally. Switch (config)# ipv6 pim rp-address 2000:112::8 ff1e::/64	

ipv6 pim rp-candidate

Command **ipv6 pim rp-candidate{vlan<vlan-id> |loopback<index> |<ifname>}[<group range>] [<priority>]**
no ipv6 pim rp-candidate

This command is the candidate RP global configure command, it is used to configure PIM-SM candidate RP information in order to compete RP router with other candidate RPs. The “no ipv6 pim rp-candidate” command cancels the candidate RP.

Parameter	vlan-id	is vlan ID
	<index>	indexing the Loopback interface
	ifname	is the name of the specified interface
	<group range>	is the group range of the candidate RP,the format is X:X::X:X/M, ipv6 address and prefix length;
	<priority>	is the RP selection priority, it ranges from 0 to 255, the default value is 192, the lower value has more priority

Default This switch is not a RP static router.

Mode Global Mode

Usage This command is the candidate RP global configure command, it is used to configure PIM-SM candidate RP information in order to compete RP router with other candidate RPs.Only this command is configured, this switch is the RP candidate router.

Example Configure vlan1 as the sending interface of candidate RP announcing sending messages
Switch (config)# ipv6 pim rp-candidate vlan1 100

ipv6 pim rp-register-kat

Command **ipv6 pim rp-register-kat <vaule>**
no ipv6 pim rp-register-kat

This command is to configure the KAT (KeepAlive Timer) value of the RP (S, G) items, the unit is second. The “no ipv6 pim rp-register-kat” command restores the default value.

Parameter	<value>	is the timer value; it ranges from 1 to 65535s.
Default	185s	

Mode Global Mode

Usage Configure rp-register-kat interval to 30s.

Example Switch(config)# ipv6 pim rp-register-kat 30

ipv6 pim scope-border

Command	ipv6 pim scope-border [<500-599> <acl_name>] no ipv6 pim scope-border	
	To configure or delete management border of PIM.	
Parameter	<500-599>	is the ACL number for the management border.
	<acl_name>	is the ACL name for the management border.
Default	Not management border. If no ACL is specified, the default management border will be used.	
Mode	Interface Configuration Mode。	
Usage	To configure the management border and the ACL for the IPV6 PIM. The multicast data flow will not be forwarded to the SCOPE-BORDER.	
Example	Switch(Config-if-Vlan2)#ipv6 pim scope-border 503	

ipv6 pim sparse-mode

Command	ipv6 pim sparse-mode [passive] no ipv6 pim sparse-mode [passive]	
	Enable PIM-SM on the interface; the “no ipv6 pim sparse-mode [passive]” command disables PIM-SM.	
Parameter	[passive]	means to disable PIM-SM (that's PIM-SM doesn't receive any packets) and only enable MLD(receive and transmit MLD packets).
Default	Do not enable PIM-SM	
Mode	Interface Configuration Mode	
Usage	Enable PIM-SM on the interface. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.	
Example	Enable PIM-SM on the interface vlan1. Switch(config)#interface vlan 1 Switch(Config-If-Vlan1)#ipv6 pim sparse-mode	

show ipv6 pim bsr-router

Command	show ipv6 pim bsr-router	
	Display BSR address	
Parameter		
Default	None	
Mode	Admin Mode and Global Mode	
Usage	Display the BSR information maintained by the PIM.	
Example	<pre>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) Displayed Information Explanations BSR address Bsr-router Address Priority Bsr-router Priority Hash mask length Bsr-router hash mask length State The current state of this candidate BSR, Elected BSR is selected BSR</pre>	

show ipv6 pim interface

Command	show ipv6 pim interface	
	Display PIM interface information	
Parameter		
Default	None	
Mode	Any Mode	
Usage	Display PIM interface information	
Example	<pre>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</pre>	

Vlan3 2 v2/S 0 1 Address : fe80::203:fff:fee3:1244 Global Address: 2000:10:1:13::1 DR : this system	
Displayed Information	Explanations
Address	Interface address
Interface	Interface name
VIF index	Interface index
Ver/Mode	Pim version and mode,usually v2,sparse mode displays S,dense mode displays D
Nbr Count	The interface's neighbor count
DR Prior	Dr priority
DR	The interface's DR address

show ipv6 pim mroute sparse-mode

Command	show ipv6 pim mroute sparse-mode
Parameter	Display the multicast route table of PIM-SM.
Default	None
Mode	Admin Mode and Configuration Mode
Usage	Display the BSP routers in the network maintained by PIM-SM.
Example	Switch#show ipv6 pim mroute sparse-mode 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, ffe::15)
RPF nbr: ::
RPF idx: None
SPT bit: 1
Upstream State: JOINED
Local .....
Joined .....
Asserted .....
Outgoing ..o.....
(2000:1:111::11, ffe::15, rpt)
RP: 2000:1:111::100
RPF nbr: ::
RPF idx: None
Upstream State: NOT PRUNED
Pruned .....
Outgoing ..o.....

```

Displayed Information

Entries

RP

RPF nbr

RPF idx

Upstream State

Local

Joined

Asserted

Outgoing

Explanations

The counts of each item

Share tree's RP address

RP direction or upneighbor of source direction.

RPF nbr interface

Upstream State, there are two state of Joined(join the tree, expect to receive data from upstream) and Not Joined(quit the tree, not expect to receive data from upstream), and more options such as RPT Not Joined, Pruned, Not Pruned are available for (S,G,rpt.)

Local join interface, this interface receive IGMPJoin

PIM join interface, this interface receive J/P messages

Asserted state

Final outgoing of multicast data

show ipv6 pim neighbor

Command

show ipv6 pim neighbor [detail]

	Display router neighbors													
Parameter														
Default	None													
Mode	Any Mode													
Usage	Display multicast router neighbors maintained by the 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 / <table><tr><th>Displayed Information</th><th>Explanations</th></tr><tr><td>Neighbor Address</td><td>Neighbor address</td></tr><tr><td>Interface</td><td>Neighbor interface</td></tr><tr><td>Uptime/Expires</td><td>Running time /overtime</td></tr><tr><td>Ver</td><td>Pim version ,v2 usually</td></tr><tr><td>DR Priority/Mode</td><td>DR priority in the hello messages from the neighbor and if the neighbor is the interface's DP.</td></tr></table>		Displayed Information	Explanations	Neighbor Address	Neighbor address	Interface	Neighbor interface	Uptime/Expires	Running time /overtime	Ver	Pim version ,v2 usually	DR Priority/Mode	DR priority in the hello messages from the neighbor and if the neighbor is the interface's DP.
Displayed Information	Explanations													
Neighbor Address	Neighbor address													
Interface	Neighbor interface													
Uptime/Expires	Running time /overtime													
Ver	Pim version ,v2 usually													
DR Priority/Mode	DR priority in the hello messages from the neighbor and if the neighbor is the interface's DP.													

show ipv6 pim nexthop

Command	show ipv6 pim nexthop
	Display the PIM buffered nexthop router in the unicast route table
Parameter	
Default	None
Mode	Any Mode
Usage	Display the PIM buffered nexthop router information.
Example	<pre>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</pre>

Displayed Information	Explanations
Destination	Destination of next item
Type	N: created nexthop, RP direction and S direction are not determined . R: RP direction S: source direction U: can't reach
Nexthop Num	Nexthop number
Nexthop Addr	Nexthop address
Nexthop Ifindex	Nexthop interface index
Nexthop Name	Nexthop name
Metric	Metric Metric to nexthop
Pref	Preference Route preference
Refcnt	Reference count

show ipv6 pim rp-hash

Command	show ip pim rp-hash X:X::X:X	
	: Display the RP address of group X:X::X's merge point.	
Parameter	X:X::X:X	Group address
Default	None	
Mode	Any Mode	
Usage	Display the RP address corresponding to 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	
	Displayed Information	Explanations
	RP	Queried group'sRP
	Info source	The source of Bootstrap information

show ipv6 pim rp mapping

Command	show ipv6 pim rp mapping

Display Group-to-RP Mapping and RP.									
Parameter									
Default	None								
Mode	Any Mode								
Usage	Display the current RP and mapping relationship.								
Example	<pre>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</pre> <table> <tr> <td>Displayed Information</td><td>Explanations</td></tr> <tr> <td>Group(s)</td><td>Group address range of RP</td></tr> <tr> <td>Info source</td><td>Source of Bootstrap messages</td></tr> <tr> <td>Priority</td><td>Priority of Bootstrap messages</td></tr> </table>	Displayed Information	Explanations	Group(s)	Group address range of RP	Info source	Source of Bootstrap messages	Priority	Priority of Bootstrap messages
Displayed Information	Explanations								
Group(s)	Group address range of RP								
Info source	Source of Bootstrap messages								
Priority	Priority of Bootstrap messages								

8 PIM-SSM6

ipv6 pim ssm

Command	ipv6 pim ssm {default range [<access-list-number> WORD]} no ipv6 pim ssm	
	Configure the range of pim ssm multicast address. The "no ipv6 pim ssm" command deletes configured pim ssm multicast group.	
Parameter	default	indicates the default range of pim ssm multicast group is ff3x::/32.
	range	Pim SSM group range
	<access-list-number>	is the name of applying access-list(500-599).
	WORD	IPv6 Named Standard Access list
Default	Do not configure the range of pim ssm group address.	
Mode	Global Mode.	
Usage	1. Only this command is configured, pim ssm can be available.	

2. Before configuring this command, make sure ipv6 pim multicasting succeed.
3. Access-list only can use the lists created by ipv6 access-list.
4. Users can execute this command first and then configure the corresponding acl; or delete corresponding acl in the bondage. After the bondage, only command no ipv6 pim ssm can release the bondage.
5. If ssm is needed, this command should be configured at the related edge route. For example, the local switch with igmp(must) and multicast source DR or RP(at least one of the two) configure this command, the middle switch need only enable PIM-SM.

Example	Configure the switch to enable PIM-SSM, the group's range is what is specified by access-list 23. Switch (config)#ipv6 pim ssm range 520 Switch(config)#ipv6 access-list standard myfilter Switch(config_IPv6_Std-Nacl-myfilter)#permit ffile::/48

9 ANYCAST RP v4

debug pim anycast-rp

Command	debug pim anycast-rp no debug pim anycast-rp
Parameter	Enable the debug switch of ANYCAST RP function; the no operation of this command will disable this debug switch.
Default	The debug switch of ANYCAST RP is disabled by default
Mode	Admin Mode.
Usage	This command is used to enable the debug switch of ANYCAST RP of the router, it can display the information of handling PIM register packet of the switch——packet, and the information of events——event.
Example	Switch#debug pim anycast-rp

ip pim anycast-rp

Command	ip pim anycast-rp no ip pim anycast-rp
	Enable the ANYCAST RP of the switch; the no operation of this command is to

Parameter	disable the ANYCAST RP function.
Default	The switch will not enable the ANYCAST RP by default.
Mode	Global Configuration Mode
Usage	This command will globally enable ANYCAST RP protocol, but in order to make ANYCAST RP work, it is necessary to configure self-rp-address and other-rp-address set.
Example	Enable ANYCAST RP in global configuration mode. Switch(config)#ip pim anycast-rp

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>
	Configure ANYCAST RP address (ARA) and the unicast addresses of other RP communicating with this router (as a RP). The no operation of this command will cancel the unicast address of another RP in accordance with the configured RP address.
Parameter	anycast-rp-addr: RP address, the absence of the candidate interface in accordance with the address is allowed. other-rp-addr: The unicast address of other RP communicating with this router (as a RP).
Default	There is no configuration by default.
Mode	Global Configuration Mode
Usage	1. The anycast-rp-addr configured on this router (as a RP) is actually the RP address configured on multiple RP in the network, in accordance with the address of RP candidate interface (or Loopback interface). The current absence of the candidate interface in accordance with the address is allowed when configuring. 2. Configure the other-rp-address of other RP communicating with this router (as a RP). The unicast address identifies other RP, and is used to communicate with the local router. 3. Once this router (as a RP) receives the register message from a DR unicast, it should forward it to other RP in the network to notify all the RP in the network of the source (S,G) state. While forwarding, the router will change the destination address of the register message into other-rp-address. 4. Multiple other-rp-addresses can be configured in accordance with one anycast-rp-addr, once the register message from a DR is received; it should be forwarded to all of these

other RP one by one.

Example

```
Configure other-rp-address in global configuration mode.  
Switch(config)#ip pim anycast-rp 1.1.1.1 192.168.3.2
```

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

Configure the self-rp-address of this router (as a RP). This address will be used to exclusively identify this router from other RP, and to communicate with other RP. The no operation of this command will cancel the configured unicast address used by this router (as a RP) to communicate with other RP.

Parameter

self-rp-addr	The unicast address used by this router (as a RP) to communicate with other RP.

Default

No self-rp-address is configured by default.

Mode

Global Configuration Mode

Usage

1. Once this router (as a RP) receives the register message from DR unicast, it needs to forward the register message to all the other RP in the network, notifying them of the state of source (S,G). While forwarding the register message, this router will change the source address of it into self-rp-address.
2. Once this router(as a RP) receives a register message from other RP unicast, such as a register message whose destination is the self-rp-address of this router, it will create (S,G) state and send back a register-stop message, whose destination address is the source address of the register message.
3. self-rp-address has to be the address of a three-layer interface on this router, but the configuration is allowed to be done with the absence of the interface.

Example

```
Configure the self-rp-address of this router in global configuration mode.  
Switch(config)#ip pim anycast-rp self-rp-address 1.1.1.1
```

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

Add a Loopback interface as a RP candidate interface based on the original PIM-

	SM command; the no operation of this command is to cancel the Loopback interface as a RP candidate interface.
Parameter	index: Loopback interface index, whose range is <1-1024>. vlan-id: the VLAN ID. ifname: the specified name of the interface. A.B.C.D/M: the ip prefix and mask. <priority>: the priority of RP election, ranging from 0 to 255, the default value is 192, the smaller the value is the higher the priority is.
Default	No RP interface is configured by default.
Mode	Global Configuration Mode
Usage	In order to support ANYCAST RP function, new rule allows configuring a Loopback interface to be the RP candidate interface, the RP candidate interface should be currently unique, and the address of which should be added into the router to make sure that PIM router can find the nearest RP. The “no ip pim rp-candidate” command can be used to cancel the RP candidate.
Example	Configure Loopback1 interface as the RP candidate interface in global configuration mode. Switch(config)#ip pim rp-candidate loopback1

show debugging pim

Command	show debugging pim
Parameter	
Default	-
Mode	Admin Mode.
Usage	The current state of ANYCAST RP debug switch.
Example	Switch(config)#show debugging pim Debugging status: PIM anycast-rp debugging is on

show ip pim anycast-rp first-hop

Command	show ip pim anycast-rp first-hop

Parameter	-						
Default	-						
Mode	Admin and Configuration Mode.						
Usage	Display the state information of ANYCAST RP, and display the mrt node information generated in the first hop RP which is currently maintained by the protocol.						
Example	<pre>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.....</pre> <table> <tr> <td>Display</td><td>Explanation</td></tr> <tr> <td>Entries</td><td>The number of all kinds of entries.</td></tr> <tr> <td>INCLUDE</td><td>The information of mrt generated in the first hop RP.</td></tr> </table>	Display	Explanation	Entries	The number of all kinds of entries.	INCLUDE	The information of mrt generated in the first hop RP.
Display	Explanation						
Entries	The number of all kinds of entries.						
INCLUDE	The information of mrt generated in the first hop RP.						

show ip pim anycast-rp non-first-hop

Command	show ip pim anycast-rp non-first-hop
Parameter	-
Default	-
Mode	Admin and Configuration Mode.
Usage	Display the state information of ANYCAST RP, and display the mrt node information generated in the non first hop RP which is currently maintained by the protocol, that is the mrt node information which is created after the first hop RP transfers the register message it received to this RP.
Example	<pre>Switch(config)#show ip pim anycast-rp non-first-hop IP Multicast Routing Table (*,G) Entries: 0</pre>

```

(S,G) Entries: 1
(E,G) Entries: 0
INCLUDE (192.168.10.120, 225.1.1.1)
Local .l.....

```

Display	Explanation
Entries	The number of all kinds of entries.
INCLUDE	The mrt information created in the first hop RP.

show ip pim anycast-rp status

Command **show ip pim anycast-rp status**

Parameter -

Default -

Mode Admin and Configuration Mode.

Usage Display the configuration information of ANYCAST RP, whether ANYCAST RP globally enables, whether the self-rp-address is configured and the list of currently configured ANYCAST RP set.

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
-----

```

Display	Explanation
anycast-rp:	Whether the ANYCAST RP switch is globally enabled.
self-rp-address:	The configured self-rp-address.
anycast-rp address:	The configured anycast-rp-address.
other rp unicast rp address:	The configured other RP communication addresses in

	accordance with the above anycast-rp-address.
other rp unicast rp address:	The configured other RP communication addresses in accordance with the above anycast-rp-address.
anycast-rp address:	The configured anycast-rp-address*.
other rp unicast rp address:	The configured other RP communication addresses in accordance with the above anycast-rp-address.

10 ANYCAST RP v6

debug ipv6 pim anycast-rp

Command	debug ipv6 pim anycast-rp no debug ipv6 pim anycast-rp
	Enable the debug switch of ANYCAST RP function; the no operation of this command will disable this debug switch.
Parameter	
Default	The debug switch of ANYCAST RP is disabled by default.
Mode	Admin Mode.
Usage	This command is used to enable the debug switch of ANYCAST RP of the router, it can display the information of handling PIM register packet of the switch——packet, and the information of events——event.
Example	Switch# debug ipv6 pim anycast-rp

ipv6 pim anycast-rp

Command	ipv6 pim anycast-rp no ipv6 pim anycast-rp
	Enable the ANYCAST RP of the switch; the no operation of this command is to disable the ANYCAST RP function.
Parameter	

Default	The switch will not enable the ANYCAST RP by default.
Mode	Global Configuration Mode
Usage	This command will globally enable ANYCAST RP protocol, but in order to make ANYCAST RP work, it is necessary to configure self-rp-address and other-rp-address set.
Example	Enable ANYCAST RP in global configuration mode. <pre>Switch(config)#ipv6 pim anycast-rp</pre>

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> Configure ANYCAST RP address (ARA) and the unicast addresses of other RP communicating with this router(as a RP). The no operation of this command will cancel the unicast address of another RP in accordance with the configured RP address.
Parameter	anycast-rp-addr : RP address, the current absence of the candidate interface in accordance with the address is allowed other-rp-addr: The unicast address of other RP communicating with this router(as a RP).
Default	There is no configuration by default.
Mode	Global Configuration Mode
Usage	1. The anycast-rp-addr configured on this router (as a RP) is actually the RP address configured on multiple RP in the network, in accordance with the address of RP candidate interface (or Loopback interface). The current absence of the candidate interface in accordance with the address is allowed when configuring. 2. Configure the other-rp-address of other RPs communicating with this router (as a RP). The unicast address identifies other RP, and is used to communicate with the local router. 3. Once this router (as a RP) receives the register message from a DR unicast, it should forward it to other RP in the network to notify all the RP in the network of the source (S,G) state. While forwarding, the router will change the destination address of the register message into other-rp-address. 4. Multiple other-rp-addresses can be configured in accordance with one anycast-rp-addr, once the register message from a DR is received, it should be forwarded to all of these other RP one by one.
Example	Configure other-rp-address in global configuration mode.

```
Switch(config)#ipv6 pim anycast-rp 2000::1 2004::2
```

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	
	Configure the self-rp-address of this router (as a RP). This address will be used to exclusively identify this router from other RP, and to communicate with other RP. The no operation of this command will cancel the configured unicast address used by this router (as a RP) to communicate with other RP.	
Parameter	self-rp-addr	The unicast address used by this router (as a RP) to communicate with other RP.
Default	No self-rp-address is configured by default.	
Mode	Global Configuration Mode	
Usage	1. Once this router (as a RP) receives the register message from DR unicast, it needs to forward the register message to all the other RP in the network, notifying them of the state of source (S,G). While forwarding the register message, this router will change the source address of it into self-rp-address. 2. Once this router(as a RP) receives a register message from other RP unicast, such as a register message whose destination is the self-rp-address of this router, it will create (S,G) state and send back a register-stop message, whose destination address is the source address of the register message. 3. self-rp-address has to be the address of a three-layer interface on this router, but the configuration is allowed to be done with the absence of the interface.	
Example	Configure the self-rp-address of this router in global configuration mode. Switch(config)#ipv6 pim anycast-rp self-rp-address 2000::1	

ipv6 pim rp-candidate

Command	ipv6 pim rp-candidate {vlan<vlan-id> loopback<index> <ifname>} [<A:B::C:D>] [<priority>] no ip pim rp-candidate	
	Add a Loopback interface as a RP candidate interface based on the original PIM6-SM command; the no operation of this command is to cancel the Loopback interface as a RP candidate interface.	

Parameter	index: Loopback interface index, whose range is <1-1024>. vlan-id: the Vlan ID. ifname: the specified name of the interface. A:B::C:D/M: the ip prefix and mask. <priority>: the priority of RP election, ranging from 0 to 255, the default value is 192, the smaller the value is the higher the priority is.
Default	No RP interface is configured by default.
Mode	Global Configuration Mode
Usage	In order to support ANYCAST RP function, new rule allows configuring a Loopback interface to be the RP candidate interface, the RP candidate interface should be currently unique, and the address of which should be added into the router to make sure that PIM router can find the nearest RP. The “no ipv6 pim rp-candidate” command can be used to cancel the RP candidate.
Example	Configure Loopback1 interface as the RP candidate interface in global configuration mode. Switch(config)#ipv6 pim rp-candidate loopback1

show debugging ipv6 pim

Command	show debugging ipv6 pim
Parameter	
Default	-
Mode	Admin and Configuration Mode.
Usage	The current state of ANYCAST RP debug switch.
Example	Switch(config)#show debugging ipv6 pim Debugging status: PIM anycast-rp debugging is on

show ipv6 pim anycast-rp first-hop

Command	show ipv6 pim anycast-rp first-hop

Parameter	-						
Default	-						
Mode	Admin and Configuration Mode.						
Usage	Display the state information of ANYCAST RP, and display the mrt node information generated in the first hop RP which is currently maintained by the protocol.						
Example	<pre>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, ff1e::1) Local .l.....</pre> <table> <tr> <td>Display</td><td>Explanation</td></tr> <tr> <td>Entries</td><td>The number of all kinds of entries.</td></tr> <tr> <td>INCLUDE</td><td>The mrt information created in the first hop RP.</td></tr> </table>	Display	Explanation	Entries	The number of all kinds of entries.	INCLUDE	The mrt information created in the first hop RP.
Display	Explanation						
Entries	The number of all kinds of entries.						
INCLUDE	The mrt information created in the first hop RP.						

show ipv6 pim anycast-rp non-first-hop

Command	show ipv6 pim anycast-rp non-first-hop
Parameter	-
Default	-
Mode	Admin and Configuration Mode.
Usage	Display the state information of ANYCAST RP, and display the mrt node information generated in the non first hop RP which is currently maintained by the protocol, that is the mrt node information which is created after the first hop RP transfers the register message it received to this RP.
Example	<pre>Switch(config)#show ip pim anycast-rp non-first-hop IP Multicast Routing Table (*,G) Entries: 0 (S,G) Entries: 1</pre>

(E,G) Entries: 0 INCLUDE (2002:1:111::2, ff1e::2) Local .l.....	
Display	Explanation
Entries	The number of all kinds of entries.
INCLUDE	The mrt information created in the first hop RP.

show ipv6 pim anycast-rp status

Command	show ipv6 pim anycast-rp status	
Parameter	-	
Default	-	
Mode	Admin and Configuration Mode.	
Usage	Display the configuration information of ANYCAST RP, whether ANYCAST RP globally enables, whether the self-rp-address is configured and the list of 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 -----	
	Display	Explanation
	anycast-rp:	Whether the ANYCAST RP switch is globally enabled.
	self-rp-address:	The configured self-rp-address.
	anycast-rp address:	The configured anycast-rp-address.
	other rp unicast rp address:	The configured other RP communication addresses in accordance with the above anycast-rp-address.
	other rp unicast rp address:	The configured other RP

	communication addresses in accordance with the above anycast-rp- address.
anycast-rp address:	The configured anycast-rp-address*.
other rp unicast rp address:	The configured other RP communication addresses in accordance with the above anycast-rp- address.

10-Commands for Security Function

1 Commands for ACL

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+Sunday} daily weekdays weekend} <start_time> to <end_time>																									
Parameter	<table><tr><td>Monday</td><td>Monday</td></tr><tr><td>Tuesday</td><td>Tuesday</td></tr><tr><td>Wednesday</td><td>Wednesday</td></tr><tr><td>Thursday</td><td>Thursday</td></tr><tr><td>Friday</td><td>Friday</td></tr><tr><td>Saturday</td><td>Saturday</td></tr><tr><td>Sunday</td><td>Sunday</td></tr><tr><td>daily</td><td>Every day of the week</td></tr><tr><td>weekdays</td><td>Monday thru Friday</td></tr><tr><td>weekend</td><td>Saturday thru Sunday</td></tr><tr><td><start_time></td><td>start time ,HH:MM:SS (hour: minute: second)</td></tr><tr><td><end_time></td><td>end time,HH:MM:SS (hour: minute: second)</td></tr></table>		Monday	Monday	Tuesday	Tuesday	Wednesday	Wednesday	Thursday	Thursday	Friday	Friday	Saturday	Saturday	Sunday	Sunday	daily	Every day of the week	weekdays	Monday thru Friday	weekend	Saturday thru Sunday	<start_time>	start time ,HH:MM:SS (hour: minute: second)	<end_time>	end time,HH:MM:SS (hour: minute: second)
Monday	Monday																									
Tuesday	Tuesday																									
Wednesday	Wednesday																									
Thursday	Thursday																									
Friday	Friday																									
Saturday	Saturday																									
Sunday	Sunday																									
daily	Every day of the week																									
weekdays	Monday thru Friday																									
weekend	Saturday thru Sunday																									
<start_time>	start time ,HH:MM:SS (hour: minute: second)																									
<end_time>	end time,HH:MM:SS (hour: minute: second)																									
Default	No time-range configuration.																									
Mode	time-range mode																									
Usage Guide	This command is used for the switch configuration command effective time-range. By creating a time period and referencing it in a command, the user can make the command take effect within the time range defined that time period. When, for example, a ACL rule only needs to take effect within a specific time range, it can be configured first and then referenced when configuring the ACL rule, so that the ACL rule can only take effect within the time range defined for that time period. In a time period, the time range can be defined in two ways: Absolute cycle time a period of time that takes effect within a specified time range, such as Tuesday 8:00 to Saturday 8:00. Periodic period: a period of time in which a cycle (such as 14 to 16:00 a week) takes effect. The no command to delete the configured time-range.																									
Example	Make configurations effective within the period from9:15:30 to 12:30:00 during Tuesday to Saturday.																									

```
Switch(config)#time-range admin_timer
Switch(config-time-range-admin_timer)#absolute-periodic Tuesday 9:15:30 to Saturday
12:30:00
```

Make configurations effective within the period from 14:30:00 to 16:45:00 on Monday, Wednesday, Friday and Sunday.

```
Switch(config-time-range-admin_timer)#periodic Monday Wednesday Friday Sunday
14:30:00 to 16:45:00
```

absolute start

Command [no] absolute start <start_time> <start_data> [end <end_time> <end_data>]

Parameter	<start_time>	start time ,HH:MM:SS (hour: minute: second)
	<start_data>	start data ,YYYY.MM.DD (year.month.day)
	<end_time>	end time ,HH:MM:SS (hour: minute: second)
	<end_data>	end data ,YYYY.MM.DD (year.month.day)

Default No time-range configuration by default.

Mode Time-range mode

Usage Guide Define an absolute time-range, this time-range operates subject to the clock of this equipment.
Absolute time and date, assign specific year, month, day, hour, minute of the start, shall not configure multiple absolute time and date, when in repeated configuration, the latter configuration covers the absolute time and date of the former configuration.

The no command delete configuration.

Example Make configurations effective from 6:00:00 to 13:30:00 from Oct. 1, 2004 to Jan. 26, 2005.

```
Switch(config)#time-range admin_timer
Switch(config-time-range-admin_timer)#absolute start 6:00:00 2004.10.1 end 13:30:00
2005.1.26
```

access-list (ip extended)

Command	access-list <num> {deny permit} icmp {{<slpAddr> <sMask>} any-source {host-source <slpAddr>}} {{<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 {{<slpAddr> <sMask>} any-source {host-source <slpAddr>}} {{<dIpAddr> <dMask>} any-destination {host-destination <dIpAddr>}} [<igmp-type>] [precedence <prec>] [tos <tos>][time-range <time-range-name>] access-list <num> {deny permit} tcp {{ <slpAddr> <sMask> } any-source {host-source <slpAddr> } } [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 {{ <slpAddr> <sMask> } any-source {host-source <slpAddr> } } [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 igmp ipinip ip ospf <protocol-num> } {{ <slpAddr> <sMask> } any-source {host-source <slpAddr> } } {{ <dIpAddr> <dMask> } any-destination {host-destination <dIpAddr> } } [precedence <prec>] [tos <tos>][time-range <time-range-name>] no access-list <num>

Parameter	<table> <tr> <td><num></td><td>the No. of access-list, 100-299</td></tr> <tr> <td>deny</td><td>deny packets</td></tr> <tr> <td>permit</td><td>permit packets</td></tr> <tr> <td><slpAddr></td><td>the source IP address, the format is dotted decimal notation</td></tr> <tr> <td><sMask></td><td>the reverse mask of source IP, the format is dotted decimal notation</td></tr> <tr> <td><sPort></td><td>source port No., 0-65535</td></tr> <tr> <td><sPortMin></td><td>the down boundary of source port</td></tr> <tr> <td><sPortMax></td><td>the up boundary of source port</td></tr> </table>	<num>	the No. of access-list, 100-299	deny	deny packets	permit	permit packets	<slpAddr>	the source IP address, the format is dotted decimal notation	<sMask>	the reverse mask of source IP, the format is dotted decimal notation	<sPort>	source port No., 0-65535	<sPortMin>	the down boundary of source port	<sPortMax>	the up boundary of source port
<num>	the No. of access-list, 100-299																
deny	deny packets																
permit	permit packets																
<slpAddr>	the source IP address, the format is dotted decimal notation																
<sMask>	the reverse mask of source IP, the format is dotted decimal notation																
<sPort>	source port No., 0-65535																
<sPortMin>	the down boundary of source port																
<sPortMax>	the up boundary of source port																

<protocol>	the No. of upper-layer protocol of ip, 0-255
<dIpAddr>	the destination IP address, the format is dotted decimal notation
<dMask>	the reverse mask of destination IP, the format is dotted decimal notation
<dPort>	destination port No. 0-65535
<dPortMin>	the down boundary of destination port
<dPortMax>	the up boundary of destination port
<igmp-type>	the type of igmp, 0-15
<icmp-type>	the type of icmp, 0-255
<icmp-code>	protocol No. of icmp, 0-255
<prec>	IP priority, 0-7
<tos>	to value, 0-15
<time-range-name>	the name of time-range

Default By default,no access-lists configured.

Mode Global mode

Usage Guide Create a numeric extended IP access rule to match specific IP protocol or all IP protocol;if access-list of this coded numeric extended does not exist,thus to create such a access-list. When the user assign specific <num> for the first time,ACL of the serial number is created,then the lists are added into this ACL;the access list which marked 200-299 can configure not continual reverse mask of IP address.

<igmp-type>represent the type of IGMP packet, and usual values please refer to the following description:

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

Particular notice:The packet types included here are not the types excluding IP OPTION. Normally, IGMP packet contains OPTION fields, and such configuration is of no use for this type of packet. If you want to configure the packets containing OPTION, please directly use the manner where OFFSET is configured.

The no command delete configuration.

Example Create the numeric extended access-list whose serial No. is 110. deny icmp packet to pass, and permit udp packet with destination address 192. 168. 0. 1 and destination port 32 to pass.

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

access-list (ip standard)

Command `access-list <num> {deny | permit} {{<slpAddr> <sMask >} | any-source}{host-source <slpAddr>}}`
`no access-list <num>`

Parameter	<num>	the No. of access-list, 100-199
	deny	deny packets
	permit	permit packets
	<slpAddr>	the source IP address, the format is dotted decimal notation
	<sMask>	the reverse mask of source IP, the format is dotted decimal notation

Default By default, no access-lists configured.

Mode Global mode

Usage Guide Create a numeric standard IP access-list. If this access-list exists, then add a rule list; When the user assigns specific <num> for the first time, ACL of the serial number is created, then the lists are added into this ACL.

The "no access-list <num>" operation of this command is to delete a numeric standard IP access-list.

Example Create a numeric standard IP access-list whose serial No. is 20, and permit data packets with source address of 10.1.1.0/24 to pass, and deny other packets with source address of 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
```

access-list(mac extended)

Command `access-list <num> {deny | permit} {any-source-mac | {host-source-mac <slpAddr>}} <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]
no access-list <num>

Parameter	<num>	the access-list No. which is a decimal's No. from 1100-1199
	deny	deny packets
	permit	permit packets
	any-source-mac	any source address
	host-source-mac	source mac address
	<slpAddr>	the source IP address, the format is dotted decimal notation
	<host_smac>	source mac address
	<smac>	source mac address
	<smac-mask>	mask (reverse mask) of source MAC address
	any-destination-mac	any destination address
	host-destination-mac	destination MAC address
	<host_dmac>	destination MAC address
	<dmac>	destination MAC address
	<dmac-mask>	mask (reverse mask) of destination MAC address
	untagged-eth2	format of untagged ethernet II packet
	tagged-eth2	format of tagged ethernet II packet;
	untagged-802-3	format of untagged ethernet 802.3 packet
	tagged-802-3	format of tagged ethernet 802.3 packet
Default	By default,no access-lists configured.	
Mode	Global mode	
Usage Guide	Define an extended numeric MAC ACL rule. When the user assign specific <num> for the first time, ACL of the serial number is created, then the lists are added into this ACL.	
	“no access-list <num>” command deletes an extended numeric MAC access-list rule.	
Example	Permit tagged-eth2 with any source MAC addresses and any destination MAC addresses and the packets pass.	
	Switch(config)#access-list 1100 permit any-source-mac any-destination-mac tagged-eth2	

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|l2l|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> ]

```

no access-list <num>

Parameter

<num>	access-list serial No. this is a decimal's No. from 3100-3299
deny	deny packets
permit	permit packets
any-source-mac	any source mac address
any-destination-mac	any destination mac address
host_smac , smac	source mac address
smac-mask	(reverse mask) of source MAC address
host_dmac , dmas	destination mac address
dmac-mask	(reverse mask) of destination MAC address
protocol	No. of name or IP protocol. It can be a key word: eigrp, gre, icmp, igmp, igrp, ip, ipinip, ospf, tcp, or udp, or an integer from 0-255 of list No. of IP address. Use key word 'ip' to match all Internet protocols (including ICMP, TCP, AND UDP) list
source-host-ip	No. of source network or source host of packet delivery. Numbers of 32-bit binary system with dotted decimal notation expression
source-wildcard	reverse of source IP. Numbers of 32-bit binary system expressed by decimal's numbers with four-point separated, reverse mask
destination-host-ip	No. of destination network or host to which packets are delivered. Numbers of 32-bit binary system with dotted decimal notation expression
destination-wildcard	mask of destination. I Numbers of 32-bit binary system expressed by decimal's numbers with four-point separated, reverse mask
s-port	means the need to match TCP/UDP source port
port1	value of TCP/UDP source interface No.,Interface No. is an integer from 0-65535
d-port	means need to match TCP/UDP destination interface
sPortMin	the down boundary of source port
sPortMax	the up boundary of source port
port3	value of TCP/UDP destination interface No., Interface No. is an integer from 0-65535
dPortMin	the down boundary of destination port
dPortMax	the up boundary of destination port
[ack] [fin] [psh] [rst] [urg] [syn]	only for TCP protocol, multi-choices of tag positions are available, and when TCP data reports the configuration of corresponding position, then initialization of TCP data report is enabled to form a match when in connection
precedence	packets can be filtered by priority which is a number from 0-7

tos	packets can be filtered by service type which is a number from 0-15
icmp-type	ICMP packets can be filtered by packet type which is a number from 0-255
icmp-code	ICMP packets can be filtered by packet code which is a number from 0-255
igmp-type	ICMP packets can be filtered by IGMP packet name or packet type which is a number from 0-255
time-range-name	name of time range

Default By default, no access-lists configured.

Mode Global mode

Usage Guide Define an extended numeric MAC-IP ACL rule.
When the user assigns specific <num> for the first time, ACL of the serial number is created, then the lists are added into this ACL; the access list which is marked 3200-3299 can configure not continual reverse mask of IP address.
The no command deletes an extended numeric MAC-IP ACL access-list rule.

Example Permit the passage of TCP packet with source MAC 00-12-34-45-XX-XX, any destination MAC address, source IP address 100.1.1.0 0.255.255.255, and source port 100.

```
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
```

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>`

Parameter	<num>	the access-list No. which is a decimal's No. from 700-799
	deny	deny packets
	permit	permit packets
	host_smac, smac	source mac address
	smac-mask	(reverse mask) of source MAC address

Default By default, no access-lists configured.

Mode Global mode

Usage Guide	Define a standard numeric MAC ACL rule. When the user assign specific <num> for the first time, ACL of the serial number is created, then the lists are added into this ACL. The no command deletes a standard numeric MAC ACL access-list rule.
Example	Permit the passage of packets with source MAC address 00-00-XX-XX-00-01, and deny passage of packets with source MAC address 00-00-00-XX-00-ab. <pre>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</pre>

clear access-group statistic

Command	clear access-group statistic [ethernet <interface-name>]
Parameter	interface-name interface-name
Default	None.
Mode	Admin Mode
Usage Guide	Empty packet statistics information of the specified interface.
Example	Empty packet statistics information of interface. <pre>Switch#clear access-group statistic</pre>

firewall

Command	firewall {enable disable}
Parameter	{enable disable} enable or disable
Default	None.
Mode	Global Mode

Usage Guide	Enable or disable firewall. Whether enabling or disabling firewall, access rules can be configured. But only when the firewall is enabled, the rules can be used in specific orientations of specific ports. When disabling the firewall, all ACL tied to ports will be deleted.
Example	Enable firewall. Switch(config)#firewall enable

ip access extended

Command	[no] ip access extended <name>	
Parameter	name	the name of the access list. The name can be formed by non-all-digit characters of length of 1 to 32.
Default	By default,no access-lists configured.	
Mode	Global mode	
Usage Guide	Create a named extended IP access list. When this command is issued for the first time, an empty access list will be created. The no prefix will remove the named extended IP access list including all the rules.	
Example	To create a extended IP access list name tcpFlow. Switch(config)#ip access-list extended tcpFlow	

ip access standard

Command	[no] ip access standard<name>	
Parameter	name	the name of the access list. The name can be formed by non-all-digit characters of length of 1 to 32

Default	By default,no access-lists configured.
Mode	Global mode
Usage Guide	Create a named standard access list. When this command is issued for the first time, an empty access list will be created. The no prefix will remove the named standard access list including all the rules in the list.
Example	To create a standard IP access list name ipFlow. Switch(config)#ip access-list standard ipFlow

ipv6 access-list

Command	ipv6 access-list <num-std> {deny permit} {<sIPv6Prefix/sPrefixlen> any-source {host-source <sIPv6Addr>}} no ipv6 access-list <num-std>	
Parameter	num-std	the list number, list range is between 500 ~ 599
	deny	deny packets
	permit	permit packets
	sIPv6Prefix	the prefix of the ipv6 source address
	sPrefixlen	the length of prefix of the ipv6 source address, range is between 1 ~ 128
	sIPv6Addr	the ipv6 source address
Default	By default,no access-lists configured.	
Mode	Global mode	
Usage Guide	Creates a numbered standard IP access-list, if the access-list already exists, then a rule will add to the current access-list.	
	The no command deletes a numbered standard IP access-list.	
Example	Creates a numbered 520 standard IP access-list, allow the source packet from 2003:1:2:3::1/64 pass through the net, and deny all the other packet from the source address 2003:1:2::1/48 pass through. 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
```

ipv6 access standard

Command	ipv6 access-list standard <name> no ipv6 access-list standard <name>		
Parameter	<table><tr><td>name</td><td>the name for access list, the character string length is from 1 to 32</td></tr></table>	name	the name for access list, the character string length is from 1 to 32
name	the name for access list, the character string length is from 1 to 32		
Default	By default,no access-lists configured.		
Mode	Global mode		
Usage Guide	Create a name-based standard IPv6 access list. When this command is run for the first time, only an empty access list with no entry will be created. The no command deletes the name-based standard IPv6 access list (including all entries).		
Example	Create a standard IPv6 access list named ip6Flow. <pre>Switch(config)#ipv6 access-list standard ip6Flow</pre>		

ipv6 access extended

Command	ipv6 access-list extended <name> no ipv6 access-list extended <name>		
Parameter	<table><tr><td>name</td><td>the name for access list, the character string length is from 1 to 32</td></tr></table>	name	the name for access list, the character string length is from 1 to 32
name	the name for access list, the character string length is from 1 to 32		
Default	By default,no access-lists configured.		
Mode	Global mode		
Usage Guide	Create a name-based extended IPv6 access list. When this command is run for the first time, only an empty access list with no entry will be		

created.

The no command delete the name-based extended IPv6 access list.

Example

Create an extensive IPv6 access list named tcpFlow.

```
Switch(config)#ipv6 access-list extended tcpFlow
```

{ip|ipv6|mac|mac-ip} access-group

Command

```
{ip|ipv6|mac|mac-ip} access-group <name> {in} [traffic-statistic]  
no {ip|ipv6|mac|mac-ip} access-group <name> {in}
```

Parameter

name	the name for access list, the character string length is from 1 to 32
traffic-statistic	flow statistics

Default

By default,the entry of port is not bound ACL.

Mode

Port Mode

Usage Guide

Apply an access-list on some direction of port, and determine if ACL rule is added statistic counter or not by options.

Note:when a ACL has multiple rules, traffic-statistic can't configure.

There are four kinds of packet head field based on concerned:MAC ACL,IP ACL,MAC-IP ACL and IPv6 ACL; to some extent,ACL filter behavior (permit,deny) has a conflict when a data packet matches multi types of four ACLs.The strict priorities are specified for each ACL based on outcome veracity.It can determine final behavior of packet filter through priority when the filter behavior has a conflict.

When binding ACL to port, there are some limits as below:

1. Each port can bind a MAC-IP ACL, a IP ACL, a MAC ACL and a IPv6 ACL.
2. When binding four ACLs and data packet matching the multi ACLs simultaneity, the priority from high to low are shown as below,
 - Ingress IPv6 ACL
 - Ingress MAC-IP ACL
 - Ingress MAC ACL
 - Ingress IP ACL

The no command deletes access-list binding on the port.

Example

Binding AAA access-list to entry direction of port.

```
Switch(config)#interface ethernet 1/0/5
Switch(config-If-Ethernet1/0/5)#ip access-group aaa in
```

mac access extended

Command	mac-access-list extended <name> no mac-access-list extended <name>	
Parameter	name	name of access-list excluding blank or quotation mark, and it must start with letter, and the length cannot exceed 32. (remark: sensitivity on capital or small letter.)
Default	By default, no access-lists configured.	
Mode	Global mode	
Usage Guide	Define a name-manner MAC ACL or enter access-list configuration mode. After assigning this command for the first time, only an empty name access-list is created and no list item included. The no command deletes this ACL.	
Example	Create an MAC ACL named mac_acl. Switch(config)# mac-access-list extended mac_acl Switch(config-mac-ext-nacl-mac_acl)#	

mac-ip access extended

Command	mac-ip-access-list extended <name> no mac-ip-access-list extended <name>	
Parameter	name	name of access-list excluding blank or quotation mark, and it must start with letter, and the length cannot exceed 32 (remark: sensitivity on capital or small letter).
Default	By default, no named MAC-IP access-list.	

Mode	Global mode
Usage Guide	Define a name-manner MAC-IP ACL or enter access-list configuration mode. After assigning this command for the first time, only an empty name access-list is created and no list item included. The no command deletes this ACL.
Example	Create an MAC-IP ACL named macip_acl. <pre>Switch(config)# mac-ip-access-list extended macip_acl Switch(config-macip-ext-nacl-macip_acl)#</pre>

permit | deny (ip extended)

Command	<pre>[no] {deny permit} icmp {{<slpAddr> <sMask>} any-source {host-source <slpAddr>}} {{<dIpAddr> <dMask>} any-destination {host-destination <dIpAddr>}} [<icmp-type> [<icmp-code>]] [precedence <prec>][tos <tos>] [time-range<time-range-name>]</pre> <pre>[no] {deny permit} igmp {{<slpAddr> <sMask>} any-source {host-source <slpAddr>}} {{<dIpAddr> <dMask>} any-destination {host-destination <dIpAddr>}} [<igmp-type>] [precedence <prec>] [tos <tos>] [time-range<time-range-name>]</pre> <pre>[no] {deny permit} tcp {{ <slpAddr> <sMask> } any-source {host-source <slpAddr> } } [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>]</pre> <pre>[no] {deny permit} udp {{ <slpAddr> <sMask> } any-source {host-source <slpAddr> } } [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>]</pre> <pre>[no] {deny permit} {eigrp gre igmp ipinip ip ospf <protocol-num>} {{<slpAddr> <sMask>} any-source {host-source <slpAddr>}} {{<dIpAddr> <dMask>} any-destination {host-destination <dIpAddr>}} [precedence <prec>] [tos <tos>][time-range<time-range-name>]</pre>

Parameter	deny	deny packets
	permit	permit packets
	<slpAddr>	the source IP address, the format is dotted decimal notation
	<sMask>	the reverse mask of source IP, the format is dotted decimal notation
	<sPort>	source port No., 0-65535
	<sPortMin>	the down boundary of source port
	<sPortMax>	the up boundary of source port
	<dIpAddr>	the destination IP address, the format is dotted decimal notation
	<dMask>	the reverse mask of destination IP, the format is dotted decimal notation, attentive position 0, ignored position 1
	<dPort>	destination port No. 0-65535
	<dPortMin>	the down boundary of destination port
	<dPortMax>	the up boundary of destination port
	<igmp-type>	the type of igmp, 0-15
	<icmp-type>	the type of icmp, 0-255
	<icmp-code>	protocol No. of icmp, 0-255
	<prec>	IP priority, 0-7
	<tos>	to value, 0-15
	<time-range-name>	time range name
Default	By default, no access-list configured.	
Mode	Name extended IP access-list configuration mode	
Usage Guide	Create a name extended IP access rule to match specific IP protocol or all IP protocol.	
	The no command will delete this access list.	
Example	Create the extended access-list, deny icmp packet to pass, and permit udp packet with destination address 192.168.0.1 and destination port 32 to pass.	
	<pre>Switch(config)# ip access-list 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</pre>	

permit | deny (ip standard)

Command	{deny permit} {{<slpAddr> <sMask>} any-source {host-source <slpAddr>}}

no {deny | permit} {{<slpAddr> <sMask>} | any-source | {host-source <slpAddr>}}

Parameter	deny	deny packets
	permit	permit packets
	<slpAddr>	the source IP address, the format is dotted decimal notation
	<sMask>	the reverse mask of source IP, the format is dotted decimal notation
Default	By default, no access-list configured.	
Mode	Name standard IP access-list configuration mode	
Usage Guide	Create a name standard IP access rule	
	The no command deletes this name standard IP access rule.	
Example	Permit packets with source address 10.1.1.0/24 to pass, and deny other packets with source address 10.1.1.0/16. <pre>Switch(config)# ip access-list 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</pre>	

permit | deny (ipv6 extended)

Command	<pre>[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>]</pre> <pre>[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>]</pre> <pre>[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>]</pre>

[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>]

Parameter

deny	deny packets
permit	permit packets
<sIPv6Addr>	the source IPv6 address
<sPrefixlen>	the length of the IPv6 address prefix, the range is 1 ~ 128
<sPort>	source port number, the range is 0 ~ 65535
<sPortMin>	the down boundary of source port
<sPortMax>	the up boundary of source port
<dIPv6Addr>	the destination IPv6 address
<dPrefixlen>	the length of the IPv6 address prefix, the range is 1 ~ 128
<d-Port>	destination port number, the range is 0 ~ 65535
<dPortMin>	the down boundary of destination port
<dPortMax>	the up boundary of destination port
<icmp-type>	icmp type
<icmp-code>	icmp protocol number
<dscp>	IPv6 priority ,the range is 0 ~ 63
<flowlabel>	value of the flow label, the range is 0 ~ 1048575
syn,ack,urg,rst,fin, psh,tcp	label position
<next-header>	the IPv6 next-header
<time-range-name>	time range name

Default

By default, No access control list configured.

Mode

IPv6 nomenclature extended access control list mode

Usage Guide

Create an extended nomenclature IPv6 access control rule for specific IPv6 protocol.

The no command will delete this access list.

Example

Create an extended access control list named udpFlow,denying the icmp packets while allowing 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 icmp any any-destination
Switch(config-ipv6-ext-nacl-udpFlow)#permit udp any-source host-destination
2001:1:2:3::1 d-port 32
```


permit | deny (ipv6 standard)

Command	[no] {deny permit} {{<sIPv6Prefix/sPrefixlen>} any-source {host-source <sIPv6Addr>}}	
Parameter	deny	deny packets
	permit	permit packets
	<sPrefixlen>	the length of the IPv6 address prefix, the valid range is 1~128
	<sIPv6Addr>	the source IPv6 address
Default	No access list configured by default.	
Mode	Standard IPv6 nomenclature access list mode	
Usage Guide	Create a standard nomenclature IPv6 access control rule.	
	The no form of this command deletes the nomenclature standard IPv6 access control rule.	
Example	Permit packets with source address of 2001:1:2:3::1/64 while denying those with source address of 2001:1:2:3::1/48. <pre>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</pre>	

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> }} [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>   ]]]
```

Parameter

deny	deny packets
permit	permit packets
any-source-mac	any source of MAC address
any-destination-mac	any destination of MAC address
host_smac, smac	source MAC address
smac-mask	mask (reverse mask) of source MAC address
host_dmac, dmas	destination MAC address
dmac-mask	(reverse mask) of destination MAC address
untagged-eth2	format of untagged ethernet II packet
tagged-eth2	format of tagged ethernet II packet
untagged-802-3	format of untagged ethernet 802.3 packet
tagged-802-3	format of tagged ethernet 802.3 packet
cos-val	cos value, 0-7
cos-bitmask	cos mask, 0-7reverse mask and mask bit is consecutive
vid-value	VLAN No, 1-4094
vid-bitmask	VLAN mask, 0-4095, reverse mask and mask bit is consecutive
protocol	specific Ethernet protocol No., 1536-65535
protocol-bitmask	protocol mask, 0-65535, reverse mask and mask bit is consecutive

Default

By default, no access-list configured.

Mode

Name extended MAC access-list configuration mode

Usage Guide

Define an extended name MAC ACL rule.

Notice: mask bit is consecutive means the effective bit must be consecutively effective from the first bit on the left, no ineffective bit can be added through. For example: the reverse mask format of one byte is: 00001111b; mask format is 11110000; and this is not permitted: 00010011.

The no command deletes this extended name IP access rule.

Example

The forward source MAC address is not permitted as 00-12-11-23-XX-XX of 802.3 data

packet.

```
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 untagged-802-3
```

permit | deny (mac-ip extended)

Command	<pre>[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>]</pre> <pre>[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>]</pre> <pre>[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>]</pre> <pre>[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>]</pre>

[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>]

Parameter

num	access-list serial No. this is a decimal's No. from 3100-3199
deny	deny packets
permit	permit packets
any-source-mac	any source MAC address
any-destination-mac	any destination MAC address
host_smac, smac	source MAC address
smac-mask	(reverse mask) of source MAC address
host_dmac, dmas	destination MAC address
dmac-mask	(reverse mask) of destination MAC address
protocol	No. of name or IP protocol. It can be a key word: eigrp, gre, icmp, igmp, igrp, ip, ipinip, ospf, tcp, or udp, or an integer from 0-255 of list No. of IP address. Use key word 'ip' to match all Internet protocols (including ICMP, TCP, AND UDP) list
source-host-ip, source	No. of source network or source host of packet delivery. Numbers of 32-bit binary system with dotted decimal notation expression
source-wildcard	reverse of source IP. Numbers of 32-bit binary system expressed by decimal's numbers with four-point separated, reverse mask
destination-host-ip, destination	destination No. of destination network or host to which packets are delivered. Numbers of 32-bit binary system with dotted decimal notation expression
destination-wildcard	mask of destination. I Numbers of 32-bit binary system expressed by decimal's numbers with four-point separated, reverse mask
s-port	means the need to match TCP/UDP source port
port1	value of TCP/UDP source interface No., Interface No. is an integer from 0-65535
<sPortMin>	the down boundary of source port
<sPortMax>	the up boundary of source port
d-port	means need to match TCP/UDP destination interface
port3	value of TCP/UDP destination interface No., Interface No. is an integer from 0-65535
<dPortMin>	the down boundary of destination port
<dPortMax>	the up boundary of destination port
[ack] [fin] [psh] [rst] [urg] [syn]	(optional) only for TCP protocol, multi-choices of tag positions are available, and when TCP data reports the configuration of corresponding position, then initialization of TCP data report is enabled to form a match when in connection
precedence	packets can be filtered by priority which is a number from 0-7

tos	packets can be filtered by service type which is a number from 0-15
icmp-type	ICMP packets can be filtered by packet type which is a number from 0-255
icmp-code	ICMP packets can be filtered by packet code which is a number from 0-255
igmp-type	ICMP packets can be filtered by IGMP packet name or packet type which is a number from 0-255
time-range-name	name of time range

Default By default, no access-list configured.

Mode Name extended MAC-IP access-list configuration mode

Usage Guide Define an extended name MAC-IP ACL rule.

No form deletes one extended numeric MAC-IP ACL access-list rule.

Example Deny the passage of UDP packets with any source MAC address and destination MAC address, any source IP address and destination IP address, and source port 100.

```
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
```

show access-lists

Command show access-lists [<num>|<acl-name>]

Parameter	<num> <acl-name>	specific ACL No specific ACL name character string

Default None.

Mode Admin Mode

Usage Guide Reveal ACL of configuration.
When not assigning names of ACL, all ACL will be revealed, used x time (s) indicates the times of ACL to be used.

Example Reveal ACL of configuration.

```
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

```

show access-group

Command `show access-group in (interface {Ethernet | Ethernet IFNAME})`

Parameter	IFNAME	Port name

Default None.

Mode admin/ Global Mode

Usage Guide Display the ACL binding status on the port.
When not assigning interface names, all ACL tied to port will be revealed.

Example Displays all ACL bound to the port.

```

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.

```

show firewall

Command `show firewall`

Parameter	none	none

Default None.

Mode	Admin/Global Mode
Usage Guide	Reveal configuration information of packet filtering functions.
Example	Display firewall status. Switch#show firewall Firewall status: Enable.

show ipv6 access-lists

Command	show ipv6 access-lists [<num> <acl-name>]	
Parameter	<num>	the number of specific access control list, the valid range is 500 ~ 699, amongst 500 ~ 599 is digit standard IPv6 ACL number, 600 ~ 699 is the digit extended IPv6 ACL number
	<acl-name>	the nomenclature character string of a specific access control list, lengthening within 1 ~ 32
Default	None.	
Mode	Admin/Global Mode	
Usage Guide	Show the configured IPv6 access control list. When no access control list is specified, all the access control lists will be displayed; in used x time (s) is shown the times the ACL had been quoted.	
Example	Show the configured IPv6 access control list. 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 	

show time-range

Command	show time-range <word>
Parameter	<word> assign name of time-range needed to be revealed
Default	None.
Mode	Admin/Global Mode
Usage Guide	Reveal configuration information of time range functions. When not assigning time-range names, all time-range will be revealed. in used x time (s) is shown the times the ACL had been quoted.
Example	Reveal configuration information of time range functions. 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

time-range

Command	[no] time-range <time_range_name>
Parameter	<time_range_name> time range name must start with letter or number, and the length cannot exceed 32 characters long
Default	By default, no time-range configuration, Valid for all time period.
Mode	Global Mode
Usage Guide	Create the name of time-range as time range name, enter the time-range mode at the same time. The no command to delete this time range.
Example	Create a time-range named admin_timer.

2 Commands for 802.1x

dot1x accept-mac

Command	[no] dot1x accept-mac <mac-address> [interface <interface-name>]	
Parameter	mac-address	stands for MAC address
	interface-name	for interface name and port number
Default	None.	
Mode	Global Mode	
Usage Guide	Add a MAC address entry to the dot1x address filter table. If a port is specified, the entry added applies to the specified port only. If no port is specified, the entry added applies to all the ports. The dot1x address filter function is implemented according to the MAC address filter table, dot1x address filter table is manually added or deleted by the user. When a port is specified in adding a dot1x address filter table entry, that entry applies to the port only; when no port is specified, the entry applies to all ports in the switch. When dot1x address filter function is enabled, the switch will filter the authentication user by the MAC address. Only the authentication request initialed by the users in the dot1x address filter table will be accepted, the rest will be rejected. The no command deletes the entry from dot1x address filter table.	
Example	Adding 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	

dot1x eapor enable

Command	[no] dot1x eapor enable	
Parameter	none	none

Default	EAP relay authentication is used by default.
Mode	Global Mode
Usage Guide	Enables the EAP relay authentication function in the switch. The switch and RADIUS may be connected via Ethernet or PPP. If an Ethernet connection exists between the switch and RADIUS server, the switch needs to authenticate the user by EAP relay (EAPoR authentication); if the switch connects to the RADIUS server by PPP, the switch will use EAP local end authentication (CHAP authentication). The switch should use different authentication methods according to the connection between the switch and the authentication server. The no command sets EAP local end authentication.
Example	Setting EAP local end authentication for the switch. <pre>Switch(config)#no dot1x eapor enable</pre>

dot1x enable

Command	[no] dot1x enable		
Parameter	<table> <tr> <td>none</td><td>none</td></tr> </table>	none	none
none	none		
Default	802.1x function is not enabled in global mode by default; if 802.1x is enabled under Global Mode, 802.1x will not be enabled for the ports by default.		
Mode	Global Mode and Port Mode		
Usage Guide	Enables the 802.1x function in the switch and ports. The 802.1x authentication for the switch must be enabled first to enable 802.1x authentication for the respective ports. If Spanning Tree or MAC binding is enabled on the port, or the port is a Trunk port or member of port aggregation group, 802.1x function cannot be enabled for that port unless such conditions are removed. The no command disables the 802.1x function.		
Example	Enabling the 802.1x function of the switch and enable 802.1x for port1/0/12. <pre>Switch(config)#dot1x enable Switch(config)#interface ethernet 1/0/12</pre>		

```
Switch(config-if-ethernet1/0/12)#dot1x enable
```

dot1x ipv6 passthrough

Command [no] dot1x ipv6 passthrough

Parameter	none	none

Default IPv6 passthrough function is disabled on the switch by default.

Mode Port Mode

Usage Guide Enable IPv6 passthrough function on a switch port, only applicable when access control mode is userbased.

The function can only be enabled when 802.1x function is enabled both globally and on the port, with userbased being the control access mode. After it is enabled, users can send IPv6 messages without authentication.

The no operation of this command will disable the function.

Example Enable IPv6 passthrough function on port Ethernet1/0/12.

```
Switch(config)#dot1x enable
Switch(config)#interface ethernet 1/0/12
Switch(config-if-ethernet1/0/12)#dot1x enable
Switch(config-if-ethernet1/0/12)#dot1x ipv6 passthrough
```

dot1x guest-vlan

Command dot1x guest-vlan <vlanid>
no dot1x guest-vlan

Parameter	vlanid	the specified VLAN id, ranging from 1 to 4094

Default By default, there is no 802.1x guest-vlan function on the port.

Mode Port Mode

Usage Guide

Set the guest-vlan of the specified port.

The access device will add the port into Guest VLAN if there is no supplicant getting authenticated successfully in a certain stretch of time because of lacking exclusive authentication supplicant system or the version of the supplicant system being too low. In Guest VLAN, users can get 802.1x supplicant system software, update supplicant system or update some other applications (such as anti-virus software, the patches of operating system).

When a user of a port within Guest VLAN starts an authentication, the port will remain in Guest VLAN in the case of a failed authentication.

If the authentication finishes successfully, there are two possible results:

- 1、The authentication server assigns an Auto VLAN, causing the port to leave Guest VLAN to join the assigned Auto VLAN. After the user gets offline, the port will be allocated back into the specified Guest VLAN.
- 2、The authentication server assigns an Auto VLAN, then the port leaves Guest VLAN and joins the specified VLAN. When the user becomes offline, the port will be allocated to the specified Guest VLAN again.

Attention:

There can be different Guest VLAN set on different ports, while only one Guest VLAN is allowed on one port.

Only when the access control mode is portbased, the Guest VLAN can take effect. If the access control mode of the port is macbased or userbased, the Guest VLAN can be successfully set without taking effect.

The no command is used to delete the guest-vlan.

Example

Set Guest-VLAN of port Ethernet1/0/3 as VLAN 10.

```
Switch(config)#dot1x enable
Switch(config)#interface ethernet 1/0/3
Switch(config-if-ethernet1/0/3)#dot1x guest-vlan 10
```

dot1x macfilter enable

Command	[no] dot1x macfilter enable

Parameter	none none

Default	dot1x address filter is disabled by default.

Mode	Global Mode

Usage Guide	Enables the dot1x address filter function in the switch. When dot1x address filter function is enabled, the switch will filter the authentication user by the MAC address. Only the authentication request initiated by the users in the dot1x address filter table will be accepted. The no command disables the dot1x address filter function.
Example	Enabling dot1x address filter function for the switch. Switch(config)#dot1x macfilter enable

dot1x macbased guest-vlan

Command	dot1x macbased guest-vlan <vlanid> no dot1x macbased guest-vlan		
Parameter	<table> <tr> <td>vlanid</td><td>the configured vlan id, the range is from 1 to 4094</td></tr> </table>	vlanid	the configured vlan id, the range is from 1 to 4094
vlanid	the configured vlan id, the range is from 1 to 4094		
Default	Do not configure 802.1x macbased guest-vlan by default.		
Mode	Port Mode		
Usage Guide	Configure to appoint the port's guest-vlan based on the mac authentication. If there is no dedicated authentication client or the client version was too low, and it makes no clients authenticate successfully on the port in some time, then the access device will make this user join to the guest VLAN. User can get the 802.1x client software in guest VLAN, update the client or do other updating things (such as anti-virus software, system patches and etc.) When the user under the port in Guest VLAN issues the authentication, this port will be stay in guest VLAN if the authentication failed; if it was successful, there are two situations as below: 1、 The authentication server issues an auto VLAN, in this time, the user left the guest VLAN and joined to the auto VLAN. After the user was downline, this user will be assigned to the configured guest VLAN again. 2、 The authentication server did not issue the VLAN, in this time, the user left the guest VLAN and joined to the configured native VLAN. After the user was downline, this user will be assigned to the configured guest VLAN again. Notice: 1、 dot1x macbased guest-vlan can be configured only on the port based on mac authentication and in HYBRID mode. 2、 Different macbased guestVLAN can be configured on different ports, but only one macbased guestVLAN can be configured on one port.		

The no command deletes this guest-vlan.

Example

Configure the guest-vlan of Ethernet1/0/3 as Vlan 10.

```
Switch(config-if-ethernet1/0/3)#dot1x macbased guest-vlan 10
```

dot1x macbased port-down-flush

Command

[no] dot1x macbased port-down-flush

Parameter

none	none

Default

The command is not enabled by default.

Mode

Global Mode

Usage Guide

Enables this command, when the dot1x certification according to mac is down, delete the user who passed the certification of the port

When users who passed the certification according to mac changed among different ports, delete the user for the new certification. The command should be enable to delete the user.

The no command does not make the down operation.

Example

When the dot1x certification according to mac is down, delete the user who passed the certification of the port.

```
Switch(config)#dot1x macbased port-down-flush
```

dot1x max-req

Command

dot1x max-req <count>
no dot1x max-req

Parameter

count	the times to re-transfer EAP request/ MD5 frames, the valid range is 1 to 10

Default

The default maximum for retransmission is 2.

Mode	Global Mode
Usage Guide	Sets the number of EAP request/MD5 frame to be sent before the switch re-initials authentication on no supplicant response. The default value is recommended in setting the EAP request/ MD5 retransmission times. The no command restores the default setting.
Example	Changing the maximum retransmission times for EAP request/ MD5 frames to 5 times. Switch(config)#dot1x max-req 5

dot1x user allow-movement

Command	[no] dot1x user allow-movement
Parameter	none none
Default	Disable the authentication function after the user moves the port.
Mode	Global Mode
Usage Guide	Enable the authentication function after the user moves the port, so the switch allows user to process this authentication. In the condition that the switch connects with hub, when the user will be moved to other port, dot1x user allow-movement command should be enabled. The no command disables the function.
Example	Enable the authentication function after the user moves the port. Switch(config)#dot1x user allow-movement

dot1x user free-resource

Command	dot1x user free-resource <prefix> <mask> no dot1x user free-resource

Parameter	prefix	the segment for limited resource, in dotted decimal format
	mask	the mask for limited resource, in dotted decimal format
Default	There is no free resource by default.	
Mode	Global Mode	
Usage Guide	To configure 802.1x free resource. This command is available only if user based access control is applied. If user based access control has been applied, this command configures the limited resources which can be accessed by the un-authenticated users. For port based and MAC based access control, users could access no network resources before authentication. If TrustView management system is available, the free resource can be configured in TrustView server, and the TrustView server will distribute the configuration to the switches. To be noticed, only one free resource can be configured for the overall network. The no form command closes this function.	
Example	To configure the free resource segment as 1.1.1.0, the mask is 255.255.255.0. Switch(config)#dot1x user free-resource 1.1.1.0 255.255.255.0	

dot1x max-user macbased

Command	dot1x max-user macbased <number> no dot1x max-user macbased	
Parameter	number	the maximum users allowed, the valid range is 1 to 256
Default	The default maximum user allowed is 1.	
Mode	Port Mode	
Usage Guide	Sets the maximum users allowed connect to the port. This command is available for ports using MAC-based access management, if MAC address authenticated exceeds the number of allowed user, additional users will not be able to access the network. The no command restores the default setting.	

Example	Setting port 1/0/3 to allow 5 users.
	Switch(config-if-ethernet1/0/3)#dot1x max-user macbased 5

dot1x max-user userbased

Command	dot1x max-user userbased <number> no dot1x max-user userbased	
Parameter	number	the maximum number of users allowed to access the network, ranging from 1 to 1~256
Default	The maximum number of users allowed to access each port is 10 by default.	
Mode	Port Mode	
Usage Guide	Set the upper limit of the number of users allowed access the specified port when using user-based access control mode. This command can only take effect when the port adopts user-based access control mode. If the number of authenticated users exceeds the upper limit of the number of users allowed access the network, those extra users can not access the network. the no command is used to reset the default value.	
Example	Setting port 1/0/3 to allow 5 users. Switch(config-if-ethernet1/0/3)#dot1x max-user userbased 5	

dot1x portbased mode single-mode

Command	[no] dot1x portbased mode single-mode	
Parameter	none	none
Default	Disable the single-mode by default.	
Mode	Port Mode	

Usage Guide

Set the single-mode based on portbase authentication mode.

This command takes effect when the access mode of the port is set as portbase only. Before configuring the single-mode, if the port has enabled dot1x port-method portbased command and exist online users, the switch will enforce all users of this port are offline. After that, this port only allows a user to pass the authentication, the user can access the specified network resource, but other authentication users of this port will be denied and can not access the network. After disabling the single-mode, the switch also enforce the authenticated user is offline.

The no command disables this function.

Example

Set port 1/0/1 based on port authentication mode to single mode.

```
Switch(config-if-ethernet1/0/1)#dot1x portbased mode single-mode
```

dot1x port-control

Command

dot1x port-control {auto | force-authorized | force-unauthorized}
no dot1x port-control

Parameter

auto	enable 802.1x authentication, the port authorization status is determined by the authentication information between the switch and the supplicant
force-authorized	sets port to authorized status, unauthenticated data is allowed to pass through the port
force-unauthorized	will set the port to non-authorized mode, the switch will not provide authentication for the supplicant and prohibit data from passing through the port

Default

When 802.1x is enabled for the port, auto is set by default.

Mode

Port Mode

Usage Guide

Sets the 802.1x authentication status.

If the port needs to provide 802.1x authentication for the user, the port authentication mode should be set to auto.

The no command restores the default setting.

Example

Setting port1/0/1 to require 802.1x authentication mode.

```
Switch(config-if-ethernet1/0/1)#dot1x port-control auto
```

dot1x port-method

Command `dot1x port-method {macbased | portbased | userbased {standard | advanced}}`
`no dot1x port-method`

Parameter	macbased	means the access control method based on MAC address
	portbased	means the access control method based on port
	userbased	means the access control method based on user, it can be divided into two types, one is standard access control method, and the other is advanced access control method
	standard	Standard Access Control Method Based on User
	advanced	Advanced User-Based Access Control

Default Advanced access control method based on user is used by default.

Mode Port Mode

Usage Guide This command is used to configure the dot1x authentication method for the specified port. When port based authentication is applied, only one host can authenticate itself through one port. And after authentication, the host will be able to access all the resources. When MAC based authentication is applied, multiple host which are connected to one port can access all the network resources after authentication. When either of the above two kinds of access control is applied, un-authenticated host cannot access any resources in the network. When user based access control is applied, un-authenticated users can only access limited resources of the network. The user based access control falls into two kinds – the standard access control and the advanced access control. The standard user based access control does not limit the access to the limited resources when the host is not authenticated yet. While the user based advanced access control can control the access to the limited resources before authentication is done.

Notes:

For standard control method based on user, the 802.1x free resource must be configured first, and it needs to be used with dot1x privateclient enable.

The no form command restores the default access control method.

Example To configure the access control method based on port for Ethernet1/0/4.

```
Switch(config-if-ethernet1/0/4)#dot1x port-method portbased
```

dot1x privateclient enable

Command	[no] dot1x privateclient enable	
Parameter	none	none
Default	Private 802.1x authentication packet format is disabled by default.	
Mode	Global Mode	
Usage Guide	To configure the switch to force the authentication client to use private 802.1x authentication protocol. To implement integrated solution, the switch must be enabled to use private 802.1x protocol, or many applications will not be able to function. For detailed information, please refer to DCBI integrated solution. If the switch forces the authentication client to use private 802.1x protocol, the standard client will not be able to work. The no prefix will disable the command and allow the authentication client to use the standard 802.1x authentication protocol.	
Example	To force the authentication client to use private 802.1x authentication protocol. Switch(config)#dot1x privateclient enable	

dot1x privateclient protect enable

Command	[no] dot1x privateclient protect enable	
Parameter	none	none
Default	Disable the privateclient protect function by default.	
Mode	Global Mode	
Usage Guide	Enable the privateclient protect function of the switch. Support the partial encryption of the privateclient protocol to advance the security of the privateclient.	

The no command disables the protect function.

Example

Enable the privateclient protect function of the switch.

```
Switch(config)#dot1x privateclient protect enable
```

dot1x re-authenticate

Command

dot1x re-authenticate [interface <interface-name>]

Parameter

interface-name	stands for port number, omitting the parameter for all ports

Default

None

Mode

Global Mode

Usage Guide

Enables real-time 802.1x re-authentication (no wait timeout requires) for all ports or a specified port.
It makes the switch to re-authenticate the client at once without waiting for re-authentication timer timeout. This command is no longer valid after authentication.

Example

Enabling real-time re-authentication on port1/0/8.

```
Switch(config)#dot1x re-authenticate interface ethernet 1/0/8
```

dot1x re-authentication

Command

[no] dot1x re-authentication

Parameter

none	none

Default

Periodical re-authentication is disabled by default.

Mode

Global Mode

Usage Guide

Enables periodical supplicant authentication.

When periodical re-authentication for supplicant is enabled, the switch will re-authenticate the supplicant at regular interval. This function is not recommended for common use.

The no command disables this function.

Example

Enabling the periodical re-authentication for authenticated users.

Switch(config)#dot1x re-authentication

dot1x timeout quiet-period

Command

dot1x timeout quiet-period <seconds>
no dot1x timeout quiet-period

Parameter

seconds	the silent time for the port in seconds, the valid range is 1 to 65535

Default

The default value is 10 seconds.

Mode

Global Mode

Usage Guide

Sets time to keep silent on supplicant authentication failure.
Default value is recommended.

The no command restores the default value.

Example

Setting the silent time to 120 seconds.

Switch(config)#dot1x timeout quiet-period 120

dot1x timeout re-authperiod

Command

dot1x timeout re-authperiod <seconds>
no dot1x timeout re-authperiod

Parameter

seconds	the interval for re-authentication, in seconds, the valid range is 1 to 65535

Default	The default value is 3600 seconds.
Mode	Global Mode
Usage Guide	Sets the supplicant re-authentication interval. dot1x re-authentication must be enabled first before supplicant re-authentication interval can be modified. If authentication is not enabled for the switch, the supplicant re-authentication interval set will not take effect. The no command restores the default setting.
Example	Setting the re-authentication time to 1200 seconds. Switch(config)#dot1x timeout re-authperiod 1200

dot1x timeout tx-period

Command	dot1x timeout tx-period <seconds> no dot1x timeout tx-period	
Parameter	seconds	the interval for re-transmission of EAP request frames, in seconds; the valid range is 1 to 65535
Default	The default value is 30 seconds.	
Mode	Global Mode	
Usage Guide	Sets the interval for the supplicant to re-transmit EAP request/identity frame. Default value is recommended. The no command restores the default setting.	
Example	Setting the EAP request frame re-transmission interval to 1200 seconds. Switch(config)#dot1x timeout tx-period 1200	

dot1x unicast enable

Command	[no] dot1x unicast enable

Parameter	none none
Default	The 802.1x unicast passthrough function is not enabled in global mode.
Mode	Global Mode
Usage Guide	Enable the 802.1x unicast passthrough function of switch. The 802.1x unicast passthrough authentication for the switch must be enabled first to enable the 802.1x unicast passthrough function, then the 802.1x function is configured. The no operation of this command will disable this function.
Example	Enabling the 802.1x unicast passthrough function of the switch and enable the 802.1x for port 1/0/1. <pre>Switch(config)#dot1x enable Switch(config)# dot1x unicast enable Switch(config)#interface ethernet1/0/1 Switch(Config-If-Ethernet1/0/1)#dot1x enable</pre>

show dot1x

Command	show dot1x [interface <interface-list>]
Parameter	interface-list the port list,If no parameter is specified, information for all ports is displayed.
Default	None.
Mode	Admin/Global Mode
Usage Guide	Displays dot1x parameter related information, if parameter information is added, corresponding dot1x status for corresponding port is displayed.
Example	Display information about dot1x global parameter for the switch. <pre>Switch#show dot1x Global 802.1x Parameters reauth-enabled no reauth-period 3600 quiet-period 10</pre>

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

3 Commands for the Number Limitation Function of MAC and IP in Port, VLAN

ip arp dynamic maximum

Command	ip arp dynamic maximum <value> no ip arp dynamic maximum	
Parameter	value	upper limit of the number of dynamic ARP in the VLAN, ranging from 1 to 4096
Default	The number limitation function of dynamic ARP in the VLAN is disabled.	
Mode	VLAN Configuration Mode	
Usage Guide	Set the max number of dynamic ARP allowed in the VLAN, and, at the same time, enable the number limitation function of dynamic ARP in the VLAN.	

When configuring the max number of dynamic ARP allowed in the VLAN, if the number of dynamically learnt ARP in the VLAN is already larger than the max number to be set, the extra dynamic ARP will be deleted.

The no command is used to disable the number limitation function of dynamic ARP in the VLAN.

Example

Enable the number limitation function of dynamic ARP in VLAN 1, the max number to be set is 50.

```
Switch(config)#interface vlan1
Switch(config-if-vlan1)# ip arp dynamic maximum 50
```

ipv6 nd dynamic maximum

Command

```
ipv6 nd dynamic maximum <value>
no ipv6 nd dynamic maximum
```

Parameter

value	upper limit of the number of dynamic NEIGHBOR in the VLAN, ranging from 1 to 4096

Default

The number limitation function of dynamic NEIGHBOR in the VLAN is disabled.

Mode

VLAN Configuration Mode

Usage Guide

Set the max number of dynamic NEIGHBOR allowed in the VLAN, and, at the same time, enable the number limitation function of dynamic NEIGHBOR in the VLAN.

When configuring the max number of dynamic NEIGHBOR allowed in the VLAN, if the number of dynamically learnt NEIGHBOR in the VLAN is already larger than the max number to be set, the extra dynamic NEIGHBOR will be deleted.

The no command is used to disable the number limitation function of dynamic NEIGHBOR in the VLAN.

Example

Enable the number limitation function of dynamic NEIGHBOR in VLAN 1, the max number to be set is 50.

```
Switch(config)#interface vlan1
Switch(config-if-vlan1)# ipv6 nd dynamic maximum 50
```

show arp-dynamic count

Command **show arp-dynamic count {vlan | interface ethernet <portName>}**

Parameter	vlan	the specified vlan ID
	portName	the name of layer-2 port

Default None.

Mode Admin/Global Mode

Usage Guide Display the number of dynamic ARP of corresponding port and VLAN.

Example Display the number of dynamic ARP of the port and VLAN which are configured with number limitation function of ARP.

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

show mac-address dynamic count

Command **show mac-address dynamic count { vlan | interface ethernet <portName>}**

Parameter	vlan	display the specified VLAN ID
	portName	the name of layer-2 port

Default None.

Mode	Admin/Global Mode
Usage Guide	Display the number of dynamic MAC of corresponding port and VLAN.
Example	Display the number of dynamic MAC of the port and VLAN which are configured with number limitation function of MAC. <pre> 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 ----- </pre>

show nd-dynamic count

Command	show nd-dynamic count { vlan interface ethernet <portName>}				
Parameter	<table> <tr> <td>vlan</td><td>display the specified VLAN ID</td></tr> <tr> <td>portName</td><td>the name of layer-2 port</td></tr> </table>	vlan	display the specified VLAN ID	portName	the name of layer-2 port
vlan	display the specified VLAN ID				
portName	the name of layer-2 port				
Default	None.				
Mode	Admin/Global Mode				
Usage Guide	Display the number of dynamic ND of corresponding port and VLAN.				
Example	Display the number of dynamic ND of the port and VLAN which are configured with number limitation function of ND. <pre> Switch(config)# show nd-dynamic dynamic count interface ethernet 1/0/3 Port MaxCount CurrentCount ----- </pre>				

Ethernet1/0/3	5	1

Switch(config)# show nd-dynamic dynamic count vlan 1		
Vlan	MaxCount	CurrentCount

1	55	15

switchport arp dynamic maximum

Command **switchport arp dynamic maximum <value>**
no switchport arp dynamic maximum

Parameter	value	upper limit of the number of dynamic ARP of the port, ranging from 1 to 4096

Default The number limitation function of dynamic ARP on the port is disabled.

Mode Port Mode

Usage Guide Set the max number of dynamic ARP allowed by the port, and, at the same time, enable the number limitation function of dynamic ARP on the port.

When configuring the max number of dynamic ARP allowed by the port, if the number of dynamically learnt ARP on the port is already larger than the max number to be set, the extra dynamic ARP will be deleted. TRUNK ports do not supports this function.

The no command is used to disable the number limitation function of dynamic ARP on the port.

Example Enable the number limitation function of dynamic ARP in port 1/0/2 mode, the max number to be set is 20.

Switch(config)#interface ethernet 1/0/2
Switch(config-if-ethernet1/0/2)# switchport arp dynamic maximum 20

switchport mac-address dynamic maximum

Command	switchport mac-address dynamic maximum <value> no switchport mac-address dynamic maximum	
Parameter	value	upper limit of the number of dynamic MAC address of the port, ranging from 1 to 4096
Default	The number limitation function of dynamic MAC address on the port is disabled.	
Mode	Port Mode	
Usage Guide	Set the max number of dynamic MAC address allowed by the port, and at the same time, enable the number limitation function of dynamic MAC address on the port. When configuring the max number of dynamic MAC address allowed by the port, if the number of dynamically learnt MAC address on the port is already larger than the max number of dynamic MAC address to be set, the extra dynamic MAC addresses will be deleted. This function is mutually exclusive to functions such as dot1x, MAC binding, if the functions of dot1x, MAC binding or TRUNK are enabled on the port, this function will not be allowed. The no command is used to disable the number limitation function of dynamic MAC address on the port.	
Example	Enable the number limitation function of dynamic MAC address in port 1/0/2 mode, the max number to be set is 20. <pre>Switch(config)#interface ethernet 1/0/2 Switch(config-if-ethernet1/0/2)# switchport mac-address dynamic maximum 20</pre>	

switchport mac-address violation

Command	switchport mac-address violation {protect shutdown} [recovery <5-3600>] no switchport mac-address violation	
Parameter	protect	protect mode
	shutdown	shutdown mode
	recovery	Configure the border port to automatically restore after execute shutdown violation mode
	<5-3600>	Recovery time, do not restore by default

Default	By default, the port is protected mode.
Mode	Port Mode
Usage Guide	Set the violation mode of the port. The port sets the violation mode after enable the number limit function of MAC only. If the violation mode is protect, the port only disable the dynamic MAC address learning function when the MAC address number of the port exceeds the upper limit of secure MAC. If the violation mode is shutdown, the port will be disabled when the MAC address number exceeds the upper limit of secure MAC, and the user can enable the port by configuring no shutdown command manually or the automatic recovery timeout. The no command restores the violation mode to protect.
Example	Set the violation mode as shutdown, the recovery time as 60s for port1. <pre>Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# switchport mac-address violation shutdown recovery 60</pre>

switchport nd dynamic maximum

Command	switchport nd dynamic maximum <value> no switchport nd dynamic maximum	
Parameter	value	upper limit of the number of dynamic NEIGHBOR of the port, ranging from 1 to 4096
Default	The number limitation function of dynamic ARP on the port is disabled.	
Mode	Port Mode	
Usage Guide	Set the max number of dynamic NEIGHBOR allowed by the port, and, at the same time, enable the number limitation function of dynamic NEIGHBOR on the port. When configuring the max number of dynamic NEIGHBOR allowed by the port, if the number of dynamically learnt NEIGHBOR on the port is already larger than the max number to be set, the extra dynamic NEIGHBOR will be deleted. TRUNK ports do not supports this function. The no command is used to disable the number limitation function of dynamic NEIGHBOR on the port.	

Example

Enable the number limitation function of dynamic NEIGHBOR in port 1/0/2 mode, the max number to be 20.

```
Switch(config)#interface ethernet 1/0/2
```

```
Switch(config-if-ethernet1/0/2)# switchport nd dynamic maximum 20
```

vlan mac-address dynamic maximum

Command

vlan mac-address dynamic maximum <value>

no vlan mac-address dynamic maximum

Parameter

value	upper limit of the number of MAC address in the VLAN, ranging from 1 to 4096

Default

The number limitation function of dynamic MAC address in the VLAN is disabled.

Mode

VLAN Configuration Mode

Usage Guide

Set the max number of dynamic MAC address allowed in the VLAN, and, at the same time, enable the number limitation function of dynamic MAC address in the VLAN.

When configuring the max number of dynamic MAC allowed in the VLAN,if the number of dynamically learnt MAC address in the VLAN is already larger than the max number to be set, the extra dynamic MAC addresses will be deleted. After enabling number limitation function of dynamic MAC in the VLAN, the number limitation of MAC is only applied to general access port, the number of MAC on TURNK ports and special ports which has enabled dot1x, MAC binding function will not be limited or counted.

The no command is used to disable the number limitation function of dynamic MAC address in the VLAN.

Example

Enable the number limitation function of dynamic MAC address in VLAN 1, the max number to be set is 50.

```
Switch(config)#vlan1
```

```
Switch(config-if-vlan1)#vlan mac-address dynamic maximum 50
```

4 Commands for AM Configuration

am enable

Command [no] am enable

Parameter	none	none

Default AM function is disabled by default.

Mode Global Mode

Usage Guide Globally enable/disable AM function.

The no command disables AM function.

Example Enable AM function on the switch.

Switch(config)#am enable

am port

Command [no] am port

Parameter	none	none

Default AM function is disabled on all port.

Mode Port Mode

Usage Guide Enable/disable AM function on port.

The no command disables AM function on the port.

Example Enable AM function on interface 1/0/3 of the switch.

Switch(config-if-ethernet 1/0/3)#am port

am ip-pool

Command `[no] am ip-pool <ip-address> <num>`

Parameter	ip-address	the starting address of an address segment in the IP address pool
	num	the number of consecutive addresses following ip-address, less than or equal with 32

Default By default, IP address pool is empty.

Mode Port Mode

Usage Guide Set the AM IP segment of the interface, allow/deny the IP messages or APRmessages from a source IP within that segment to be forwarded via the interface.

The no command delete configuration.

Example Configure that interface 1/0/3 of the switch will forward data packets from an IP address which is one of 10 consecutive IP addresses starting from 10.10.10.1.

```
Switch(config-if-ethernet 1/0/3)#am ip-pool 10.10.10.1 10
```

am mac-ip-pool

Command `[no] am mac-ip-pool <mac-address> <ip-address>`

Parameter	mac-address	the source MAC address
	ip-address	the source IP address of the packets, which is a 32 bit binary number represented in four decimal numbers

Default By default, MAC-IP address pool is empty.

Mode Port Mode

Usage Guide Set the AM MAC-IP address of the interface, allow/deny the IP messages or APR messages from a source IP within that segment to be forwarded via the interface.

The no command delete configuration.

Example	Configure that the interface 1/0/3 of the switch will allow data packets with a source MAC address of 11-22-22-11-11-11 and a source IP address of 10.10.10.1 to be forwarded. <pre>Switch(config-if-ethernet 1/0/3)#am mac-ip-pool 11-22-22-11-11-11 10.10.10.1</pre>

no am all

Command	no am all [ip-pool mac-ip-pool]				
Parameter	<table> <tr> <td>ip-pool</td><td>the IP address pool</td></tr> <tr> <td>mac-ip-pool</td><td>the MAC-IP address pool</td></tr> </table>	ip-pool	the IP address pool	mac-ip-pool	the MAC-IP address pool
ip-pool	the IP address pool				
mac-ip-pool	the MAC-IP address pool				
Default	By default, both address pools are empty at the beginning.				
Mode	Global Mode				
Usage Guide	Delete MAC-IP address pool or IP address pool or both pools configured by all users.				
Example	Delete all configured IP address pools. <pre>Switch(config)#no am all ip-pool</pre>				

show am

Command	show am [interface <interface-name>]		
Parameter	<table> <tr> <td>interface-name</td><td>the name of the interface of which the configuration information will be displayed</td></tr> </table>	interface-name	the name of the interface of which the configuration information will be displayed
interface-name	the name of the interface of which the configuration information will be displayed		
Default	None.		
Mode	Admin/Global Mode		
Usage Guide	Display the configured AM entries. No parameter means to display the AM configuration information of all interfaces.		
Example	Display all configured AM entries.		

```
Switch#show am interface ethernet 1/0/5
AM is enabled
Interface Ethernet1/0/5
    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
```

5 Commands for Security Feature

dosattack-check srcip-equal-dstip enable

Command	[no] dosattack-check srcip-equal-dstip enable	
Parameter	none	none
Default	Disable the function by which the switch checks if the source IP address is equal to the destination IP address.	
Mode	Global Mode	
Usage Guide	Enable the function by which the switch checks if the source IP address is equal to the destination IP address. By enabling this function, data packet whose source IP address is equal to its destination address will be dropped. The “no” form of this command disables this function.	
Example	Drop the data packet whose source IP address is equal to its destination address. <pre>Switch(config)# dosattack-check srcip-equal-dstip enable</pre>	

dosattack-check tcp-flags enable

Command	[no] dosattack-check srcip-equal-dstip enable	

Parameter	none none
Default	This function disable on the switch by default.
Mode	Global Mode
Usage Guide	Enable the function by which the switch will check the unauthorized TCP label function. With this function enabled, the switch will be able to drop follow four data packets containing unauthorized TCP label: SYN=1 while source port is smaller than 1024;TCP label positions are all 0 while its serial No. =0;FIN=1,URG=1,PSH=1 and the TCP serial No.=0;SYN=1 and FIN=1. This function can be used associating the “dosattack-check ipv4-first-fragment enable” command. The “no” form of this command will disable this function.
Example	Drop one or more types of above four packet types. Switch(config)# dosattack-check tcp-flags enable

dosattack-check srcport-equal-dstport enable

Command	[no] dosattack-check srcport-equal-dstport enable
Parameter	none none
Default	Disable the function by which the switch will check if the source port is equal to the destination port.
Mode	Global Mode
Usage Guide	Enable the function by which the switch will check if the source port is equal to the destination port. With this function enabled, the switch will be able to drop TCP and UDP data packet whose destination port is equal to the source port. This function can be used associating the “dosattack-check ipv4-first-fragment enable” function so to block the IPv4 fragment TCP and UDP data packet whose destination port is equal to the source port. The no command disables this function.
Example	Drop the non-fragment TCP and UDP data packet whose destination port is equal to the source port.

6 Commands for TACACS+

tacacs-server authentication host

Command **tacacs-server authentication host <ip-address> [port <port-number>][timeout <seconds>] [key {0 | 7} <string>] [primary]**
no tacacs-server authentication host <ip-address>

Parameter	ip-address	the IP address of the server
	port-number	the listening port number of the server, the valid range is 0~65535, amongst 0 indicates it will not be an authentication server
	seconds	the value of TACACS+ authentication timeout timer, shown in seconds and the valid range is 1~60
	string	the key string, If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters
	primary	indicates it's a primary server

Default No TACACS+ authentication configured on the system by default.

Mode Global Mode

Usage Guide This command is for specifying the IP address, port number, timeout timer value and the key string of the TACACS+ server used on authenticating with the switch.

The parameter port is for define an authentication port number which must be in accordance with the authentication port number of specified TACACS+ server which is 49 by default. The parameters key and timeout is used to configure the self-key and self-timeout, if the switch is not configure the timeout<seconds> and key<string>, it will use the global value and key by command tacacs-server timeout<seconds> and tacacs-server key <string>. This command can configure several TACACS+ servers communicate with the switch. The configuration sequence will be used as authentication server sequence. And in case primary is configured on one TACACS+ server, the server will be the primary server.

The no form of this command deletes TACACS+ authentication server.

Example Configure the TACACS+ authentication server address to 192.168.1.2, and use the global configured key.

Switch(config)#tacacs-server authentication host 192.168.1.2

tacacs-server key

Command	tacacs-server key {0 7} <string> no tacacs-server key	
Parameter	string	the key string of the TACACS+ server. If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters.
Default	None.	
Mode	Global Mode	
Usage Guide	Configure the key of TACACS+ authentication server. The key is used on encrypted packet communication between the switch and the TACACS+ server. The configured key must be in accordance with the one on the TACACS+ server or else no correct TACACS+ authentication will be performed. It is recommended to configure the authentication server key to ensure the data security. The no command deletes the TACACS+ server key.	
Example	Configure test as the TACACS+ server authentication key. <pre>Switch(config)#tacacs-server key 0 test</pre>	

tacacs-server nas-ipv4

Command	tacacs-server nas-ipv4 <ip-address> no tacacs-server nas-ipv4	
Parameter	ip-address	the source IP address of TACACS+ packet, in dotted decimal notation, it must be a valid unicast IP address
Default	By default, no specific source IP address for TACACS+ packet is configured, the IP address of the interface from which the TACACS+ packets are sent is used as source IP address of TACACS+ packet.	

Mode	Global Mode
Usage Guide	Configure the source IP address of TACACS+ packet sent by the switch. The source IP address must belongs to one of the IP interface of the switch, otherwise an failure message of binding IP address will be returned when the switch send TACACS+ packet. We suggest using the IP address of loopback interface as source IP address, it avoids that the packets from TACACS+ server are dropped when the interface link-down. The no command deletes the configuration.
Example	Configure the source ip address of TACACS+ packet as 192.168.2.254. <pre>Switch(config)#tacacs-server nas-ipv4 192.168.2.254</pre>

tacacs-server timeout

Command	tacacs-server timeout <seconds> no tacacs-server timeout	
Parameter	seconds	the value of TACACS+ authentication timeout timer, shown in seconds and the valid range is 1~60
Default	3 seconds by default.	
Mode	Global Mode	
Usage Guide	Configure a TACACS+ server authentication timeout timer. The command specifies the period the switch wait for the authentication through TACACS+ server. When connected to the TACACS+, and after sent the authentication query data packet to the TACACS+ server, the switch waits for the response. If no replay is received during specified period, the authentication is considered failed. The no command restores the default configuration.	
Example	Configure the timeout timer of the tacacs+ server to 30 seconds. <pre>Switch(config)#tacacs-server timeout 30</pre>	

7 Commands for RADIUS

aaa enable

Command	[no] aaa enable	
Parameter	none	none
Default	AAA authentication is not enabled by default.	
Mode	Global Mode	
Usage Guide	Enables the AAA authentication function in the switch. The AAA authentication for the switch must be enabled first to enable IEEE 802.1x authentication for the switch. The no command disables the AAA authentication function.	
Example	Enabling AAA function for the switch. Switch(config)#aaa enable	

aaa-accounting enable

Command	[no] aaa-accounting enable	
Parameter	none	none
Default	AAA accounting is not enabled by default.	
Mode	Global Mode	
Usage Guide	Enables the AAA accounting function in the switch. When accounting is enabled in the switch, accounting will be performed according to the traffic or online time for port the authenticated user is using. The switch will send an “accounting started” message to the RADIUS accounting server on starting the accounting, and an accounting packet for the online user to the RADIUS accounting server every five seconds, and an “accounting stopped” message is sent to the RADIUS accounting server on accounting end. Note: The switch send the “user offline” message to the RADIUS accounting server only when accounting is enabled, the “user offline” message will not be sent to the RADIUS authentication server.	

The no command disables the AAA accounting function.

Example

Enabling AAA accounting for the switch.

```
Switch(config)#aaa-accounting enable
```

aaa-accounting update

Command

aaa-accounting update {enable | disable}

Parameter

none	none

Default

By default, Enable the AAA update accounting function.

Mode

Global Mode

Usage Guide

Enable or disable the AAA update accounting function.
After the update accounting function is enabled, the switch will sending accounting message to each online user on time.

Example

Disable the AAA update accounting function for switch.

```
Switch(config)#aaa-accounting update disable
```

radius nas-ipv4

Command

radius nas-ipv4 <ip-address>
no radius nas-ipv4

Parameter

ip-address	the source IP address of the RADIUS packet, in dotted decimal notation, it must be a valid unicast IP address

Default

By default, No specific source IP address for RADIUS packet is configured, the IP address of the interface from which the RADIUS packets are sent is used as source IP address of RADIUS packet.

Mode	Global Mode
Usage Guide	Configure the source IP address for RADIUS packet sent by the switch. The source IP address must belongs to one of the IP interface of the switch, otherwise an failure message of binding IP address will be returned when the switch send RADIUS packet. We suggest using the IP address of loopback interface as source IP address, it avoids that the packets from RADIUS server are dropped when the interface link-down. The no command deletes the configuration.
Example	Configure the source ip address of RADIUS packet as 192.168.2.254. <pre>Switch(config)#radius nas-ipv4 192.168.2.254</pre>

radius nas-ipv6

Command	radius nas-ipv6 <ipv6-address> no radius nas-ipv6		
Parameter	<table> <tr> <td>ipv6-address</td><td>the source IPv6 address of the RADIUS packet, it must be a valid unicast IPv6 address</td></tr> </table>	ipv6-address	the source IPv6 address of the RADIUS packet, it must be a valid unicast IPv6 address
ipv6-address	the source IPv6 address of the RADIUS packet, it must be a valid unicast IPv6 address		
Default	By default, No specific source IPv6 address for RADIUS packet is configured, the IPv6 address of the interface from which the RADIUS packets are sent is used as source IPv6 address of RADIUS packet.		
Mode	Global Mode		
Usage Guide	Configure the source IPv6 address for RADIUS packet sent by the switch. The source IPv6 address must belongs to one of the IPv6 interface of the switch, otherwise a failure message of binding IPv6 address will be returned when the switch send RADIUS packet. We suggest using the IPv6 address of loopback interface as source IPv6 address, it avoids that the packets from RADIUS server are dropped when the interface link-down. The no command deletes the configuration.		
Example	Configure the source ipv6 address of RADIUS packet as 2001:da8:456::1. <pre>Switch(config)#radius nas-ipv6 2001:da8:456::1</pre>		

radius-server accounting host

Command **radius-server accounting host** {<ipv4-address> | <ipv6-address>} [port <port-number>] [key {0 | 7} <string>] [primary]
no radius-server accounting host {<ipv4-address> | <ipv6-address>}

Parameter	ipv4-address	stands for the server IPv4 address
	ipv6-address	stands for the server IPv6 address
	port-number	server listening port number from 0 to 65535
	string	the key string. If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters
	primary	for primary server. Multiple RADIUS sever can be configured and would be available. RADIUS server will be searched by the configured order if primary is not configured, otherwise, the specified RADIUS server will be used first

Default No RADIUS accounting server is configured by default.

Mode Global Mode

Usage Guide Specifies the IPv4/IPv6 address and the port number, whether be primary server for RADIUS accounting server.
This command is used to specify the IPv4/IPv6 address and port number of the specified RADIUS server for switch accounting, multiple command instances can be configured. The <port-number> parameter is used to specify accounting port number, which must be the same as the specified accounting port in the RADIUS server; the default port number is 1813. If this port number is set to 0, accounting port number will be generated at random and can result in invalid configuration. This command can be used repeatedly to configure multiple RADIUS servers communicating with the switch, the switch will send accounting packets to all the configured accounting servers, and all the accounting servers can be backup servers for each other. If primary is specified, then the specified RADIUS server will be the primary server. It only configures a RADIUS primary server whether the server use IPv4 address or IPv6 address.

The no command deletes the RADIUS accounting server.

Example Sets the RADIUS accounting server of IPv6 address to 2004:1:2:3::2, as the primary server, with the accounting port number as 3000.

Switch(config)#radius-server accounting host 2004:1:2:3::2 port 3000 primary

radius-server authentication host

Command **radius-server authentication host** {<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>}

Parameter	ipv4-address	stands for the server IPv4 address
	ipv6-address	stands for the server IPv6 address
	port-number	server listening port number from 0 to 65535
	string	the key string. If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters
	primary	for primary server. Multiple RADIUS sever can be configured and would be available. RADIUS server will be searched by the configured order if primary is not configured, otherwise, the specified RADIUS server will be used first
	dot1x telnet	designates the current RADIUS server only use 802.1x authentication or telnet authentication, all services can use current RADIUS server by default

Default No RADIUS authentication server is configured by default.

Mode Global Mode

Usage Guide Specifies the IPv4 address or IPv6 address and listening port number, cipher key, whether be primary server or not and access mode for the RADIUS server.

This command is used to specify the IPv4 address or IPv6 address and port number, cipher key string and access mode of the specified RADIUS server for switch authentication, multiple command instances can be configured. The port parameter is used to specify authentication port number, which must be the same as the specified authentication port in the RADIUS server, the default port number is 1812. If this port number is set to 0, the specified server is regard as non-authenticating. This command can be used repeatedly to configure multiple RADIUS servers communicating with the switch, the configured order is used as the priority for the switch authentication server. When the first server has responded (whether the authentication is succeeded or failed), switch does not send the authentication request to the next. If primary is specified, then the specified RADIUS server will be the primary server. It will use the cipher key which be configured by radius-server key <string> global command if the current RADIUS server not configure key<string>. Besides, it can designate the current RADIUS server only use 802.1x authentication or telnet authentication via access-mode option. It is not configure access-mode option and all services can use current RADIUS server by default.

The no command deletes the RADIUS authentication server.

Example Setting the RADIUS authentication server address as 2004:1:2:3::2.

```
Switch(config)#radius-server authentication host 2004:1:2:3::2
```

radius-server dead-time

Command	radius-server dead-time <minutes> no radius-server dead-time	
Parameter	minutes	the down -restore time for RADIUS server in minutes, the valid range is 1 to 255
Default	The default value is 5 minutes.	
Mode	Global Mode	
Usage Guide	This command specifies the time to wait for the RADIUS server to recover from inaccessible to accessible. When the switch acknowledges a server to be inaccessible, it marks that server as having invalid status, after the interval specified by this command; the system resets the status for that server to valid. The no command restores the default setting.	
Example	Setting the down-restore time for RADIUS server to 3 minutes. <pre>Switch(config)#radius-server dead-time 3</pre>	

radius-server key

Command	radius-server key {0 7} <string> no radius-server key	
Parameter	string	a key string for RADIUS server, If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters
Default	None.	

Mode	Global Mode
Usage Guide	Specifies the key for the RADIUS server (authentication and accounting). The key is used in the encrypted communication between the switch and the specified RADIUS server. The key set must be the same as the RADIUS server set, otherwise, proper RADIUS authentication and accounting will not perform properly. The no command deletes the key for RADIUS server.
Example	Setting the RADIUS authentication key to be "test". Switch(config)#radius-server key 0 test

radius-server retransmit

Command	radius-server retransmit <retries> no radius-server retransmit
Parameter	retries a retransmission times for RADIUS server, the valid range is 0 to 100
Default	The default value is 3 times.
Mode	Global Mode
Usage Guide	This command specifies the retransmission time for a packet without a RADIUS server response after the switch sends the packet to the RADIUS server. If authentication information is missing from the authentication server, AAA authentication request will need to be re-transmitted to the authentication server. If AAA request retransmission count reaches the retransmission time threshold without the server responding, the server will be considered to as not work, the switch sets the server as invalid. The no command restores the default setting.
Example	Setting the RADIUS authentication packet retransmission time to five times. Switch(config)#radius-server retransmit 5

radius-server timeout

Command	radius-server timeout <seconds> no radius-server timeout	
Parameter	seconds	the timer value (second) for RADIUS server timeout, the valid range is 1 to 1000
Default	The default value is 3 seconds.	
Mode	Global Mode	
Usage Guide	This command specifies the interval for the switch to wait RADIUS server response. The switch waits for corresponding response packets after sending RADIUS Server request packets. If RADIUS server response is not received in the specified waiting time, the switch resends the request packet or sets the server as invalid according to the current conditions. The no command restores the default setting.	
Example	Setting the RADIUS authentication timeout timer value to 30 seconds. Switch(config)#radius-server timeout 30	

radius-server accounting-interim-update timeout

Command	radius-server accounting-interim-update timeout <seconds> no radius-server accounting-interim-update timeout	
Parameter	seconds	the interval of sending fee-counting update messages, in seconds, ranging from 60 to 3600
Default	The default interval of sending fee-counting update messages is 300 seconds.	
Mode	Global Mode	
Usage Guide	This command set the interval at which NAS sends fee-counting update messages. In order to realize the real time fee-counting of users, from the moment the user becomes online, NAS will send a fee-counting update message of this user to the RADIUS server at the configured interval.	

The interval of sending fee-counting update messages is relative to the maximum number of users supported by NAS. The smaller the interval, the less the maximum number of the users supported by NAS; the bigger the interval, the more the maximum number of the users supported by NAS. The following is the recommended ratio of interval of sending fee-counting update messages to the maximum number of the users supported by NAS:

The maximum number of users	The interval of sending fee-counting update messages(in seconds)
1-299	300 (default)
300-599	600
600-1199	1200
1200-1799	1800
≥1800	3600

The no operation of this command will reset to the default configuration.

Example

The maximum number of users supported by NAS is 700, the interval of sending fee-counting update messages 1200 seconds.

Switch(config)#radius-server accounting-interim-update timeout 1200

show aaa authenticated-user

Command

show aaa authenticated-user

Parameter

none none

Default

None.

Mode

Admin/Global Mode

Usage Guide

Displays the authenticated users online.
Usually the administrator concerns only information about the online user, the other information displayed is used for troubleshooting by technical support.

Example

Displays the authenticated users online.

Switch(config)#show aaa authenticated-user

```

----- authenticated users -----
-----
UserName  Retry RadID  Port  EapID  ChapID  OnTime  UserIP  MAC
-----
```

----- total: 0 -----

show aaa authenticating-user

Command	show aaa authenticating-user
Parameter	none none
Default	None.
Mode	Admin/Global Mode
Usage Guide	Display the authenticating users. Usually the administrator concerns only information about the authenticating user, the other information displays is used for troubleshooting by the technical support.
Example	Display the authenticating users. Switch(config)#show aaa authenticating-user ----- authenticating users ----- ----- User-name Retry-time Radius-ID Port Eap-ID Chap-ID Mem-Addr State ----- ----- ----- total: 0 -----

show aaa config

Command	show aaa config
Parameter	none none
Default	None.
Mode	Admin/Global Mode
Usage Guide	Displays whether aaa authentication, accounting are enabled and information for key,

authentication and accounting server specified.

Example

Display aaa configuration information.

Switch(config)#show aaa config

----- AAA config data -----

Is Aaa Enabled = 1 :1 means AAA authentication is enabled, 0 means is not enabled

Is Account Enabled= 1 :1 means AAA account is enabled, 0 means is not enabled

MD5 Server Key = yangshifeng : Authentication key

authentication server sum = 2 :Configure the number of authentication server

.....

show radius authenticated-user count

Command

show radius authenticated-user count

Parameter

none none

Default

None.

Mode

Admin/Global Mode

Usage Guide

Show the number of on-line users who have already passed the authentication.

Example

Show the number of on-line users who have already passed the authentication.

Switch(config)#show radius authenticated-user count

The authenticated online user num is: 105

show radius authenticating-user count

Command

show radius authenticating-user count

Parameter

none none

Default

None.

Mode	Admin/Global Mode
Usage Guide	Show the number of the authenticating-user.
Example	Show the number of the authenticating-user. Switch(config)#show radius authenticating-user count The authenticating user num is: 10

8 Commands for SSL Configuration

ip http secure-server

Command	[no] ip http secure-server
Parameter	none none
Default	By default, this function is disabled.
Mode	Global Mode
Usage Guide	This command is used for enable and disable SSL function. After enable SSL function, the users visit the switch through https client, switch and client use SSL connect, can form safety SSL connect channel. After that, all the data which transmit of the application layer will be encrypted, then ensure the privacy of the communication. The no command disables SSL function.
Example	Enable SSL function. Switch(config)#ip http secure-server

ip http secure-port

Command	ip http secure-port <port-number> no ip http secure-port

Parameter	<table> <tr> <td>port-number</td><td>means configured port number, range between 1025 and 65535. 443 is for default</td></tr> </table>	port-number	means configured port number, range between 1025 and 65535. 443 is for default
port-number	means configured port number, range between 1025 and 65535. 443 is for default		
Default	By default, SSL port number is not configured.		
Mode	Global Mode		
Usage Guide	Configure/delete port number by SSL used. If this command is used to configure the port number, then the configured port number is used to monitor. If the port number for https is changed, when users try to use https to connect, must use the changed one. For example:https://device:port_number. SSL function must reboot after every change. The no command removes the configured port number.		
Example	Configure the port number is 1028. Switch(config)#ip http secure-port 1028		

ip http secure- ciphersuite

Command	ip http secure-ciphersuite { aes256-sha ecdhe-rsa-aes256-sha } no ip http secure-ciphersuite	
Parameter	aes256-sha	AES256-SHA
	ecdhe-rsa-aes256-sha	ECDHE-RSA-AES256-SHA
Default	By default, SSL secure password suite is not configured.	
Mode	Global Mode	
Usage Guide	Configure/delete secure cipher suite by SSL used. If this command is used to configure the secure cipher suite, specified encryption method will be used. The SSL should be restarted to take effect after changes on configuration.	
	No command removes the configured secure password suite.	
Example	Configure the secure cipher suite is aes256-sha. Switch(config)#ip http secure- ciphersuite aes256-sha	

show ip http secure-server status

Command	show ip http secure-server status	
Parameter	none	none
Default	None.	
Mode	Admin/Global Mode	
Usage Guide	Show the status for the configured SSL.	
Example	Show the status for the configured SSL. Switch(config)#show ip http secure-server status HTTP secure server status: Enabled HTTP secure server port: 1028 HTTP secure server ciphersuite: rc4-128-sha	

9 Commands for IPv6 Security RA

ipv6 security-ra enable

Command	[no] ipv6 security-ra enable	
Parameter	none	none
Default	The IPv6 security RA function is disabled by default.	
Mode	Global Mode	
Usage Guide	Globally enable IPv6 security RA function, all the RA advertisement messages will not be forwarded through hardware, but only sent to CPU to handle. Only after enabling the global security RA function, the security RA on a port can be enabled. Globally disabling security RA will clear all the configured security RA ports. The global security RA function and the global IPv6 SAVI function are mutually exclusive, so they can not	

be enabled at the same time.

The no operation of this command will globally disable IPv6 security RA function.

Example

Globally enable IPv6 security RA.

Switch(config)#ipv6 security-ra enable

ipv6 security-ra enable

Command

[no] ipv6 security-ra enable

Parameter

none	none

Default

The IPv6 security RA function is disabled by default.

Mode

Port Configuration Mode

Usage Guide

Enable IPv6 security RA on a port, causing this port not to forward the received RA message.

Only after globally enabling the security RA function, can the security RA on a port be enabled. Globally disabling security RA will clear all the configured security RA ports.

The no ipv6 security-ra enable will disable the IPv6 security RA on a port.

Example

Enable IPv6 security RA on a port.

Switch(config-if-ethernet1/0/2)#ipv6 security-ra enable

show ipv6 security-ra

Command

show ipv6 security-ra [interface <interface-list>]

Parameter

interface-list	Specifies the port number. No parameter will display all distrust ports, entering a parameter will display the corresponding distrust port.

Default	None.
Mode	Admin/Global Mode
Usage Guide	Display all the interfaces with IPv6 RA function enabled.
Example	Display all the interfaces with IPv6 RA function enabled. 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

10 Commands for MAB

authentication mab

Command	authentication mab {radius local} (none) no authentication mab	
Parameter	radius	means RADIUS authentication mode
	local	means the local authentication
	none	means the authentication is needless
Default	By default, using RADIUS authentication mode.	
Mode	Global Mode	
Usage Guide	Configure the authentication mode and priority of MAC address authentication. none option is used to the fleeing function of MAC address authentication. If all configured RADIUS servers don't respond, switch will adopt none authentication mode to allow that MAC address authentication users access the network directly. The option of local is used for the local authentication of MAC address, it authenticates through the local user name and password. If configured as the method of authentication mab radius local none, judge if configured the user name and password used in mab authentication in local when the radius server has no response. If it has been configured, use the local authentication, if not, use the backup none authentication. The no command restores the default authentication mode.	

Example

Configure the local authentication and the fleeing function of MAC address authentication.

```
Switch(config)#authentication mab radius local none
```

clear mac-authentication-bypass binding

Command

```
clear mac-authentication-bypass binding {mac WORD | interface (ethernet IFNAME | IFNAME) | all}
```

Parameter

mac	Delete MAB binding of the specified MAC address
IFNAME	Delete MAB binding of the specified port
all	Delete all MAB binding

Default

None.

Mode

Admin Mode

Usage Guide

Clear MAB binding information.

Example

Delete all MAB binding.

```
Switch#clear mac-authentication-bypass binding all
```

mac-authentication-bypass binding-limit

Command

```
mac-authentication-bypass binding-limit <1-100>  
no mac-authentication-bypass binding-limit
```

Parameter

1-100	the max binding number of MAB, ranging from 1 to 100

Default

By default, the max binding number of MAB is 3.

Mode

Port Configuration Mode

Usage Guide

Set the max binding number of MAB.

Set the max binding number of MAB. When the binding number reaches to the max value, the port will stop binding, if the max binding number is less than the current binding number of the port, the setting will be unsuccessful.

The no command will restore the default binding number as 3.

Example

Configure the max binding number as 10.

```
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#mac-authentication-bypass binding-limit 10
```

mac-authentication-bypass enable

Command	[no] mac-authentication-bypass enable

Parameter	none none

Default	By default, disable the global and port MAB function.

Mode	Port Configuration Mode

Usage Guide	Enable the global and port MAB function. To process MAB authentication of a port, enable the global MAB function first, and then, enable the MAB function of the corresponding port. The no command disables MAB function.

Example	Enable the global and port Eth1/0/1 MAB function.

```
Switch(config)#mac-authentication-bypass enable
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#mac-authentication-bypass enable
```

mac-authentication-bypass guest-vlan

Command	mac-authentication-bypass guest-vlan <1-4094> no mac-authentication-bypass guest-vlan

Parameter	1-4094 guest vlan ID, ranging from 1 to 4094
Default	None.
Mode	Port Configuration Mode
Usage Guide	Set guest vlan of MAB authentication. Set guest vlan of MAB authentication, only Hybrid port use this command, it is not take effect on access port. After MAB authentication is failing, if the existent guest vlan is configured by the port connecting to the MAB user, the MAB user can join and access guest vlan. The no command deletes guest vlan.
Example	Configure guest vlan of MAB authentication for port 1/0/1. <pre>Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#mac-authentication-bypass guest-vlan 10</pre>

mac-authentication-bypass spoofing-garp-check

Command	[no] mac-authentication-bypass spoofing-garp-check
Parameter	none none
Default	By default, disable spoofing-garp-check function.
Mode	Global Mode
Usage Guide	Enable the spoofing-garp-check function, MAB function will not deal with spoofing-garp any more When the terminal of Windows operating system detects the address conflict, it will sends a gratuitous ARP to correct the error ARP entries generated by gratuitous ARP of the conflict detection. This command is used to detect the spoofing-garp when occuring the address conflict, MAB function is not deal with the packet any more. Notice: when enabling the check function, all ARP will be processed the software check, it will add switch's load. The no command disables the function.
Example	Enable spoofing-garp-check function.

Switch(config)#mac-authentication-bypass spoofing-garp-check enable

mac-authentication-bypass timeout linkup-period

Command	mac-authentication-bypass timeout linkup-period <0-30> no mac-authentication-bypass timeout linkup-period	
Parameter	0-30	After the port is shutdown automatically, the interval before it up again, the unit is second, 0 means there is no down/up operation
Default	By default, the interval is 0.	
Mode	Global Mode	
Usage Guide	Set the interval between down and up when VLAN binding in a port is changing to assure the user can obtain IP again. When MAB authentication is successful, belong to vlan according to auto-vlan setting, when MAB authentication is failing, belong to vlan according to guest-vlan setting. After linkup-period is set, when VLAN binding of a port is changing, the port will be shutdown automatically, and will be up again after linkup-period to assure the client obtain IP. The no command to restore default values.	
Example	Configure down/up time as 12s. Switch(config)#mac-authentication-bypass timeout linkup-period 12	

mac-authentication-bypass timeout offline-detect

Command	mac-authentication-bypass timeout offline-detect (0 <60-43200>) no mac-authentication-bypass timeout offline-detect	
Parameter	0 <60-43200>	offline-detect time, the range is 0 or 60 to 43200s
Default	By default, offline-detect time is 180s.	

Mode	Global Mode
Usage Guide	Configure offline-detect time. When offline-detect time is 0, the switch does not detect MAB binding, when offline-detect time is 60s to 43200s, the switch timely detects the flow corresponding to the MAB binding. If there is no flow in the period of offline-detect time, it will delete this binding and forbid the flow to pass. The no command restores the default value.
Example	Configure offline-detect time as 200s. <pre>Switch(config)#mac-authentication-bypass timeout offline-detect 200</pre>

mac-authentication-bypass timeout quiet-period

Command	<pre>mac-authentication-bypass timeout quiet-period <1-60> no mac-authentication-bypass timeout quiet-period</pre>		
Parameter	<table> <tr> <td>1-60</td><td>quiet-period, ranging from 1 to 60s</td></tr> </table>	1-60	quiet-period, ranging from 1 to 60s
1-60	quiet-period, ranging from 1 to 60s		
Default	By default, quiet-period is 30s.		
Mode	Global Mode		
Usage Guide	Set quiet-period of MAB authentication. If MAB authentication is failing, within the quiet-period the switch will not respond the authentication request of this MAC, after quiet-period, it will respond the request again. The no command restores quiet-period as the default value.		
Example	Configure quiet-period of MAB authentication as 60s. <pre>Switch(config)#mac-authentication-bypass timeout quiet-period 60</pre>		

mac-authentication-bypass timeout reauth-period

Command	mac-authentication-bypass timeout reauth-period <1-3600> no mac-authentication-bypass timeout reauth-period
Parameter	1-3600 reauthentication interval, ranging from 1 to 3600s
Default	By default, reauthentication interval is 30s.
Mode	Global Mode
Usage Guide	Set the reauthentication interval at failing authentication state. At failing authentication state, the user processes the reauthentication timely until the authentication is successful; at the successful state, the user can access the network resources. The no command restores the default value.
Example	Configure reauthentication time as 20s. Switch(config)#mac-authentication-bypass timeout reauth-period 20

mac-authentication-bypass timeout stale-period

Command	mac-authentication-bypass timeout stale-period <0-60> no mac-authentication-bypass timeout stale-period
Parameter	0-60 The time that delete the binding, ranging from 0 to 60s
Default	By default, it takes 30 s. to delete the binding.
Mode	Global Mode
Usage Guide	Set the time that delete the binding user after MAB port is down. If the time that delete the binding as 0, delete all user binding of this port as soon as the MAB port is down, if the time is bigger than 0, delete the user binding with a delay after the MAB port is down. The no command restores the default value.
Example	Configure the deletion time as 40s. Switch(config)#mac-authentication-bypass timeout stale-period 40

mac-authentication-bypass username-format

Command	[no] mac-authentication-bypass username-format {mac-address {fixed username WORD password WORD}}	
Parameter	mac-address	Use MAC address of MAB user as username and password to authenticate
	fixed username WORD	Use the specified username and password to authenticate, the length of username and password ranges between 1 and 32
	password WORD	characters
Default	By default, use MAC address of MAB user as username and password to authenticate.	
Mode	Global Mode	
Usage Guide	Set the authenticate method of MAB authentication. There are two methods for MAB authentication: use MAC address of MAB user as username and password to authenticate or use the specified username and password to authenticate. If there is no specified username and password, the device uses the first method to authenticate by default. The no command to restore default values.	
Example	All MAB users use the same username and password to authenticate, the username is mab-user, the password is mab-pwd. <pre>Switch(config)#mac-authentication-bypass username-format fixed username mab-user password mab-pwd</pre>	

show mac-authentication-bypass

Command	show mac-authentication-bypass {interface {ethernet IFNAME IFNAME}}	
Parameter	IFNAME	Port name
Default	None.	

Mode	Admin/Global Mode
Usage Guide	Show the binding information of MAB authentication.

Example Show the binding information of MAB authentication.

Switch#show mac-authentication-bypass

The Number of all binding is 5

MAC	Interface	Vlan ID	State

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

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: Ethernet1/1

Client MAC: 00-0a-eb-6a-7f-8e

Binding State: MAB_AUTHENTICATED

Binding State Lease: 164 seconds left

11 Commands for MAB PPPoE Intermediate Agent

pppoe intermediate-agent

Command [no] pppoe intermediate-agent

Parameter	none	none

Default By default, disable global PPPoE intermediate agent function.

Mode Global Mode

Usage Guide Enable global PPPoE intermediate agent function.
After enable global PPPoE IA function, process the packet of PPPoE discovery stage according to the related configuration.

The no command disables global PPPoE intermediate agent function.

Example

Enable global PPPoE intermediate agent function.

```
Switch(config)#pppoe intermediate-agent
```

pppoe intermediate-agent (Port)

Command

[no] pppoe intermediate-agent

Parameter

none	none

Default

By default, disable PPPoE intermediate agent function of the port.

Mode

Port Configuration Mode

Usage Guide

Enable PPPoE intermediate agent function of the port.

After enable PPPoE IA function of the port, add vendor tag for PPPoE packet of the port.

Note:

1. It must enable global pppoe intermediate-agent function.
2. At least one port is connected to PPPoE server, and the port mode is trust.

The no command disables PPPoE intermediate agent function of the port.

Example

Enable PPPoE intermediate agent function of the port ethernet 1/0/2.

```
Switch(config-if-ethernet1/0/2)#pppoe intermediate agent
```

pppoe intermediate-agent circuit-id

Command

[no] pppoe intermediate-agent circuit-id <string>

Parameter

string	circuit-id, the max character number is 63 bytes

Default

This function is not configured by default.

Mode	Port Configuration Mode
Usage Guide	Configure circuit ID of the port. This command configures circuit-id alone for each port, the priority is higher than pppoe intermediate-agent identifier-string command. The no command cancels this configuration.
Example	Configure circuit-id as abcd/efgh on port ethernet1/0/3 of vlan3. <pre>Switch(config-if-ethernet1/0/3)#pppoe intermediate-agent circuit-id abcd/efgh</pre>

pppoe intermediate-agent delimiter

Command	pppoe intermediate-agent delimiter <WORD> no pppoe intermediate-agent delimiter
Parameter	WORD the delimiter, its range is (# . . : / space)
Default	By default, the fields is comparted with '\0'.
Mode	Global Mode
Usage Guide	Configure the delimiter among the fields in circuit-id and remote-id. After configuring the delimiter, the added fields of circuit-id and remote-id use the configured delimiter to compart. Notice: The global pppoe intermediate-agent function must be enabled. The no command cancels the configuration.
Example	Configuration delimiter is space. <pre>Switch(config)#pppoe intermediate-agent delimiter space</pre>

pppoe intermediate-agent format

Command	pppoe intermediate-agent format (circuit-id remote-id) (hex ascii) no pppoe intermediate-agent format (circuit-id remote-id)

Parameter	hex	hexadecimal
	ascii	ASCII code
Default	This function is not configured by default.	
Mode	Global Mode	
Usage Guide	Configure the format with hex or ASCII for circuit-id and remote-id. Encapsulation circuit-id and remote-id with hex ASCII format to vendor tag. Notice: The global pppoe intermediate-agent function must be enabled. The no command cancels the configuration.	
Example	Configure the trust port 1/0/1 to enable vendor-tag strip function. Switch(config)#pppoe intermediate-agent format remote-id ascii	

pppoe intermediate-agent remote-id

Command	[no] pppoe intermediate-agent remote-id <string>	
Parameter	string	remote-id, the max character number is 63 bytes
Default	This function is not configured by default.	
Mode	Port Configuration Mode	
Usage Guide	Configure remote-id of the port. Configure remote-id for each port, if there is no configuration, use switch's MAC as remote-id value. The no command cancels this configuration.	
Example	Configure remote-id as abcd on port ethernet1/0/2. Switch(config-if-ethernet1/0/2)# pppoe intermediate-agent remote-id abcd	

pppoe intermediate-agent trust

Command [no] pppoe intermediate-agent trust

Parameter	none	none

Default By default, the port is a untrust port.

Mode Port Configuration Mode

Usage Guide Configure the port as trust port.
The port which connect to server must be configured as trust port.
Note: At least one trust port is connected to PPPoE server.

The no command configures the port as untrust port.

Example Configure port ethernet1/0/1 as trust port.

Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent trust

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

Parameter	vlan	VLAN ID
	port	port number
	id switch-id mac	the local MAC address
	id switch-id hostname	the local host name
	remote-mac	the remote MAC address
	string WORD	the specified keyword

Default By default, this configuration is null.

Mode Global Mode

Usage Guide Configure the self-defined circuit-id.

This configuration and type tr-101 circuit-id are mutually exclusive, it will clear the corresponding configuration of type tr-101 circuit-id.

The no command cancels the configuration.

Example

Configure the self-defined circuit-id as vlan port id switch-id hostname.

Switch(config)#pppoe intermediate-agent type self-defined circuit-id vlan port id switch-id hostname

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

Parameter

mac	Ethernet port MAC address
vlan-mac	IP interface MAC address
hostname	the local host name
string WORD	the specified keyword

Default

By default, this configuration is empty.

Mode

Global Mode

Usage Guide

Configure the self-defined remote-id.
Configuration order of this command according to the fields order in remote-id.

The no command cancels the configuration.

Example

Configure the self-defined remote-id as string abcd mac hostname.

Switch(config)#pppoe intermediate-agent type self-defined remoteid string abcd mac hostname

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

Parameter	string access-node-id, the max character number is 47 bytes.
Default	By default, MAC address of the switch.
Mode	Global Mode
Usage Guide	Configure access-node-id field value of circuit ID in the added vendor tag with tr-101 standard. Use this configuration to create access-node-id of circuit ID in vendor tag.circuit-id value is access-node-id + " eth " + Slot ID + delimiter + Port Index + delimiter + Vlan ID, access-node-id occupies n bytes (n<48), " eth " is space + e + t + h + space, it occupies 5 bytes, Slot ID occupies 2 bytes, Port Index occupies 3 bytes, Vlan ID occupies 4 bytes, delimiter occupies 1 byte. In default state, access-node-id value of circuit-id is switch's MAC, it occupies 6 bytes. For example: MAC address is "0a0b0c0d0e0f", Slot ID is 12, Port Index is 34, Vlan ID is 567, the default circuit-id value is "0a0b0c0d0e0f eth 12/034:0567". The no command unconfigured.
Example	Configure access-node-id value of circuit ID as abcd in vendor tag. <pre>Switch(config)#pppoe intermediate-agent type tr-101 circuit-id access-node-id abcd</pre>

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						
Parameter	<table><tr><td>string</td><td>identifier-string, the max character number is 47 bytes</td></tr><tr><td>{sp sv pv spv}</td><td>This option can select the combination format for slot, port, vlan, sp means slot and port, sv means slot and vlan, pv means port and vlan, spv means slot, port and vlan</td></tr><tr><td>WORD</td><td>The delimiter between slot, port and vlan, the range is (# . , ; : / space). Note: There are two delimiter WORDs in spv combo mode, the first between slot and port, the second between port and vlan</td></tr></table>	string	identifier-string, the max character number is 47 bytes	{sp sv pv spv}	This option can select the combination format for slot, port, vlan, sp means slot and port, sv means slot and vlan, pv means port and vlan, spv means slot, port and vlan	WORD	The delimiter between slot, port and vlan, the range is (# . , ; : / space). Note: There are two delimiter WORDs in spv combo mode, the first between slot and port, the second between port and vlan
string	identifier-string, the max character number is 47 bytes						
{sp sv pv spv}	This option can select the combination format for slot, port, vlan, sp means slot and port, sv means slot and vlan, pv means port and vlan, spv means slot, port and vlan						
WORD	The delimiter between slot, port and vlan, the range is (# . , ; : / space). Note: There are two delimiter WORDs in spv combo mode, the first between slot and port, the second between port and vlan						

Default	By default, this configuration is empty.
Mode	Global Mode
Usage Guide	Configure circuit-id of the added vendor tag with tr-101 standard. This command is used to configure global circuit id, the priority is higher than pppoe intermediate-agent access-node-id command. circuit-id value is access-node-id + " eth " + Slot ID + delimiter + Port Index + delimiter + Vlan ID, access-node-id occupies n bytes (n<48), " eth " is space + e + t + h + space, it occupies 5 bytes, Slot ID occupies 2 bytes, Port Index occupies 3 bytes, Vlan ID occupies 4 bytes, delimiter occupies 1 byte. The no command deletes this configuration.
Example	Configure access-node-id as xyz, use spv combination mode, delimiter with "#"between Slot ID and Port ID, delimiter with "/"between Port ID and Vlan ID. <pre>Switch(config)# pppoe intermediate-agent type tr-101 circuit-id 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 : "/" "</pre> After port ethernet1/0/3 of vlan3 receives PPPoE packets, circuit-id value of the added vendor tag is "xyz eth 01#003/0003".

pppoe intermediate-agent vendor-tag strip

Command	[no] pppoe intermediate-agent vendor-tag strip	
Parameter	none	none
Default	By default, disable vendor-tag strip function of the port.	
Mode	Port Configuration Mode	
Usage Guide	Enable vendor-tag strip function of the port. If the received packet includes vendor tag from server to client, strip this vendor tag. Note:	

1. Must enable global pppoe intermediate-agent function.
2. It must be configured on trust port.

The no command cancels this function.

Example

Trust port ethernet1/0/1 enables vendor tag strip function.

```
Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent trust
Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent vendor-tag strip
```

show pppoe intermediate-agent access-node-id

Command

show pppoe intermediate-agent access-node-id

Parameter

none	none

Default

By default,the configuration information is null.

Mode

Admin mode

Usage Guide

This command is used to show access-node-id configured by user.

Example

Show access-node-id configuration information.

```
Switch#show pppoe intermediate-agent access-node-id
pppoe intermediate-agent access-node-id is : abcd
```

show pppoe intermediate-agent identifier-string option delimiter

Command

show pppoe intermediate-agent identifier-string option delimiter

Parameter

none	none

Default

By default,the configuration information is null.

Mode

Admin mode

Usage Guide	Show the configured identifier-string, the combo format and delimiter of slot, port and vlan.
Example	Show the configuration information for pppoe intermediate-agent identifier-string. <pre>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 : "/" "</pre>

show pppoe intermediate-agent info

Command	show pppoe intermediate-agent info [interface ethernet <interface-name>]		
Parameter	<table> <tr> <th>interface-name</th><th>port name</th></tr> </table>	interface-name	port name
interface-name	port name		
Default	By default,the configuration information is null.		
Mode	Admin mode		
Usage Guide	Show the related PPPoE IA configuration information of all ports or the specified port. Check the configuration information of the corresponding port, show whether the port is trust port, strip function is enabled, rate limit is enabled, show the configured circuit ID and remote ID.		
Example	Show pppoe intermediate-agent configuration information of port ethernet1/0/2. <pre>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</pre>		

12 Commands for VLAN-ACL

clear vACL statistic vLAN

Command	clear vACL [in out] statistic vLAN [<1-4094>]

Parameter	in out	Clear the traffic statistic of the ingress/egress
	1-4094	The VLAN which needs to clear the VACL statistic information. If do not input VLAN ID, then clear all VLAN statistic information
Default	None.	
Mode	Admin mode	
Usage Guide	This command can clear the statistic information of VACL.	
Example	Clear VACL statistic information of Vlan1. Switch#clear vACL statistic vlan 1	

show vACL vlan

Command	show vACL [in out] vlan [<1-4094>] [begin include exclude <regular-expression>]	
Parameter	in out	Show ingress/egress configuration and statistic
	1-4094	The VLAN which needs to show the configuration and the statistic information of VACL. If do not input VLAN ID, then show VACL configuration and statistic information of all VLANs.
	begin include exclude <regular-expression>	the regular expression . match any characters except the line feed character ^ match the beginning of the row \$ match the end of the row match the character string at the left or right of upright line [0-9] match the number 0 to the number 9 [a-z] match the lowercase a to z [aeiou] match any letter in "aeiou" \ Escape Character is used to match the intervocalic character, for example, \\$ will match the \$ character, but it is not match the end of the character string \w match the letter, the number or the underline \b match the beginning or the end of the words \W match any characters which are not alphabet letter, number and underline \B match the locations which are not the begin or end of the word [^x] match any characters except x

	[^aeiou] match any characters except including aeiou letters * repeat zero time or many times + repeat one time or many times (n) repeat n times (n,) repeat n or more times (n, m) repeat n to m times At present, the regular expression used does not support the following Commandes: \s match the blank character \d match the number \S match any characters except blank character \D match non-number character ? repeat zero time or one time
Default	None.
Mode	Admin Mode
Usage Guide	This command shows the configuration and the statistic information of VACL.
Example	Show vlan2 VACL statistics. Switch (config)#show vACL vlan 2 Vlan 2: IP Ingress access-list used is 100, traffic-statistics Disable.

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	
Parameter	<1-299> WORD	Configure the numeric IP ACL (include: standard ACL rule <1-99>, extended ACL rule <100-299>) or the named ACL.
	in out	Filter the ingress/egress traffic
	traffic-statistic	Enable the statistic of matched packets number
	vlan WORD	The VLAN will be bound to VACL
Default	None	
Mode	Global Mode	
Usage Guide	This command configure VACL of IP type on the specific VLAN.	

Use “;” or “-” to input the VLAN or multi-VLANs, but do not exceed 128, and CLI length cannot exceed 80 characters. Egress direction filtering is not supported by switch.

The no command unconfigured.

Example

Configure the numeric IP ACL and enable the statistic function for Vlan 1-5,6,7-9.

```
Switch(config)#vacl ip access-group 1 in traffic-statistic vlan 1-5; 6; 7-9
```

vacl ipv6 access-group

Command

```
vacl ipv6 access-group (<500-699> | WORD) {in } (traffic-statistic) vlan WORD  
no ipv6 access-group {<500-699> | WORD} {in } vlan WORD
```

Parameter

<500-699> WORD	Configure the IPv6 numeric standard ACL or IPV6 standard ACL rule.
in out	Filter inlet/ outlet flow
traffic-statistic	Enable the statistic of matched packets number
vlan WORD	The VLAN will be bound to VACL.

Default

None.

Mode

Global Mode

Usage Guide

This command configure VACL of IPv6 on the specific VLAN.
Use “;” or “-” to input the VLAN or multi-VLANs, but do not exceed 128, and CLI length cannot exceed 80 characters. Egress direction filtering and extended IPv6 is not supported by switch.

The no command unconfigured.

Example

Configure the numeric IPv6 ACL for Vlan 5.

```
Switch(config)#vacl ipv6 access-group 600 in traffic-statistic vlan 5
```

vacl mac access-group

Command

```
vacl mac access-group {<700-1199> | WORD} {in } [traffic-statistic] vlan WORD  
no vACL mac access-group {<700-1199> | WORD} {in } vlan WORD
```

Parameter	<700-1199>		Configure the numeric IP ACL (include: <700-799> MAC standard access list, <1100-1199> MAC extended access list) or the named ACL
	WORD		
	in		Filter the ingress traffic
	traffic-statistic		Enable the statistic of matched packets number
	vlan WORD		The VLAN will be bound to VACL
Default	None.		
Mode	Global Mode		
Usage Guide	This command configure VACL of MAC type on the specific VLAN. Use “,” or “-” to input the VLAN or multi-VLANs, but do not exceed 128, and CLI length cannot exceed 80 characters. Egress direction filtering is not supported by switch. The no command unconfigured.		
Example	Configure the numeric MAC ACL for Vlan 1-5 Switch(config)#vACL mac access-group 700 in traffic-statistic vlan 1-5		

vACL mac-ip access-group

Command	vACL mac-ip access-group {<3100-3299> WORD} {in } [traffic-statistic] vlan WORD no vACL mac-ip access-group {<3100-3299> WORD} {in } vlan WORD		
Parameter	<3100-3299>		Configure the numeric MAC-IP ACL or the named ACL
	WORD		
	in		Filter the ingress traffic
	traffic-statistic		Enable the statistic of matched packets number
	vlan WORD		The VLAN will be bound to VACL.
Default	None.		
Mode	Global mode		
Usage Guide	This command configure VACL of MAC-IP type on the specific VLAN. Use “,” or “-” to input the VLAN or multi-VLANs, but do not exceed 128, and CLI length cannot exceed 80 characters. Egress direction filtering is not supported by switch. The no command unconfigured.		

Example

Configure the numeric MAC-IP ACL for Vlan 1, 2, 5.

```
Switch(config)#vACL mac-ip access-group 3100 in traffic-statistic vlan 1;2;5
```

13 Commands for SAVI

ipv6 cps prefix

Command

```
ipv6 cps prefix <ipv6-address> vlan <vid>  
no ipv6 cps prefix<ipv6-address>
```

Parameter

ipv6-address	the address prefix of link, like 2001::/64
vid	vlan ID of the current link

Default

None.

Mode

Global Mode

Usage Guide

Configure IPv6 address prefix of the link manually.
Users should configure local address prefix: fe80::/64 of the link before enable the function of matching address prefix of the link, it accepts the packets of which source addresses are the local addresses of the link.

The no command deletes IPv6 address prefix.

Example

Configure IPv6 address prefix of the link manually is 2001::/64。

```
Switch(config)#ipv6 cps prefix 2001::/64 vlan 20
```

ipv6 cps prefix check enable

Command

```
[no] ipv6 cps prefix check enable
```

Parameter

none	none

Default

By default,disable SAVI address prefix check function.

Mode	Global Mode
Usage Guide	Enable SAVI address prefix check function. After enable the prefix check function, if the IPv6 address prefix of the packets does not accord with the link prefix, then do not establish the corresponding IPv6 address binding. If users enable the matched address prefix of the link, configure the local address prefix of fe80::/64 first to accept the packets with the source address as local link address. Disable address prefix check function by default. The no command will disable this function.
Example	Enable SAVI address prefix check function. Switch(config)#ipv6 cps prefix check enable

ipv6 dhcp snooping trust

Command	[no] ipv6 dhcp snooping trust		
Parameter	<table> <tr> <td>none</td><td>none</td></tr> </table>	none	none
none	none		
Default	By default, this function is disabled.		
Mode	Port Mode		
Usage Guide	Configure the port as dhcpv6 trust port, it does not establish dynamic DHCPv6 binding again and allows all DHCPv6 protocol packets to pass. Set the port as dhcpv6 trust attribute, enable uplink port of the switch with SAVI function for connecting dhcpv6 server or dhcpv6 relay generally. no command deletes the port trust function.		
Example	Set ethernet1/0/1 to be DHCP trust port. Switch(config)#interface ethernet1/0/1 Switch(config-if-ethernet1/0/1)#ipv6 dhcp snooping trust		

ipv6 nd snooping trust

Command	[no] ipv6 nd snooping trust	
Parameter	none	none
Default	By default, this function is disabled.	
Mode	Port Mode	
Usage Guide	Configure the port as slaac trust and RA trust port, this port will not establish dynamic slaac binding anymore and forwards RA packets. If the port disables ipv6 nd snooping trust function, it is considered to untrust RA packets port and discards all RA packets. Setting the port as trust attribute, enable the uplink port of the switch with SAVI or the conjoint port between switches with SAVI generally. The no command deletes the port trust function.	
Example	Set the port ethernet1/0/1 to be nd trust port. <pre>Switch(config)#interface ethernet1/0/1 Switch(config-if-ethernet1/0/1)#ipv6 nd snooping trust</pre>	

savi check binding

Command	savi check binding <simple probe> mode no savi check binding mode	
Parameter	simple	only check the port state for conflict binding, if the state is up,keep the conflict binding and do not set new binding. If the state is down, delete the conflict binding to set a new one
	probe	besides checking the port state for conflict binding, it will send NS packets to probe the usability of the corresponding user when the port state is up. If receiving the responded NA packets from users, it will keep the current conflict binding and does not set new binding, otherwise delete the conflict binding to set new one
Default	Disable the conflict binding check mode by default. It will adopt the mode that delete the conflict binding directly to set new one.	

Mode	Global Mode
Usage Guide	Configure the check mode for conflict binding. It is recommended to configure probe mode to prevent the attack that the spurious address conflict binding deletes the legal user binding. The no command deletes the check mode.
Example	Configure the conflict binding check mode to probe mode. Switch(config)#savi check binding probe mode

savi enable

Command	[no] savi enable		
Parameter	<table> <tr> <td>none</td><td>none</td></tr> </table>	none	none
none	none		
Default	By default,disable the global SAVI function.		
Mode	Global Mode		
Usage Guide	Enable the global SAVI function. Command configuration can be processed for SAVI function after enabling the global SAVI function. Because SAVI function has already contained security RA function, global SAVI function and security RA function are mutually exclusive in the global mode. The no command disables this global function.		
Example	Enable SAVI function. Switch(config)#savi enable		

savi ipv6 binding num

Command	savi ipv6 binding num <limit-num> no savi ipv6 binding num

Parameter	<table border="1"> <tr> <td>limit-num</td><td>set the range from 0 to 100</td></tr> </table>	limit-num	set the range from 0 to 100
limit-num	set the range from 0 to 100		
Default	The default value of the port binding number is 0.		
Mode	Port Mode		
Usage Guide	Configure the number of the corresponding binding with the port. The configured binding number only include the dynamic binding type of slaac, dhcp. If the binding sum exceeds the configured number, this port does not create new dynamic binding any more, if the configured number is 0, this port does not create any dynamic binding. The no command restores the default value.		
Example	Configure the binding number to be 100 for port ethernet1/0/1. <pre>Switch(config)#interface ethernet1/0/1 Switch(config-if-ethernet1/0/1)# savi ipv6 binding num 100</pre>		

savi ipv6 check source binding

Command	<pre>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></pre>												
Parameter	<table border="1"> <tr> <td>ip-address</td><td>the unicast IPv6 address, including local link and global unicast address</td></tr> <tr> <td>mac-address</td><td>the mac address of Ethernet</td></tr> <tr> <td>if-name</td><td>the port name, like interface ethernet 1/0/1</td></tr> <tr> <td>slaac dhcp</td><td>slaac means create the dynamic binding for slaac type, dhcp means create the dynamic binding for dhcp type</td></tr> <tr> <td>lifetime</td><td>configure the lifetime period for the dynamic binding, the unit is second</td></tr> <tr> <td>static</td><td>create the binding of the static type</td></tr> </table>	ip-address	the unicast IPv6 address, including local link and global unicast address	mac-address	the mac address of Ethernet	if-name	the port name, like interface ethernet 1/0/1	slaac dhcp	slaac means create the dynamic binding for slaac type, dhcp means create the dynamic binding for dhcp type	lifetime	configure the lifetime period for the dynamic binding, the unit is second	static	create the binding of the static type
ip-address	the unicast IPv6 address, including local link and global unicast address												
mac-address	the mac address of Ethernet												
if-name	the port name, like interface ethernet 1/0/1												
slaac dhcp	slaac means create the dynamic binding for slaac type, dhcp means create the dynamic binding for dhcp type												
lifetime	configure the lifetime period for the dynamic binding, the unit is second												
static	create the binding of the static type												
Default	None.												
Mode	Global Mode												
Usage Guide	Configure the static or dynamic binding function manually。 After the dynamic binding configured by handwork is overtime, the corresponding binding												

will be deleted but the configuration is still be kept, so the binding still be shown. If the binding needs to take effect again, it should delete it first and configure a new binding again.
When the binding type is static type, do not configure lifetime period, the lifetime period is infinite.

The no command deletes the configured binding.

Example

Configure the dynamic binding of slaac type for SAVI 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 the static binding for SAVI manually.

Switch(config)#savi ipv6 check source binding ip 2001::20 mac 00-25-64-BB-8F-04
Interface ethernet1/0/1 type static

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

Parameter	none	none

Default By default,disable the control filtering function of the port.

Mode Port Mode

Usage Guide Enable the control authentication function for the packets of the port.
The global SAVI function must be enabled before configuring this command.

The no command disables this function.

Example Enable the control filtering function of the packets on port ethernet1/0/1.

Switch(config)#interface ethernet1/0/1
Switch(config-if-ethernet1/0/1)# savi ipv6 check source ip-address mac-address

savi ipv6 {dhcp-only | slaac-only | dhcp-slaac} enable

Command	[no] savi ipv6 {dhcp-only slaac-only dhcp-slaac} enable	
Parameter	dhcp-only	dhcp-only application scene
	slaac-only	slaac-only application scene
	dhcp-slaac	combination application scene of dhcp-only and slaac-only
Default	By default,disable SAVI application scene.	
Mode	Global Mode	
Usage Guide	Enable SAVI application scene function. dhcp-only application scene only detects DHCPv6 packets and DAD NS packets of link-local ipv6 address to be IPv6 address with target field, it does not detect DAD NS packets of non-link-local address. slaac-only application scene detects DAD NS packets of all types. dhcp-slaac combination application scene detects all DHCPv6 and DAD NS packets. Disable all kinds of application scene detection function for SAVI by default. The no command disables the function.	
Example	Enable the specified dhcp-only application scene for SAVI. Switch(config)#savi ipv6 dhcp-only enable	

savi ipv6 mac-binding-limit

Command	savi ipv6 mac-binding-limit <limit-num> no savi ipv6 mac-binding-limit	
Parameter	limit-num	set the ranging from 1 to 10, the default dynamic binding number is 32 for the same MAC address
Default	The default dynamic binding number is 32 for the same MAC address.	
Mode	Global Mode	
Usage Guide	Configure the dynamic binding number of the same MAC address. This command is used to prevent the exhaust attack of the dynamic binding entry for SAVI.	

The no command restores the default value.

Example

Set the dynamic binding number to be 5 for the same MAC address.

```
Switch(config)#savi ipv6 mac-binding-limit 5
```

savi max-dad-dalay

Command

```
savi max-dad-delay <max-dad-delay>  
no savi max-dad-delay
```

Parameter

max-dad-delay	set the ranging between 1 and 65535 seconds, its default value is 1 second

Default

Its default value is 1 second.

Mode

Global Mode

Usage Guide

Configure the dynamic binding at DETECTION state and send lifetime period of DAD NS packet detection.
It is recommended to use the default value.

The no command restores the default value.

Example

Set the detection lifetime as 2 seconds.

```
Switch(config)#savi max-dad-delay 2
```

savi max-dad-prepare-delay

Command

```
savi max-dad-prepare-delay <max-dad-prepare-delay>  
no savi max-dad-prepare-delay
```

Parameter

max-dad-prepare-delay	set the ranging between 1 and 65535 seconds, its default value is 1 second

Default

Its default value is 1 second.

Mode	Global Mode
Usage Guide	Configure lifetime period of redetection for the dynamic binding. It is recommended to user the default value. The no command restores the default value.
Example	Set the redetection lifetime as 2 seconds. Switch(config)#savi max-dad-prepare-delay 2

savi max-slaac-life

Command	savi max-slaac-life <max-slaac-life> no savi max-slaac-life	
Parameter	max-slaac-life	set the ranging between 1 and 31536000 seconds, its default value is 4 hours
Default	Its default value is 4 hours.	
Mode	Global Mode	
Usage Guide	Configure lifetime period of slaac dynamic binding at BOUND state. The no command restores the default value.	
Example	Configure lifetime period of slaac binding type as 2010 seconds at BOUND state. Switch(config)#savi max-slaac-life 2000	

savi timeout bind-protect

Command	savi timeout bind-protect <protect-time> no savi timeout bind-protect

Parameter	protect-time set the ranging between 1 and 300 seconds, its default value is 30 seconds
Default	Its default value is 30 seconds.
Mode	Global Mode
Usage Guide	Configure the bind-protect lifetime period for a port after its state from up to down. After the configured lifetime period is overtime, the port is still at down state, the binding of this port will be deleted. If the port state is changed from down to up state during the configured lifetime period, the binding of the port will reset it as lifetime period of BOUND state. If the configured parameter is 0 second, all binding of the port will be deleted immediately. The no command restores the default value.
Example	Set bind-protect lifetime period to be 20 seconds. <pre>Switch(config)#savi timeout bind-protect 20</pre>

show savi ipv6 check source binding

Command	show savi ipv6 check source binding [interface<if-name>]																				
Parameter	if-name port name such as interface ethernet 1/0/1																				
Default	None.																				
Mode	Admin Mode																				
Usage Guide	Show the global SAVI binding entry list.																				
Example	Show the global binding state of SAVI. Switch(config)#show savi ipv6 check source binding Static binding count: 0 Dynamic binding count: 3 Binding count: 3 <table><thead><tr><th>MAC</th><th>IP</th><th>VLAN</th><th>Port</th><th>Type</th><th>State</th><th>Expires</th></tr></thead><tbody><tr><td colspan="7">-----</td></tr></tbody></table>							MAC	IP	VLAN	Port	Type	State	Expires	-----						
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	1	Ethernet1/0/5	slaac	BOUND	14370	
00-25-64-bb-8f-04	2001::10:1	1	Ethernet1/0/5	slaac	BOUND	14370	

14 Commands for IPSG

ip-source-guard

Command	ip-source-guard (ip ip-mac) interface <interface-name> no ip-source-guard interface <interface-name>						
Parameter	<table> <tr> <td>ip</td><td>Source IP + Port + VLAN filtering</td></tr> <tr> <td>ip-mac</td><td>Source IP + Port + VLAN + Source MAC filtering</td></tr> <tr> <td>interface-name</td><td>Port name</td></tr> </table>	ip	Source IP + Port + VLAN filtering	ip-mac	Source IP + Port + VLAN + Source MAC filtering	interface-name	Port name
ip	Source IP + Port + VLAN filtering						
ip-mac	Source IP + Port + VLAN + Source MAC filtering						
interface-name	Port name						
Default	By default, this function is disabled.						
Mode	Global Mode						
Usage Guide	This command is used to enable the port ip-source-guard function.						
Example	Issue the command to enable IP Source Guard. Switch(config)# ip-source-guard ip-mac interface ethernet 1/0/1						

ip-source-guard max-entry

Command	ip-source-guard max-entry <0 – 50> interface <interface-name> no ip-source-guard max-entry interface <interface-name>				
Parameter	<table> <tr> <td>max-entry</td><td>Maximum value of IP source protection</td></tr> <tr> <td>interface-name</td><td>Port name</td></tr> </table>	max-entry	Maximum value of IP source protection	interface-name	Port name
max-entry	Maximum value of IP source protection				
interface-name	Port name				
Default	By default, the maximum value of IP source protection is 0.				

Mode	Global Mode
Usage Guide	This command is used to set the maximum range for the IP source protection feature of the port ip-source-guard.
Example	Switch(config)# ip-source-guard max-entry 20 interface ethernet 1/0/1

ip-source-guard binding

Command	[no] ip-source-guard binding ((ip-address A.B.C.D) ((ip-address A.B.C.D) (mac-address FF-FF-FF-FF-FF-FF)) (vlan-id <1-4094>) (interface <interface-name>)	
Parameter	ip-address	The IP address bound to the ip-source-guard
	mac-address	The MAC address bound to the ip-source-guard
	vlan-id	The VLAN information bound by ip-source-guard
	interface-name	Port name
Default	-	
Mode	Global Mode	
Usage Guide	This command is used for the static table entries of the port ip-source-guard function.	
Example	Issue the static entry of ip-source-guard. Switch(config)# ip-source-guard binding ip-address 1.1.1.1 interface ethernet 1/0/1	

clear ip-source-guard binding

Command	clear ip-source-guard binding (static (vlan <1-4094> interface <interface-name> ip-address A.B.C.D) dynamic (vlan <1-4094> interface <interface-name> ip-address A.B.C.D) all)	
Parameter	static	Static entry
	dynamic	Dynamic entry
	ip-address	The IP address bound to the ip-source-guard
	mac-address	The MAC address bound to the ip-source-guard
	vlan-id	The VLAN information bound by ip-source-guard
	interface-name	Port name
	all	All items

Default	–
Mode	Global Mode
Usage Guide	This command is used to clear the ip-source-guard table entries for the port.
Example	Clear all ip-source-guard table entries. Switch(config)# clear ip-source-guard binding all

show ip-source-guard

Command	show ip-source-guard interface <interface-name>				
Parameter	interface-name	Port name			
Default	-				
Mode	Global Mode				
Usage Guide	This command is used to display the ip-source-guard table entries under the interface.				
Example	Display the ip-source-guard table entries under the display interface.				
	Switch(config)# show ip-source-guard interface ethernet 1/0/1				
	Interface	Vlan ID	IP address	MAC	USED
	Ethernet1/0/1		1.1.1.1	00-00-12-11-22-33	enable

show ip-source-guard binding

Command	show ip-source-guard interface (static dynamic)	
Parameter	static	Static entry
	dynamic	Dynamic entry
Default	-	
Mode	Global Mode	
Usage Guide	This command is used to display the ip-source-guard table entries under the interface.	

Example

Display the static ip-source-guard table entries.**Switch(config)# show ip-source-guard binding static**

Interface	Vlan ID	IP address	MAC	USED
Ethernet1/0/1		1.1.1.1	00-00-12-11-22-33	enable
Ethernet1/0/2		2.2.2.2	00-00-11-22-22-11	enable

11-Commands for Reliability

1 Commands for MRPP

control-vlan

Command	control-vlan <vid> no control-vlan	
parameter	vid	expresses control VLAN ID, the valid range is from 1 to 4094
default	-	
Mode	MRPP ring mode	
Usage Guide	The command specifies Virtual VLAN ID of MRPP ring, currently it can be any value in 1-4094. To avoid confusion, it is recommended that the ID is non-configured VLAN ID, and the same to MRPP ring ID. In configuration of MRPP ring of the same MRPP loop switches, the control VLAN ID must be the same, otherwise the whole MRPP loop may not be able to work normally or form broadcast. The mrpp enable command must be start before the control-vlan command be used. If primary port, secondary port, node-mode and enable commands all be configured after control-vlan, the mrpp-ring function is enabled.	
Example	Configure control VLAN of mrpp ring 4000 is 4000. <pre>Switch(config)#mrpp ring 4000 Switch(mrpp-ring-4000)#control-vlan 4000</pre>	

clear mrpp statistics

Command	clear mrpp statistics [<ring-id>]	
parameter	ring-id	is MRPP ring ID, the valid range is from 1 to 4096, if not specified ID, it clears all of MRPP ring statistic information.
default	-	
Mode	Admin Mode.	
Usage Guide	Clears statistics for MRPP packets received and transmitted by the MRPP loop.	
Example	Clear switch MRP P ring 4000 statistics. <pre>Switch#clear mrpp statistics 4000</pre>	

enable

Command	enable no enable
parameter	-
default	Default disable MRPP ring
Mode	MRPP ring mode
Usage Guide	This command is used to enable the configured MRPP ring , "no enable" command disables this enabled MRPP ring.

Example	Configure MRPP ring 4000 of switch to primary node, and enable the MRPP 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

errp domain

Command	errp domain <domain-id> no errp domain <domain-id>
parameter	domain-id domain ID of ERRP, the range between 1 and 15.
default	Default Unconfigured ID
Mode	Global mode
Usage Guide	If domain ID of ERRP needs to be configured, the compatible mode of ERRP should be enabled firstly. When executing this command, it should create a new

ERRP domain if there is no ERRP domain. However, the no command is used to delete the corresponding domain ID of ERRP.

Example

Configure domain ID for ERRP globally.
Switch(Config)#errp domain 1

fail-timer

Command **fail-timer <timer>**
 no fail-timer

parameter *timer* valid range is from 3 to 300s.

default Default configure timer interval 3s

Mode MRPP ring mode

Usage Guide If primary node of MRPP ring doesn't receives Hello packet from primary port of primary node on configured fail timer, the whole loop is fail. Transfer node of MRPP doesn't need this timer and configure. To avoid time delay by transfer node forwards Hello packet, the value of fail timer must be more than or equal to 3 times of Hello timer. On time delay loop, it needs to modify the default and increase the value to avoid primary node doesn't receive Hello packet on fail timer due to time delay.

Example

Configure fail timer of MRPP ring 4000 to 10s.
Switch(config)# mrpp ring 4000
Switch(mrpp-ring-4000)#fail-timer 10

hello-timer

Command **hello-timer <timer>**
 no hello-timer

parameter *timer* valid range is from 1 to 100s.

default Default configuration timer interval is 1s.

Mode MRPP ring mode

Usage Guide	The primary node of MRPP ring continuously sends Hello packet on configured Hello timer interval, if secondary port of primary node can receive this packet in configured period; the whole loop is normal, otherwise fail. Transfer node of MRPP ring doesn't need this timer and configure.

Example	Configure hello-timer of MRPP ring 4000 to 3 seconds. Switch(config)# mrpp ring 4000 Switch(mrpp-ring-4000)#hello-timer 3

mrpp eaps compatible

Command	mrpp eaps compatible no mrpp eaps compatible
parameter	-
default	Disable the compatible function of EAPS
Mode	Global mode
Usage Guide	If the compatible function of EAPS needs to be configured, MRPP protocol should be enabled firstly. When executing no mrpp eaps compatible command, it should ensure that the switch has enabled MRPP protocol.

Example	Enable the compatible function of EAPS globally Switch(Config)#mrpp enable Switch(Config)#mrpp eaps compatible

mrpp enable

Command	mrpp enable no mrpp enable
parameter	-
default	The system doesn't enable MRPP protocol module
Mode	Global Mode
Usage Guide	If it needs to configure MRPP ring, it enables MRPP protocol. Executing "no mrpp enable" command, it ensures to disable the switch enabled MRPP ring.

Example	Globally enable MRPP.

Switch(config)#mrpp enable

mrpp errp compatible

Command	mrpp errp compatible no mrpp errp compatible
parameter	-
default	Disable the compatible function of ERRP.
Mode	Global mode
Usage Guide	If the compatible function of ERRP needs to be configured, MRPP protocol should be enabled firstly. Furthermore, the port with ERRP compatible mode should be configured as hybrid or trunk mode and allow the packets with Control Vlan information.

Example

Enable the compatible function of ERRP 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-ethernet1/51)#switchport mode hybrid
Switch(config-if-ethernet1/51)#switchport hybrid allowed vlan 4000 tag
Switch(config-if-ethernet1/52)#switchport mode hybrid
Switch(config-if-ethernet1/52)#switchport hybrid allowed vlan 4000 tag
```

mrpp poll-time

Command	mrpp poll-time <20-2000>
parameter	<20-2000> Enquiry Time, Unit: ms
default	Default configuration ms 100
Mode	Global mode.
Usage Guide	Configure the query time to adjust the query interval of MRPP, the default interval is 100ms.

Example

Set the query time as 200ms.

Switch(Config)# mrpp poll-time 200

mrpp ring

Command	mrpp ring <ring-id> no mrpp ring <ring-id>	
parameter	ring-id	is MRPP ring ID, the valid range is from 1 to 4096
default	Default does not configure ring id	
Mode	Global mode	
Usage Guide	If this MRPP ring doesn't exist it create new MRPP ring when executing the command, and then it enter MRPP ring mode. It needs to ensure disable this MRPP ring when executing the "no mrpp ring" command.	
Example	Create a mrpp ring 100. Switch(config)#mrpp ring 100	

mrpp ring primary-port

Command	mrpp ring <ring-id> primary-port {cos <cos> } no mrpp ring <ring-id> primary-port	
parameter	ring-id	is the ID of MRPP ring; range is <1-4096>.
	cos <cos>	is the cos value in the packet head; range is <0-7>
default	There is no configuration and the cos value is 0 as default.	
Mode	Port mode	
Usage Guide	The command specifies MRPP ring primary port. Primary node uses primary port to send Hello packet, secondary port is used to receive Hello packet from primary node. There are no difference on function between primary port and secondary of secondary node.	
Example	Configure the primary 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
```

mrpp ring secondary-port

Command **mrpp ring < ring-id > secondary-port {cos <cos>|}**
no mrpp ring < ring-id > secondary-port

parameter	ring-id	is the ID of MRPP ring; range is <1-4096>.
	cos <cos>	is the cos value in the packet head; range is <0-7>.

default There is no configuration and the cos value is 0 as default

Mode Port mode

Usage Guide The command specifies secondary port of MRPP ring. The primary node uses secondary port to receive Hello packet from primary node. There are no difference on function between primary port and secondary of secondary node.
The mrpp enable command must be enabled before the control-vlan command be used. If primary port, secondary port, node-mode and enable commands all be configured after control-vlan, then the mrpp-ring function is enabled.

Example Configure secondary port of MRPP ring to 1/0/3.
Switch(config)#interface ethernet1/0/3
Switch(Config-If-Ethernet1/0/3)#mrpp ring 4000 secondary-port

node-mode

Command **node-mode {maser | transit}**

parameter -
default Default the node mode is secondary node.

Mode MRPP ring mode

Usage Guide This command configures the node type as the primary or secondary node.

Example Configure the switch to primary node. MRPP ring 4000.
Switch(config)# mrpp ring 4000

Switch(mrpp-ring-4000)#node-mode master

show mrpp

Command	show mrpp [<ring-id>]	
parameter	<i>ring-id</i>	is MRPP ring ID, the valid range is from 1 to 4096, if not specified ID, it display all of MRPP ring configuration.
default	-	
Mode	Admin and Configuration Mode	
Usage Guide	This command is used to view the MRPP ring configuration.	
Example	Display configuration of MRPP ring 4000 of switch Switch# show mrpp 4000	

show mrpp statistics

Command	show mrpp statistics [<ring-id>]	
parameter	<i>ring-id</i>	is MRPP ring ID, the valid range is from 1 to 4096, if not specified ID, it displays all of MRPP ring statistic information.
default	-	
Mode	Admin and Configuration Mode.	
Usage Guide	This command is used to display the statistics of the MRPP loop receiving and transmitting packets.	
Example	Display statistic information of MRPP ring 4000 of switch. Switch# show mrpp statistic 4000	

2 Commands for ULPP

clear ulpp flush counter interface

Command	clear ulpp flush counter interface <i><name></i>	
parameter	<i>name</i>	is the name of the port
default	-	
Mode	Admin mode	
Usage Guide	Clear the statistics of the packets.	
Example	Clear the statistic information of the flush packets for the port1/0/1 Switch#clear ulpp flush counter interface e1/0/1	

control vlan

Command	control vlan <i><integer></i> no control vlan	
parameter	<i>integer</i>	is the control VLAN ID that sends the flush packets, range from 1 to 4094.
default	The default is VLAN 1	
Mode	ULPP group configuration mode.	
Usage Guide	Configure the control VLAN of ULPP group. This VLAN must correspond the existent VLAN, after it is configured, this VLAN can't be deleted. It must belong to the VLAN protected by ULPP group to avoid flush packets loopback.	
Example	Configure the sending control VLAN of ULPP group as 10. Switch(config)# ulpp group 20 Switch(ulpp-group-20)# control vlan 10	

description

Command	description <i><string></i> no description	

parameter	<i>string</i>	is the name of ULPP group, the max number of the characters is 128.
default	Do not configure ULPP name by default.	
Mode	ULPP group configuration mode.	
Usage Guide	Configure the description string for the ULPP group. Delete description no command.	
Example	Configure the description of ULPP group as switch. Switch(config)# ulpp group 20 Switch(ulpp-group-20)# description switch	

flush {enable | disable} arp

Command	flush {enable disable} arp	
parameter	-	
default	By default, enable the sending function of the flush packets which are deleted by ARP.	
Mode	ULPP group configuration mode.	
Usage Guide	If configure this command, when the link is switched, it will not actively send the flush packets to notify the upstream device to delete the entries of ARP.	
Example	Disable sending the flush packets of deleting ARP. Switch(config)# ulpp group 20 Switch(ulpp-group-20)# flush disable arp	

flush {enable | disable} mac

Command	flush {enable disable}mac	
parameter	-	
default	By default, enable sending the flush packets of updating MAC address.	
Mode	ULPP group configuration mode.	
Usage Guide	If configure this command, when the link is switched, it will not actively send the flush packets to notify the upstream device to update the MAC address table.	
Example	Disable sending the flush packets of updating MAC address.	

```
Switch(config)# ulpp group 20
Switch(ulpp-group-20)# flush disable mac
```

flush {enable | disable} mac-vlan

Command	flush {enable disable}mac-vlan
parameter	-
default	Disable.
Mode	ULPP group configuration mode
Usage Guide	If configure this command, when the link is switched, it will not actively send the flush packets to notify the upstream device to delete the dynamic unicast mac according to vlan.
Example	Disable sending the flush packets deleted by mac-vlan. Switch(config)#ulpp group 1 Switch(ulpp-group-1)#flush disable mac-vlan

preemption delay

Command	preemption delay <integer> no preemption delay
parameter	<i>integer</i> the preemption delay, range from 1 to 600, in second.
default	The default preemption delay is 30.
Mode	ULPP group configuration mode.
Usage Guide	The preemption delay is the delay time before the master port is preempted as the forwarding state, for avoiding the link oscillation in a short time. After the preemption mode is enabled, the preemption delay takes effect.
Example	Configure the preemption delay as 50s for ULPP group. Switch(config)# ulpp group 20 Switch(ulpp-group-20)# preemption delay 50

preemption mode

Command	preemption mode no preemption mode
parameter	-
default	Do not preempt.
Mode	ULPP group configuration mode.
Usage Guide	If the preemption mode configured by ULPP group, and the slave port is in forwarding state, and the master port is in the standby state, the master port will turn into the forwarding state and the slave port turn into the standby state after the preemption delay.
Example	Configure the preemption mode of ULPP group. Switch(config)# ulpp group 20 Switch(ulpp-group-20)# preemption mode

protect vlan-reference-instance

Command	protect vlan-reference-instance <instance-list> no protect vlan-reference-instance <instance-list>
parameter	<i>instance-list</i> is MSTP instance list, such as: i; j-k. The number of the instances is not limited in the list.
default	Do not protect any VLANs by default that means any instances are not quoted.
Mode	ULPP group configuration mode.
Usage Guide	Quote the instances of MSTP to protect the VLANs. The VLAN corresponds to this instance is at the forwarding state on one port of this group, and at the blocked state on another port of this group. Each ULPP group can quotes all instances of MSTP. And it can quotes the inexistent MSTP instances that means any VLANs are not protected, the different ULPP groups can't quote the same instance.
Example	Configure the protective VLAN quoted from instance 1 for ULPP group. Switch(config)# ulpp group 20 Switch(ulpp-group-20)# protect vlan-reference-instance 1

show ulpp flush counter interface

Command	show ulpp flush counter interface {ethernet <IFNAME> <IFNAME>}	
parameter	IFNAME	is the name of the ports.
default	-	
Mode	Admin mode.	
Usage Guide	Show the statistic information of the flush packets, such as: the information of the flush packets number which has been received, the time information that receive the flush packets finally.	
Example	Show the statistic information of the flush packets for ULPP group1. Switch# show ulpp flush counter interface e1/0/1 Received flush packets: 10	

show ulpp flush-receive-port

Command	show ulpp flush-receive-port	
parameter	-	
default	-	
Mode	Admin mode.	
Usage Guide	displays the port that receives the flush packet, flush type, and control VLAN.	
Example	Show the information that the port receives 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	

show ulpp group

Command	show ulpp group [group-id]	
parameter	group-id	Show the information of the specific ULPP group
default	By default, show the information of all ULPP groups which have been configured	

Mode	Admin mode.
Usage Guide	Show the configuration information of ULPP groups which have been configured, such as: the state of the master port and the slave port, the preemption mode, the preemption delay, etc.
Example	Show the configuration information of ULPP group1. <pre>Switch# show ulpp group 1 ULPP flush-receive portlist: Portname Type Control Vlan ----- ----- Switch#show ulpp group 20 ULPP group 20 information: Description: switch Preemption mode: ON Preemption delay: 50s Control VLAN: 10 Flush packet: NONE Protected VLAN: Reference Instance 1 Member Role State Track-cfm-level ----- -----</pre>

ulpp control vlan

Command	ulpp control vlan <vlan-list> no ulpp control vlan <vlan-list>	
parameter	vlan-list	specify the control VLAN list that receives the flush packets, such as: i; j-k. The number of VLANs in Each character string cannot exceed 100. The receiving control VLAN of the port can be added.
default	The default is VLAN 1.	
Mode	Port mode	
Usage Guide	Configure the receiving control VLAN for the port. This VLAN must correspond the existent VLAN, after it is configured, this VLAN can't be deleted.	
Example	Configure the receiving control VLAN as 10 <pre>Switch(config)# interface ethernet 1/0/1</pre>	

```
Switch(config-If-Ethernet1/0/1)# ulpp control vlan 10
```

ulpp flush {enable | disable} arp

Command	ulpp flush {[enable disable]} arp
parameter	-
default	By default, disable receiving the flush packets of deleting ARP
Mode	Port mode.
Usage Guide	If this command is configured, then it will not receive the flush packets of deleting ARP.
Example	Disable receiving the flush packets of deleting ARP. Switch(config)# interface ethernet 1/0/1 Switch(config-If-Ethernet1/0/1)# ulpp flush disable arp

ulpp flush {enable | disable} mac

Command	ulpp flush {enable disable} mac
parameter	-
default	By default, disable receiving the flush packets of updating MAC address.
Mode	Port mode.
Usage Guide	If this command is configured, then it will not receive the flush packets of updating MAC address.
Example	Disable receiving the flush packets of updating MAC address. Switch(config)# interface ethernet 1/0/1 Switch(config-If-Ethernet1/0/1)# ulpp flush disable mac

ulpp flush {enable | disable} mac-vlan

Command	ulpp flush {enable disable} mac-vlan
parameter	-
default	Disable
Mode	Port mode.

Usage Guide	If enabling this function, forward the hardware of the flush packets with mac-vlan type received in port. It will not be analyzed.
Example	Disable receiving the flush packets deleted by mac-vlan of port. Switch(config)#interface e1/0/2 Switch(config-if-ethernet1/0/2)#ulpp flush disable mac-vlan

ulpp group

Command	ulpp group <integer> no ulpp group <integer>
parameter	<i>integer</i> is the ID of ULPP group, range from 1 to 48.
default	Any ULPP groups are not configured.
Mode	Global Mode.
Usage Guide	Create a ULPP group. If the group exists, enter the configuration mode of the ULPP group. no command delete ULPP group.
Example	Configure ulpp group 20 or enter the mode of ulpp group 20. Switch(config)# ulpp group 20 Switch(ulpp-group-20)#

ulpp group {master|slave}

Command	ulpp group <integer> {master slave} no ulpp group <integer> {master slave}
parameter	<i>integer</i> is the ID of ULPP group, range from 1 to 48.
default	There is no master port configured by default.
Mode	Port mode

Usage Guide

There is no sequence requirement for the master and slave port configuration in a group, but the protective VLANs must be configured before the member ports. Each group has only one master port, if the master port exists, then the configuration fail.

Example

Configure the master port of ULPP group.
Switch(config)# interface ethernet 1/0/2
Switch(config-if-Ethernet1/0/2)# ulpp group 20 slave

3 Commands for ULSM

show ulsm group

Command

show ulsm group [group-id]

parameter

group-id	ULSM group ID range:<1-32>

default

By default, show the information of all ULSM groups which have been configured

Mode

Admin Mode

Usage Guide

This command is used to display configuration information for ULSM groups.

Example

Show the configuration information of ULSM group1.
Switch# show ulsm group 1

ulsm group

Command

ulsm group <group-id>
no ulsm group <group-id>

parameter

group-id	is the ID of ULSM group, range from 1 to 32.

default

There is no ULSM group configured by default.

Mode

Global Mode.

Usage Guide

This command is used to create a ULSM group. no command delete ULSM group.

Example

Create ULSM group 10.

Switch(config)# ulsm group 10

ulsm group {uplink | downlink}

Command **ulsm group <group-id> {uplink | downlink}**
no ulsm group <group-id>

parameter	group-id	The ID of ULSM group, the range from 1 to 32.
	uplink	Configure the port as the uplink port
	downlink	Configure the port as the downlink port.

default The port does not belong to any ULSM group

Mode Port Mode

Usage Guide Configure the uplink/downlink ports of ULSM group. Each ULSM group can configure 8 uplink ports and 16 downlink ports at most.

Example Configure port1/0/3 as the uplink port of ULSM group10.
Switch(config)# interface ethernet 1/0/3
Switch(config-If-Ethernet1/0/3)# ulsm group 10 uplink

4 Commands for NQA

nqa agent enable

Command **nqa agent enable**
nqa agent disable

parameter	-

default By default, the NQA client function module is not enabled.

Mode Global Mode

Usage Guide Only after enabling the NQA client function can the relevant configuration of the NQA client be permitted.

Example Enable NQA client
Switch(config)#nqa agent enable

Nqa agent start.
Switch(config)#

nqa server instance enable

Command **nqa server instance <1-10> enable**
 nqa server instance <1-10> disable

parameter	<1-10>	Server instance configuration range: 1 - 10

default The NQA server function module is not enabled by default.

Mode Global Mode

Usage Guide Only after enabling the NQA server function will the relevant configuration of the NQA server take effect.
As a server, NQA only activates the NQA-TCP and NQA-UDP functions.
Before configuring the enable command, please ensure that the server instance command has been configured first.

Example Enable the NQA server
Switch(config)#nqa server instance 1 enable
Switch(config)#

nqa server instance

Command **nqa server instance <1-10> (tcp-private-connect | tcp-public-connect | udp-private-echo | udp-public-echo) A.B.C.D (<1024-65535> |)**

parameter	<1-10>	Server instance configuration range: 1 - 10
	tcp-private-connect	The equipment is used to test the TCP protocol on the specified port of the server.
	tcp-public-connect	The equipment is used to test the TCP protocol for the server without specifying the port.
	udp-private-echo	The equipment is used to test the UDP protocol on the specified port of the server.
	udp-public-echo	The equipment is used to test the UDP protocol for the server without specifying the port.
	A.B.C.D	The available IP address of the equipment as the accessible IP

	address for the NQA server (not supporting IPv6)
<1024-65535>	Tcp\Udp test, specified port range is <1024 - 65535>

default	The default TCP public-connect and UDP public-echo ports are set to 512.
Mode	Global Mode
Usage Guide	Configure instance ID (1-10); The IP address must be the IP address of the device management port/virtual interface. Only the private test supports specifying the port number; the configuration range is <1024 - 65535>; Public testing cannot enable multiple at the same time. The default port will be preempted.

Example	Configure the NQA server instance Switch(config)#nqa server instance 1 tcp-private-connect 1.1.1.1 20000 Switch(config)#

nqa entry domain tag

Command	nqa entry domain tag no nqa entry domain tag	
parameter	domain tag	admin-name <1-32> character operation-tag
default	-	
Mode	Global Mode	
Usage Guide	Configure the NQA client instance, where the instance is determined jointly by the domain and the tag.	
Example	Configure the NQA client instance. Switch(config)#nqa entry 1 1 Nqa group name:1 tag:1 add. Switch(nqa-1-1)#	

type

Command	type (dhcp ftp http icmp snmp tcp-private tcp-public udp-private udp-public)	
parameter AA	dhcp	dhcp type
	ftp	ftp type
	http	http type
	icmp	icmp type
	snmp	snmp type
	tcp-private	tp-private type
	tcp-public	tcp-public type
	udp-private	udp-private type
	udp-public	udp-public type
default	-	
Mode	nqa group mode	
Usage Guide	Configure the NQA client instance and select the test type.	
Example	Configure the test type for the NQA client. Switch(nqa-1-1)#type ftp Switch(nqa-type-ftp)#	

community read WORD

Command	community read WORD	
parameter	WORD	community-name
default	-	
Mode	nqa type mode	
Usage Guide	Configure the NQA-SNMP test parameter. The community name must match the one configured on the opposite end.	
Example	Configure the SNMP test type group name for the NQA client. Switch(nqa-type-snmp)#community read public Switch(nqa-type-snmp)#	

destination IP

Command	destination IP <ip-address>	
parameter	IP	NQA test group destination ip
	<ip-address>	A.B.C.D server IP address
default	-	
Mode	nqa type mode	
Usage Guide	Configure the NQA test parameters and the destination IP. To ensure the normal operation of the test, please ensure that the IP is reachable.	
Example	Configure the destination IP of the NQA client. Switch(nqa-type-snmp)#destination ip 1.1.1.1 Switch(nqa-type-snmp)#	

destination port

Command	destination port <1-65535>	
parameter	<1-65535>	The selectable range of communication ports is <1 - 65535>
default	The tcp\udp-public test is set to 512. In "tcp\udp-private", it is specified by the user. For the rest, this configuration does not take effect.	
Mode	nqa type mode	
Usage Guide	Configure the NQA test parameters and destination port. To ensure the normal operation of the test, please make sure that the port number is not occupied by other functions.	
Example	Configure the destination port for the NQA client. Switch(nqa-type-tcp-private)#destination port 6666 Switch(nqa-type-tcp-private)#	

filename

Command	filename WORD	
parameter	WORD	filename <1-128>
default	-	
Mode	nqa type mode	
Usage Guide	Configure the NQA-ftp test parameter, and the file used for the FTP test.	
Example	Configure the file name of the NQA client. Switch(nqa-type-ftp)#filename AAA.cfg Switch(nqa-type-ftp)#	

ftp-operation

Command	ftp-operation (get put)	
parameter	get put	download upload
default	get	
Mode	nqa type mode	
Usage Guide	Configure NQA-ftp test parameters, specifying the direction of FTP file transfer.	
Example	Configure the file transfer direction of the NQA client Switch(nqa-type-ftp)#ftp-operation get Switch(nqa-type-ftp)#	

ftp-password (cipher | simple)

Command	ftp-password (cipher simple) WORD	
parameter	cipher	encrypted password

simple	simple password
WORD	password string

default	simple
Mode	nqa type mode
Usage Guide	Configure the NQA-ftp test parameter and the password for the FTP server.
Example	Configure the NQA client and the FTP server password Switch(nqa-type-ftp)#ftp-password simple 12345678 Switch(nqa-type-ftp)#

ftp-username

Command	ftp-username WORD	
parameter	WORD	the name of ftp
default	-	
Mode	nqa type mode	
Usage Guide	Configure the NQA-ftp test parameters and the FTP server account.	
Example	Configure the FTP server account for the NQA client Switch(nqa-type-ftp)#ftp-username admin Switch(nqa-type-ftp)#	

mode

Command	mode (active passive)	
parameter	active	active mode
	passive	passive mode
default	active	
Mode	nqa type mode	

Usage Guide	Configure the NQA-ftp test parameter and select the HTTP test transmission mode.
Example	Configure the NQA client and select the HTTP testing transmission method Switch(nqa-type-ftp)#mode active Switch(nqa-type-ftp)#

http-operation

Command	http-operation (get post raw)	
parameter	get	get of HTTP operation
	post	post of HTTP operation
default	get	
Mode	nqa type mode	
Usage Guide	Configure the NQA-http test parameter and specify the transmission direction for the HTTP test.	
Example	Configure the NQA client and specify the transmission direction for the HTTP test. Switch(nqa-type-http)#http-operation get Switch(nqa-type-http)#	

out interface vlan

Command	out interface vlan WORD	
parameter	WORD	Vlan ID <1-4094>
default	-	
Mode	nqa type mode	
Usage Guide	Configure the NQA-dhcp test parameter and select the virtual interface VLAN.	
Example	Configure the NQA client, with the DHCP virtual interface set to VLAN 1 Switch(nqa-type-dhcp)#out interface vlan 1 Switch(nqa-type-dhcp)#	

source IP

Command	Source IP <ip address>	
parameter	IP	NQA test group source ip
	<ip address>	A.B.C.D, aClient IP address
default	-	
Mode	nqa type mode	
Usage Guide	Configure NQA test parameters, source IP. This configuration is a mandatory option in the ftp\tcp-public\tcp-private tests.	
Example	Configure the source IP of the NQA client Switch(nqa-type-tcp-private)#source ip 2.2.2.2	

source port

Command	source port <1-65535>	
parameter	<1-65535>	The selectable range of communication ports is <1 - 65535>
default	The tcp\udp-public test is set to 512. In "tcp\udp-private", it is specified by the user. For the rest, this configuration does not take effect.	
Mode	nqa type mode	
Usage Guide	Configure the NQA test parameters and source port. To ensure the normal operation of the test, please make sure that the port number is not occupied by other functions.	
Example	Configure the source port of the NQA client Switch(nqa-type-tcp-private)#source port 6666 Switch(nqa-type-tcp-private)#	

version

Command	version v1dot (1 0)	
parameter	0	v1.0 of http version
	1	v1.1 of http version
default	-	
Mode	nqa type mode	
Usage Guide	Configure the NQA test parameters, and specify the HTTP version for the HTTP test.	
Example	Configure the NQA client to specify the version Switch(nqa-type-http)#version v1dot 0 Switch(nqa-type-http)#	

test

Command	test (dhcp ftp http icmp snmp tcp-private tcp-public udp-private udp-public) no test (dhcp ftp http icmp snmp tcp-private tcp-public udp-private udp-private)	
parameter	dhcp	dhcp test
	ftp	ftp test
	http	http test
	icmp	icmp test
	snmp	snmp test
	tcp-private	tp-private test
	tcp-public	tcp-public test
	udp-private	udp-private test
	udp- public	udp-public test
default	-	
Mode	nqa type mode	
Usage Guide	Configure the NQA test parameters and start/stop a specific test.	
Example	Configure the NQA client and start the test. Switch(nqa-type-snmp)#test snmp Switch(nqa-type-snmp)#	

```

***** begin test :1/5 *****

NQA-SNMP test 1/5 successful!

***** begin test :2/5 *****

NQA-SNMP test 2/5 successful!

***** begin test :3/5 *****

NQA-SNMP test 3/5 successful!

***** begin test :4/5 *****

NQA-SNMP test 4/5 successful!

***** begin test :5/5 *****

NQA-SNMP test 5/5 successful!
NQA test 5 times! Test finish.

```

show nqa result

Command	show nqa result <WORD> <WORD1>	
parameter	<WORD>	test grout name
	<WORD1>	operation tag
default	-	
Mode	Admin Mode	
Usage Guide	Configure the NQA test parameters and view the results of one round of the NQA test.	
Example	Configure the NQA client settings Switch(nqa-type-snmp)#show nqa result 1 1 NQA contains a group with the same name as adminname:1,opertag:1 NQA entry (1 1) test results: Send operation times: 5 Receive response times:0 Min/Max/Average round trip time: 0/0/0 Square-Sum of round trip time: 0	

Last succeeded probe time:
Extended results:
Packet loss ratio: 100.00%
Failures due to timeout: 0
Failures due to internal error: 0
Failures due to other errors: 0
Switch(nqa-type-snmp)#

12-Commands for Mirroring Configuration

1 Commands for Mirroring Configuration

monitor session source interface

Command	monitor session <session> source {interface <interface-list> / cpu} [member <member id>] {rx tx both} no monitor session <session> source {interface <interface-list> / cpu}	
parameter	<i>session</i>	<1-7> SPAN session numberList
	<i>interface-list</i>	is the list of source interfaces of the mirror which can be separated by "-" and ",".
	<i>cpu</i>	means the CPU on the board to be the source of the mirror for debugging. Datagram received by or sent by the CPU
	< member id>	<1-8> Member ID <1-8>
	<i>rx</i>	means to filter the datagram received by the interface
	<i>tx</i>	for the datagram sent out
	<i>both</i>	means both of income and outcome datagram
default	Default does not match any mirror source port	
Mode	Global mode	
Usage Guide	This command is used to configure the source interfaces for the mirror. It is not restricted the source interface of the mirror on the switch. The source can be one interface, or can be multiple interfaces. Both of the income and outcome datagram can be mirrored, or they can be mirrored selectively. If no [rx tx both] is specified, both are made to be the default. When multiple interfaces are mirrored, the direction of the mirror can be different, but they should be configured separately.	
Example	Configure to mirror the datagram sent out by interface 1/0/1-4 and to mirror the datagram received by interface1/0/5。 Switch(config)#monitor session 1 source interface ethernet 1/0/1-4 tx Switch(config)#monitor session 1 source interface ethernet1/0/5 rx	

monitor session source interface access-list

Command	monitor session <session> source {interface <interface-list>} access-list <num> [<rx>]

no monitor session *<session>* source {interface *<interface-list>*} access-list *<num>*

parameter	<i>session</i>	is the session number for the mirror. Currently only 1 is supported
	<i>interface-list</i>	is the list of source interfaces of the mirror which can be separated by '-' and ';'
	<i>num</i>	is the number of the access list
	rx	means to filter the datagram received by the interface

default Default not configured

Mode Global Mode

Usage Guide This command is used to configure the source interfaces for the mirror. It is not restricted the source interface of the mirror on the switch. The source can be one interface, or can be multiple interfaces. For flow mirror, only datagram received can be mirrored. The parameters can be rx, tx, both. The related access list should be prepared before this command is issued. For how to configure the access list, please refer to ACL configuration. The mirror can only be created after the destination interface of the corresponding session has been configured. In the moment, the command only IP ACL and MAC ACL

Example Configure the mirror interface 1/0/6 to filter with access list 120 in session 1.
Switch(config)#monitor session 1 source interface 1/0/6 access-list 120 rx

monitor session destination interface

Command **monitor session** *<session>* destination interface [ethernet] *<interface-number>*
no monitor session *<session>* destination interface [ethernet] *<interface-number>*

parameter	<i>session</i>	is the session number of the mirror, which is currently limited to 1-7
	<i>interface-number</i>	Interface name or number

default Default does not match mirror destination port

Mode Global mode

Usage Guide Only four destination mirror interface is supported on the switch. To be mentioned. The interface which is configured as the destination of the mirror should not be configured as the member of the interface trunk. And the maximum throughput of the interface is recommended to be larger than the total throughput of the interfaces to be mirrored. If the destination is removed, the mirror path configured will be removed

at the same time. And if the destination interface is reconfigured, the interface, CPU mirror path will be recovered. To be mentioned, the flow mirror can only be recovered after the destination of the interface is re-configured.

Example

Configure interface 1/0/7 as the destination of the mirror.
Switch(config)#monitor session 1 destination interface ethernet 1/0/7

show monitor

Command	show monitor

parameter	-

default	-

Mode	Admin Mode

Usage Guide	This command is used to display the source and destination ports for the configured mirror sessions. For port mirroring, CPU mirroring, and flow mirroring, the mirror mode of the source can be displayed.

Example

View configuration information for the current image.
Switch#show monitor

2 Commands for sFlow

sflow agent-address

Command	sflow agent-address [<ip-address> ipv6 <ipv6-address>] no sflow agent-address [ipv6]

parameter	<ip-address>	IP Address of Agent
	<ipv6-address>	IPv6 Address of Agent

default	None default value

Mode	Global Mode

Usage Guide	For configuring sflow proxy address, The proxy address is used to mark the sample proxy which is similar to OSPF or the Router ID in the BGP. However it is not necessary to make the sFlow sample proxy work properly.

Example

Sample the proxy address at global mode.

switch (config)#sflow agent-address 192.168.1.200

sflow analyzer sflowtrend

Command	sflow analyzer sflowtrend no sflow analyzer sflowtrend
parameter	-
default	Do not configure
Mode	Global Mode
Usage Guide	This command is used to configure sFlow analyzer, no the command disables the analyzer,Configure this command when using sFlowTrend.
Example	Enable sFlow analyzer. Switch(config)#sflow analyzer sflowtrend

sflow counter-interval

Command	sflow counter-interval <i><interval-value></i> no sflow counter-interval
parameter	<i>interval-value</i> is the value of the interval with a valid range of 20~120 and shown in second.
default	No default value
Mode	Port Mode
Usage Guide	If no statistic sampling interval is configured, there will not be any statistic sampling on the interface.
Example	Set the statistic sampling interval on the interface e1/0/1 to 20 seconds. Switch(Config-If-Ethernet1/0/1)#sflow counter-interval 20

sflow data-len

Command	sflow data-len <length-value> no sflow data-len	
parameter	length-value	is the value of the length with a value range of 500-1470
default	The value is 1400 by default.	
Mode	Port Mode	
Usage Guide	For configuring sflow packet length. When combining several samples to a sFlow group to be sent, the length of the group excluding the MAC head and IP head parts should not exceed the configured value.	
Example	Configure the max length of the sFlow packet data to 1000. switch (Config-If-Ethernet1/0/2)#sflow data-len 1000	

sflow destination

Command	sflow destination [<ip-address> ipv6 <ipv6-address>] [<value>] no sflow destination	
parameter	<ip-address>	IP Address of Collector
	<ipv6-address>	IPv6 Address of Collector
	<value>	<1025-65535> Destination Port of Collector
default	The destination port of the sFlow packet is defaulted at 6343, and the analyzer has no default address.	
Mode	Global Mode and Port Mode.	
Usage Guide	If the analyzer address is configured at Port Mode, this IP address and port configured at Port Mode will be applied when sending the sample packet. Or else the address and port configured at global mode will be applied. The analyzer address should be configured to let the sFlow sample proxy work properly.	
Example	Configure the analyzer address and port at global mode. switch (config)#sflow destination 192.168.1.200 1025	

sflow header-len

Command	sflow header-len <length-value> no sflow header-len	
parameter	length-value	is the value of the length with a valid range of 32-256.
default	128 by default.	
Mode	Port Mode.	
Usage Guide	Configure the length of header packets copied in sFlow data sampling. no" form reduction default value for this command. If the packet sample can not be identified whether it is IPv4 or IPv6 when sent to the CPU, certain length of the head of the group has to be copied to the sFlow packet and sent out. The length of the copied content is configured by this command.	
Example	Configure the length of the packet data head copied in the sFlow data sampling to 50. Switch(Config-If-Ethernet1/0/2)#sflow header-len 50	

sflow rate

Command	Port Mode: sflow rate [input output] enable no sflow rate [input output] enable Global Mode: sflow rate [input <Value> output <Value1>]		
parameter	input	Input Packet Sampling	
	output	Output Packet Sampling	
	enable	Enable sflow rate	
	<Value>	<1000-16383500>	Rate Value(pps)
	<Value1>	<1000-1073741823>	Rate Value(pps)
default	No default value.		
Mode	Port Mode or Global Mode		
Usage Guide	The traffic sampling will not be performed if the sampling rate is not configured on the port. And if the ingress group sampling rate is set to 10000, this indicates there will be one group be sampled every 10000 ingress groups.		
Example	Configure the ingress sample rate on port e1/0/1 to 10000 and the egress		

sample rate to 20000.
Switch(Config-If-Ethernet1/0/1)#sflow rate input enable
Switch(config)#sflow rate input 20000

show sflow

Command **show sflow**

parameter -

default -

Mode All Modes.

Usage Guide This command is used to acknowledge the operation state of sFlow.

Example View sFlow configuration information.
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(Ethernet1/0/2)
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
```

Display information	describe
Sflow version 1.2	Indicates sFlow version 1.2
Agent address is 172.16.1.100	sFlow agent address :172.16.1.1100
Collector address have not configured	the sFlow global analyzer address is not configured
Collector port is 6343	the sFlow global destination port is the defaulted 6343
Sampler priority is 2	The priority of sFlow when receiving packets from the hardware is 2.
Sflow DataSource: type 2, index 194(Ethernet1/0/1)	One sample proxy data source of the sFlow is the

	interface e1/0/1 and its type is 2 (Ethernet), the interface index is 194.
Collector address is 192.168.1.200	The analyzer address of the sampling address of the E1/0/1 interface is 192.168.1.200
Collector port is 6343	Default value of the port on E1/0/1 interface sampling proxy is 6343.
Counter interval is 20	The statistic sampling interval on e1/0/1 interface is 20 seconds
Sample rate is input 10000, output 0	The ingress traffic rate of e1/0/1 interface sampling proxy is 10000 and no egress traffic sampling will be performed
Sample packet max len is 1400	The length of the sFlow group data sent by the e1/0/1 interface should not exceed 1400 bytes.
Sample header max len is 50	The length of the packet data head copied in the data sampling of the e1/0/1 interface sampling proxy is 50
Sample version is 4	The datagram version of the sFlow group sent by the E1/0/1 interface sampling proxy is 4.

3 Commands for RSPAN Configuration

remote-span

Command	remote-span no remote-span
parameter	-
default	Not configured
Mode	VLAN Configuration Mode
Usage Guide	This command is used to configure the existing VLAN as RSPAN VLAN. Dedicated RSPAN VLAN should be configured before RSPAN can function. When configuring RSPAN VLAN, it should be made sure that specialized VLAN, such as the default VLAN, dynamic VLAN, private VLAN, multicast VLAN, and layer 3 interface enabled VLAN,

should not be configured as RSPAN VLAN. If any existing sessions are still working when RSPAN is disabled, these sessions will be still working regardless the configuration change. However, if any layer 3 interface is configure in the VLAN after RSPAN is disable, the existing RSPAN session will be stopped.

Example

RSPAN VLAN. VLAN 5 configured.
Switch(Config-Vlan5)#remote-span

monitor session remote vlan

Command

monitor session <session> remote vlan <vid>
no monitor session <session> remote vlan

parameter

<session>	SPAN session numberList, range between 1~7
<vid>	VLAN ID: 1-4094

default

Not configured

Mode

Global Mode

Usage Guide

To configure local mirror session to RSPAN. The VLAN id is the RSPAN VLAN. The mirrored data grams will be attached with RSPAN tags.

Example

Configure the remote vlan of mirror session 1 to 5.
Switch(config)#monitor session 1 remote vlan 5

monitor session reflector-port

Command

monitor session <session> reflector-port interface [<ethernet>] <IFNAME>
no monitor session <session> reflector-port <interface-number>

parameter

<i>session</i>	<1-7> SPAN session numberListA
<IFNAME>	Interface name or number

default

Not configured

Mode

Global Mode.

Usage Guide

This command configures the reflector port for the destination of mirror data grams, and disables the MAC learning function of the specified port. The configuration of reflector port is to change the mode of the local port from the destination port mode to be the reflector mode. Hence, the configuration of reflector port and the destination

port are exclusive. The no command is used to restore the reflector port to normal port. The source port, in access or trunk mode, should not be added to RSPAN VLAN. When the reflector port is configured as springboard of CPU TX direction mirroring, it must be configured as TRUNK port and allows the RSPAN VLAN data passing, the Native VLAN should not be configured as RSPAN VLAN. After configured RSPAN, the vlan tag will be added on the packet of the egress mirror. It will cause the abort error frame on the reflection port, so the default MTU value of the switch should be modified.

Example

Configure port 1/0/5 as a reflection port.

```
Switch(config)#monitor session 1 reflector-port ethernet1/0/5
```

13-Commands for Network Time Management

1 Commands for SNTP

clock timezone

Command	clock timezone WORD {add subtract} <0-23> [<0-59>] no clock timezone	
Parameter	WORD	timezone name, the length should not exceed 16
	add subtract	the action of timezone
	<0-23>	the hour value
	<0-59>	the minute value
Default	None.	
Mode	Global Mode	
Usage Guide	This command configures timezone in global mode. The timezone name is invalid with the blank, the hour and minute value must be in the specific range. The no command deletes the configured timezone.	
Example	Configure the action as add for the eighth timezone globally. Switch(config)#clock timezone aaa add 8	

sntp polltime

Command	sntp polltime <interval> no sntp polltime	
Parameter	<interval>	is the interval value from 16 to 16284
Default	The default polltime is 64 seconds.	
Mode	Global Mode	
Usage Guide	Sets the interval for SNTP clients to send requests to NTP/SNTP.	

The no command cancels the polltime sets and restores the default setting.

Example

Setting the client to send request to the server every 128 seconds.

```
Switch(config)#ntp polltime128
```

sntp server

Command

```
sntp server [vrf <WORD>]{<ip-address> | <ipv6-address>} [source {vlan <vlan no> | loopback <loopback no>}] [version <version_no>]  
no sntp server {<ip-address> | <ipv6-address>} [source {vlan <vlan no> | loopback <loopback no>}] [version <version_no>]
```

Parameter

<WORD>	Virtual Routing and Forwarding instance name
<ip-address>	IPv4 address of time server
<ipv6-address>	IPv6 address of time server
<vlan no>	Virtual LAN number, ranging from 1 to 4094
<loopback no>	Loopback identifier, ranging from 1 to 1024
<version_no>	Version number, ranging from 1 to 4, the default is 4

Default

By default,do not configure the time server.

Mode

Global Mode

Usage Guide

Enable the specified time server as clock source

The no command deletes the specified time server.

Example

Configure the time server address as 1.1.1.1, specify the interface of the source address as vlan1:

```
Switch(config)#ntp server 1.1.1.1 source vlan 1
```

show sntp

Command

```
show sntp
```

Parameter

none	none

Default	None.
Mode	Admin/Global mode
Usage Guide	Displays current SNTP client configuration and server status.
Example	Displaying current SNTP configuration. Switch(config)#show sntp

2 Commands for NTP

ntp access-group server

Command	ntp access-group server <acl> no ntp access-group server <acl>
Parameter	<acl> ACL number, range is from 1 to 99
Default	Not configure the access control of NTP Server by default.
Mode	Global Mode
Usage Guide	To configure/cancel the access control list of NTP Server. The no command delete configuration.
Example	To configure access control list 2 on the switch. Switch(config)#ntp access-group server 2

ntp authenticate

Command	ntp authenticate no ntp authenticate
Parameter	none none

Default	By default, NTP authentication is cancelled.
Mode	Global Mode
Usage Guide	To enable/cancel NTP authentication function. The no command cancel NTP authentication function.
Example	To enable NTP authentication function. Switch(config)#ntp authenticate

ntp authentication-key

Command	ntp authentication-key <key-id> md5 <value> no ntp authentication-key <key-id>	
Parameter	<key-id>	The id of key, range is from 1 to 4294967295
	<value>	The value of key, range between 1 to 16 of ascii code
Default	The authentication key of NTP authentication is not configured by default.	
Mode	Global Mode	
Usage Guide	To enable/cancel NTP authentication function, and defined NTP authentication key. The no command cancel NTP authentication function	
Example	To define the authentication key of NTP authentication, the key-id is 20, the md5 is abc. Switch(config)#ntp authentication-key 20 md5 abc	

ntp broadcast server count

Command	ntp broadcast server count <number>

no ntp broadcast server count

Parameter	<number> the max number of broadcast servers, 1-100
Default	The default max number of broadcast servers is 50.
Mode	Global Mode
Usage Guide	Set the max number of broadcast or multicast servers supported by the NTP client. The no operation will cancel the configuration and restore the default value.
Example	Configure the max number of broadcast servers is 70 on the switch. Switch(config)#ntp broadcast server count 70

ntp disable

Command	ntp disable no ntp disable
Parameter	none none
Default	By default, NTP function are enabled on all ports.
Mode	VLAN Configuration Mode
Usage Guide	To disable/enable the NTP function on port. The no command disables the NTP function on the port.
Example	To disable the NTP function on vlan1 interface. Switch(config)# interface vlan 1 Switch(config-if-Vlan1)#ntp disable

ntp enable

Command	ntp enable ntp disable
Parameter	none none
Default	By default, global disable NTP function.
Mode	Global Mode
Usage Guide	To enable/disable NTP function globally. Disable command global disable NTP function.
Example	Configure switch global enable NTP function. Switch(config)# ntp enable

ntp ipv6 multicast client

Command	ntp ipv6 multicast client no ntp ipv6 multicast client
Parameter	none none
Default	By default, Interface does not receive IPv6 NTP multicast packets.
Mode	VLAN Configuration mode
Usage Guide	Configure the specified interface to receive IPv6 NTP multicast packets The no command will cancels the specified interface to receive IPv6 NTP multicast packets.
Example	Enable the function for receiving IPv6 NTP multicast packets on vlan1 interface. Switch(config)# interface vlan 1 Switch(config-if-Vlan1)#ntp ipv6 multicast client

ntp multicast client

Command	ntp multicast client no ntp multicast client		
Parameter	<table><tr><td>none</td><td>none</td></tr></table>	none	none
none	none		
Default	By default, Interface does not receive NTP multicast packets.		
Mode	VLAN Configuration mode		
Usage Guide	Configure the specified interface to receive NTP multicast packets. The no command will cancels the specified interface to receive NTP multicast packets.		
Example	Enable the function for receiving NTP multicast packets on vlan1 interface. Switch(config)# interface vlan 1 Switch(config-if-Vlan1)#ntp multicast client		

ntp server

Command	ntp server [host [vrf <WORD>] <WORD1>] {<ip-address> <ipv6-address>} [source loopback <Loopback ID> vlan <Vlan port number>] [version <version_no>] [key <key-id>] no ntp server [host [vrf <WORD>] <WORD1>] {<ip-address> <ipv6-address>}												
Parameter	<table><tr><td><WORD></td><td>Virtual Routing and Forwarding instance name</td></tr><tr><td><WORD1></td><td>hostname of server</td></tr><tr><td><ip-address></td><td>IPv4 address of time server</td></tr><tr><td><ipv6-address></td><td>IPv6 address of time server</td></tr><tr><td><version_no></td><td><1-4> NTP version number</td></tr><tr><td><key-id></td><td><1-4294967295> Key number</td></tr></table>	<WORD>	Virtual Routing and Forwarding instance name	<WORD1>	hostname of server	<ip-address>	IPv4 address of time server	<ipv6-address>	IPv6 address of time server	<version_no>	<1-4> NTP version number	<key-id>	<1-4294967295> Key number
<WORD>	Virtual Routing and Forwarding instance name												
<WORD1>	hostname of server												
<ip-address>	IPv4 address of time server												
<ipv6-address>	IPv6 address of time server												
<version_no>	<1-4> NTP version number												
<key-id>	<1-4294967295> Key number												
Default	By default, disable.												
Mode	Global Mode												

Usage Guide	To enable specified time server of time source. The no form of this command cancels the specified time server of time source.
Example	To configure time server address as 1.1.1.1 on switch. <pre>Switch(config)# ntp server 1.1.1.1</pre>

ntp syn-interval

Command	ntp syn-interval <1-3600> no ntp syn-interval
Parameter	<1-3600> the request packet sending interval of ntp client as 1s-3600s
Default	By default, 64s interval.
Mode	Global Mode
Usage Guide	Configure the request packet sending interval of ntp client as 1s-3600s. For responding the risk of ntp adjusting the system time under the high latency network, ntp client will select the time information with the smallest latency for the system time synchronization after sent 8 ntp time requisitions. So at the default configuration, ntp client sends the requisition packet once every 64s, after 8 times, it will adjust the time. It means to adjust the system time every 8 minutes. If user wants to configure the interval, such as one hour, user should adjust the packet sending interval as 450(3600/8) s. The no command recovers to be the default value of 64s.
Example	Configure to adjust the system time once an hour, and the packet sending time is 450s. <pre>Switch(config)# ntp syn-interval 450</pre>

ntp trusted-key

Command	ntp trusted-key <key-id> no ntp trusted-key <key-id>	
Parameter	<key-id>	The id of key, range is from 1 to 4294967295
Default	Trusted key is not configured by default.	
Mode	Global Mode	
Usage Guide	To configure the trusted key. The no command cancels the trusted key.	
Example	To configure the specified key 20 to trusted key. Switch(config)# ntp trusted-key 20	

show ntp status

Command	show ntp status	
Parameter	none	none
Default	None.	
Mode	Admin/Global Mode	
Usage Guide	To display time synchronization status, include synchronized or not, layers, address of time source and so on.	
Example	Display time synchronization status. Switch(config)# 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

show ntp session

Command `show ntp session [vrf <WORD>] [<ip-address> | <ipv6-address>]`

Parameter	<WORD>	Virtual Routing and Forwarding instance name
	<ip-address>	The IPv4 address of some specifics configured time server
	<ipv6-address>	The IPv6 address of some specifics configured time server

Default None.

Mode Admin/Global Mode

Usage Guide To display the information of all NTP session or one specific session, include server ID, server layer, and the local offset according to server. (The symbol * means this server is the selected local time source)

Example To display the information of all NTP session.

Switch(config)# 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

3 Commands for Summer Time

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

Parameter	<word>	the time zone name of summer time
	<HH:MM>	the start time, the format is hour (from 0 to 23):minute (from 0 to 59)
	<YYYY.MM.DD>	the start date, the format is year (from 1970 to 2038).month (from 1 to 12).date (from 1 to 31)
	<HH:MM>	the end time, the format is hour (from 0 to 23):minute (from 0 to 59)
	<YYYY.MM.DD>	the end date, the format is year (from 1970 to 2038).month (from 1 to 12).date (from 1 to 31)
	<offset>	the time offset, the range from 1 to 1440, unit is minute, default value is 60 minutes

Default By default, there is no summer time range.

Mode Global Mode

Usage Guide Configure summer time range, the time in this range is summer time.
This command sets the absolute start and end time for summer time. When the system time reaches to the start time point of summer time, the clock is changed and increase <offset> value, the system enters summer time. When the system time reaches to the end time point of summer time, the clock is changed again, subtract <offset> value from system time, the system finishes summer time. Note: the end time should be bigger than the start time for configuring summer time.

The no command deletes the configuration.

Example Configure the time range of summer time at 12:10 from april 6th to august 6th in 2010, offset value as 70 minutes, summer time is named as aaa.

Switch(config)#clock summer-time aaa absolute 12:10 2010.4.6 12:10 2010.8.6 70

clock summer-time recurring

Command clock summer-time <word> recurring <HH:MM> <MM.DD> <HH:MM>
 <MM.DD> [<offset>]
 no clock summer-time

Parameter	<word>	the time zone name of summer time
	<HH:MM>	the start time, the format is hour (from 0 to 23):minute (from 0 to 59)
	<MM.DD>	the start date, the format is month(from 1 to 12).date(from 1 to 31)
	<HH:MM>	the end time, the format is hour(from 0 to 23):minute(from 0 to 59)
	<MM.DD>	the end date, the format is month(from 1 to 12).date(from 1 to 31)
	<offset>	the time offset, the range from 1 to 1440, unit is minute, default value is 60 minutes.

Default By default, there is no summer time range.

Mode Global Mode

Usage Guide Configure the recurrent summer time range, the time in this range is summer time. This command sets the start and the end time for the recurrent summer time. When the system time reaches to the start time point of summer time, the clock is changed and increase <offset> value, the system enters summer time. When the system time reaches to the end time point of summer time, the clock is changed again, subtract <offset> value from system time, the system finishes summer time. There is no relation between the recurrent summer time to the year, the system clock will be changed when it reaches to the start and the end time point of summer time year after year. This command supports the summer time of southern hemisphere.

The no command delete summer time configuration.

Example Configure the time range of summer time at 12:10 from april 6th to august 6th year after year, offset value as 70 minutes, summer time is named as aaa.

Switch(config)#clock summer-time aaa recurring 12:10 4.6 12:10 8.6 70

clock summer-time recurring

Command clock summer-time <word> recurring<HH:MM> <week>|<first>|<last> <day>
 <month>< HH:MM> <week>|<first>|<last> <day> <month> [<offset>]
no clock summer-time

Parameter	<word>	the time zone name of summer time
	<HH:MM>	the start time, the format is hour(from 0 to 23):minute(from 0 to 59)
	<week>	the week from 1 to 4, first or last
	<first>	First weekday of the month
	<last>	Last weekday of the month
	<day>	the week value, the value as "Sun", "Mon", "Tue", "Wed", "Thu", "Fri", "Sat"
	<month>	the month, the value as "Jan", "Feb", "Mar", "Apr", "May", "Jun", "Jul", "Aug", "Sep", "Oct", "Nov", "Dec"
	<HH:MM>	the end time, the format is hour(from 0 to 23):minute(from 0 to 59)
	<week>	the week from 1 to 4, first or last
	<day>	the week value, the value as "Sun", "Mon", "Tue", "Wed", "Thu", "Fri", "Sat"
	<month>	the month, the value as "Jan", "Feb", "Mar", "Apr", "May", "Jun", "Jul", "Aug", "Sep", "Oct", "Nov", "Dec"
	<offset>	the time offset, the range from 1 to 1440, unit is minute, default value is 60 minutes

Default By default, there is no summer time range.

Mode Global Mode

Usage Guide Configure the recurrent summer time range, the time in this range is summer time. This command sets the start and end time for the recurrent summer time flexibly. When the system time reaches to the start time point of summer time, the clock is changed and increase <offset> value, the system enters summer time. When the system time reaches to the end time point of summer time, the clock is changed again, subtract <offset> value from system time, the system finishes summer time. There is no relation between the recurrent summer time to the year, the system clock will be changed when it reaches to the start and the end time point of summer time year after year. This command supports summer time of southern hemisphere.

The no command delete summer time configuration.

Example Configure summer time at 12:10 from the first Monday of april to the last Saturday of august year after year, offset value as 70 minutes, summer time is named as

4 Commands for PTP

The PTP protocol employs constraints.

1. Bidirectional synchronization between the PTP clock and the system clock is not supported.
2. The transparent clock mode does not support cross-VLAN functionality.
3. It supports 1 profile at the same time. Different profiles are mutually exclusive, and only one can be enabled at a time.
4. It supports 1 mode at the same time. Different modes are mutually exclusive. Only one mode can be enabled at the same time.
5. When the configuration mode is set to "oc", only one port PTP enablement can be configured. When changing ports, the previously configured port needs to be cancelled. The OC mode only supports one port.
6. The configuration mode is set to tc (e2etc / p2ptc), and the clock-step only supports two-step, while one-step configuration is not supported.
7. At the same time, only one domain is supported. The default is 0. Configuring other domains will overwrite the currently configured domain. PTP multi-domain functionality is not supported.
8. Delete or switch the profile. The PTP and other configurations under the global and interface sections will be automatically cleared. Please confirm whether to proceed.
9. After deleting or switching the mode and enabling PTP on the interface, the PTP-related configurations on the interface will be automatically cleared. Please confirm whether to proceed. If PTP enable is not enabled on the interface, the PTP configurations will be directly cleared.
10. When configuring the st2059-2 or aes67-2015 profile, the PTP transport-protocol udp configuration will be automatically generated. At the same time, the UDP mode cannot be cancelled. If you try to cancel it, an error will occur because the st2059-2 or aes67-2015 profile only supports the UDP mode.
11. After configuring the profile, it is not recommended to deploy devices that do not support PTP in a PTP network. This will reduce the synchronization accuracy.
12. PTP is not supported in the IPv6 and VRF environment.
13. In the VSF (Virtual Switching Framework) environment, PTP is not supported.
14. If multiple devices in the network are configured with the role of mandatory master clock, it will directly disrupt the normal synchronization logic of PTP. Therefore, only one device in the system should be configured with the role of mandatory master clock.

ptp profile

Command

ptp profile { 1588v2 | aes67-2015 | st2059-2 }
no ptp profile

In config view, use this command to set the PTP protocol standard. Use the no ptp profile command to delete the PTP protocol standard.

Parameter

1588v2	IEEE 1588 Version 2
aes67-2015	AES67-2015
st2059-2	SMPTE ST 2059-2

Default

N/A

Mode	config mode
Usage Guide	Before enabling the PTP function, you must first configure the PTP profile. All PTP-related commands are premised on the PTP profile being configured first. Changing the PTP profile will prompt that related PTP configurations will be cleared and that the relevant PTP settings will be updated to comply with the protocol standard.
Example	The following example shows how to configure the PTP profile as 1588v2 in config view. Switch#config Switch(config)# ptp profile 1588v2

ptp mode

Command	ptp mode {oc bc e2etc p2ptc} no ptp mode
	Configure the device type in the PTP protocol. The no ptp mode command is used to remove the configured mode.
Parameter	oc Ordinary clock。 bc Boundary clock e2etc End-to-End transparent clock p2ptc Peer-to-Peer transparent clock
Default	oc
Mode	Config mode
Usage Guide	When the device type is configured as OC, PTP can be enabled on only one interface. When configured as BC, E2ETC, or P2PTC, PTP must be enabled on at least two interfaces. If PTP enable has been configured on interfaces, changing the PTP mode will prompt a warning to clear the related PTP configurations on those interfaces. If PTP enable has not been configured, changing the PTP mode will directly clear the related PTP configurations on the interfaces. The P2PTC and E2ETC PTP modes are mutually exclusive with one-step.
Example	Switch# (config)ptp mode oc

ptp clock-step

Command	ptp clock-step {one-step two-step} no ptp clock-step This command is used to select the PTP clock-step mode. The no ptp clock-step command is used to restore the PTP clock-step to two-step mode.
Parameter	{one-step two-step} clock-step, One-step or two-step mode.
Default	two-step
Mode	config mode
Usage Guide	ptp clock-step is a core command in the PTP protocol used to specify the timestamp distribution mode of the master clock. The core difference between the two modes lies in the mechanism for carrying the "precise transmission timestamp": in one-step mode, the timestamp is embedded directly in the Sync or Pdelay_Resp message; in two-step mode, a Sync or Pdelay_Resp message without a precise timestamp is sent first, followed immediately by a Follow_Up or Pdelay_Resp_Follow_Up message that carries the precise transmission timestamp of the preceding message. One-step mode is mutually exclusive with ptp mode p2ptc or e2etc.
Example	Switch(config)# ptp clock-step one-step

ptp enable

Command	ptp enable no ptp enable Enable the PTP function on a port. The no ptp enable command disables the PTP function on a port.
Parameter	N/A
Default	disable
Mode	port mode
Usage Guide	Before configuring this command, you must first configure the ptp profile command.
Example	Switch(config-if-ethernet1/0/5)#ptp enable

ptp delay-mechanism

Command	ptp delay-mechanism {e2e p2p} no ptp delay-mechanism
	Configure the delay mechanism on a port. The no ptp delay-mechanism command is used to remove the delay mechanism from an interface.
Parameter	e2e The port delay measurement mechanism is set to E2E mode. p2p The port delay measurement mechanism is set to P2P mode.
Default	disable
Mode	port mode
Usage Guide	This command can be issued only when the PTP mode is set to BC or OC.
Example	Switch(config-if-ethernet1/0/5)#ptp delay-mechanism e2e

ptp clock-class

Command	ptp clock-class <0-255> no ptp clock-class
	Set the local PTP clock-class. The no ptp clock-class command is used to restore the clock-class to its default value.
Parameter	<0-255> Value range: 0 to 255.
Default	248
Mode	config mode
Usage Guide	PTP clock-class is a level identifier used to describe clock quality and traceability. In a PTP network, it is one of the key factors that determine which clock can become the GrandMaster clock. Simply put, a smaller clock-class value indicates a higher level and greater reliability of the clock source. The BMCA election determines the best master clock in the following order (the next parameter is compared only if the previous one is the same): priority1 → clock-class → clock-accuracy → priority2 → clock-identity
Example	Switch(config)#ptp clock-class 10

ptp clock-accuracy

Command	ptp clock-accuracy {<32-47> <128-253>} no ptp clock-accuracy	
	Set the local PTP clock-accuracy. The no ptp clock-accuracy command is used to restore the clock-accuracy to its default value.	
Parameter	<32-47>	Value range: 32-47
	<128-253>	Value range: 128-253
Default	32	
Mode	config mode	
Usage Guide	PTP clock-accuracy is a key attribute that describes clock quality. It quantifies the degree of deviation of the clock from a standard time reference, such as UTC — in other words, the "precision" of the clock. Simply put, a smaller clock-accuracy value indicates that the clock is more accurate. The BMCA election determines the best master clock in the following order (the next parameter is compared only if the previous one is the same): priority1 → clock-class → clock-accuracy → priority2 → clock-identity	
Example	Switch(config)#ptp clock-accuracy 130	

ptp priority1

Command	ptp priority1 <0-255> no ptp priority1	
	Set the local PTP priority1. The no ptp priority1 command is used to restore priority1 to its default value.	
Parameter	<0-255>	Value range: 0 -255
Default	128	
Mode	config mode	
Usage Guide	PTP priority1 is the most important and highest-priority election attribute in the PTP protocol. Essentially, it is a configurable user priority that allows network administrators to manually intervene in the master clock election process. The BMCA election determines the best master clock in the following order (the next parameter is compared only if the previous one is the same): priority1 → clock-class → clock-accuracy → priority2 → clock-identity. When the PTP mode is OC, priority1 is 128. When the mode is BC or TC,	

priority1 is 254. When force-state master is configured, priority1 is 0.

Example

Switch(config)#ptp priority1 130

ptp priority2

Command

ptp priority2 <0-255>
no ptp priority2

Set the local PTP priority2. The no ptp priority2 command is used to restore priority2 to its default value.

Parameter

<0-255> **Value range: 0 -255**

Default

128

Mode

config mode

Usage Guide

PTP priority2 is an attribute defined in the PTP (Precision Time Protocol) protocol. It is used in the Best Master Clock Algorithm (BMCA) as a secondary criterion for participating in the Grandmaster election process. The BMCA election determines the best master clock in the following order (the next parameter is compared only if the previous one is the same):
priority1 → clock-class → clock-accuracy → priority2 → clock-identity.

When force-state master is configured, priority2 is 0.

Example

Switch(config)#ptp priority2 130

ptp domain

Command

ptp domain <0-255>
no ptp domain

This command is used to set the PTP domain ID. The no ptp domain command is used to restore the PTP domain ID to 0.

Parameter

<0-255> Specify the domain ID. The valid value range is 0 to 255.

Default	0
Mode	config mode
Usage Guide	The ptp domain is a core configuration command in the PTP (IEEE 1588) protocol used to define PTP domains. Its primary function is to group and isolate different PTP devices — devices within the same domain participate in BMCA election and time synchronization, while devices in different domains do not interfere with each other.
Example	Switch(config)#ptp domain 10

ptp transport-protocol

Command	ptp transport-protocol udp no ptp transport-protocol udp
	This command is used to encapsulate PTP messages in UDP/IP packets for transmission. The no ptp transport command is used to restore the PTP message encapsulation to Ethernet frames.
Parameter	-
Default	N/A
Mode	config mode
Usage Guide	This command must be used together with ptp source ip-address.
Example	Switch(config)# ptp transport-protocol udp

ptp source ip-address

Command	ptp source ip-address A.B.C.D/M no ptp source ip-address
	This command is used to specify the source IPv4 address that the device uses when sending PTP messages (encapsulated over UDP/IPv4). The no ptp bc udp command is used to remove the configured source IPv4 address.
Parameter	A. B. C. D/M: IPv4 address
Default	N/A
Mode	config mode

Usage Guide	Before using this command, you must first configure ptp transport-protocol udp.
Example	Switch(config)ptp source ip-address 11.1.1.1/16

ptp dscp

Command	ptp dscp <0-63> no ptp dscp
	This command is used to configure the queue priority for PTP messages.
Parameter	<0-63> DSCP value
Default	When the PTP profile is 1588v2 or AES67-2015, the DSCP value defaults to 0. When the PTP profile is ST2059-2, the DSCP value defaults to 63.
Mode	config mode
Usage Guide	Adjust the message transmission queue priority — a higher value indicates a higher priority.
Example	Switch(config)ptp dscp 10

ptp announce-interval

Command	ptp announce-interval WORD no ptp announce-interval
	This command is used to configure the announce message transmission interval. The no ptp announce-interval command is used to restore the announce message transmission interval to its default value.
Parameter	WORD 0to4 (ptp profile 1588v2/aes67-2015) -3to1 (ptp profile st2059-2)
Default	By default, when the PTP profile is 1588v2 or AES67-2015, the announce-interval is 1; for ST2059-2, the announce-interval is -2.
Mode	port mode
Usage Guide	N/A
Example	Switch(config-if-ethernet1/0/1)#ptp announce-interval 0

ptp announce-timeout multiple-value

Command	ptp announce-timeout multiple-value <2-10> no ptp announce-timeout multiple-value This is a core command in the PTP protocol used to configure the announce message receipt timeout threshold for the slave clock. The no ptp announce-receipt-timeout command is used to restore the announce message timeout threshold to 3.
Parameter	<2-10> Configure the timeout multiplier.
Default	3
Mode	port mode
Usage Guide	N/A
Example	Switch(config-if-ethernet1/0/1)#ptp announce-receipt-timeout 4

ptp sync-interval

Command	ptp sync-interval WORD no ptp sync-interval This command is used to configure the sync message transmission interval. The no ptp sync-interval command is used to restore the sync message transmission interval to its default value.
Parameter	WORD -1to1 (ptp profile 1588v2) -4to1 (ptp profile aes67-2015) -5to-1 (ptp profile st2059-2)
Default	By default, when the PTP profile is 1588v2, the sync-interval is 0; for AES67-2015, the sync-interval is -3; and for ST2059-2, the sync-interval is -3.
Mode	port mode
Usage Guide	N/A
Example	Switch(config-if-ethernet1/0/1)#ptp sync-interval 1

ptp pdelay-req-interval

Command	ptp pdelay-req-interval WORD no ptp pdelay-req-interval
	This command is used to configure the pdelay-req message transmission interval. The no ptp pdelay-req-interval command is used to restore the pdelay-req message transmission interval to its default value.
Parameter	WORD 0to5 (ptp profile 1588v2/ aes67-2015) -5to4 (ptp profile st2059-2)
Default	0
Mode	port mode
Usage Guide	N/A
Example	Switch(config-if-ethernet1/0/1)#ptp pdelay-req-interval 1

ptp vlan

Command	ptp vlan <1-4094> no ptp vlan
	Use this command to specify a VLAN for PTP messages on an interface. The no ptp vlan command is used to remove the VLAN configured for PTP messages on an interface.
Parameter	<1-4094> Specify the VLAN value.
Default	N/A
Mode	port mode
Usage Guide	When the interface is in trunk mode, this command must be used to specify a specific tagged VLAN for PTP messages.
Example	Switch(config-if-ethernet1/0/1)#ptp vlan 100

ptp force-state

Command	ptp force-state {master passive slave } no ptp force-state
	Use this command to force the role of an OC device. The no ptp force-state

	command is used to cancel the forced state.
Parameter	master: Configure the port as a master clock port. passive: Configure the port as a passive port. slave: Configure the port as a slave clock port.
Default	N/A
Mode	port mode
Usage Guide	This command can be used only when the PTP mode is set to OC.
Example	Switch(config-if-ethernet1/0/1)#ptp force-state slave

show ptp clock

Command	show ptp clock
	Use this command to view detailed status information of the local PTP service.
Parameter	-
Default	N/A
Mode	all mode
Usage Guide	N/A
Example	Switch# show ptp clock

show ptp config

Command	show ptp config
	This command is used to view PTP configuration information and PTP port configuration information.
Parameter	-
Default	N/A
Mode	all mode
Usage Guide	N/A

Example	Switch# show ptp config

show ptp packet-statistics

Command	show ptp packet-statistics

View PTP packet reception statistics.

Parameter	-

Default	N/A

Mode	all mode

Usage Guide	N/A

Example	Switch#show ptp packet-statistics

show ptp port

Command	show ptp port

This command is used to query the local PTP port configuration and status.

Parameter	-

Default	N/A

Mode	all mode

Usage Guide	N/A

Example	Switch#show ptp port

show ptp parent

Command	show ptp parent This command is used to query the key information about the parent clock of the local PTP clock.
Parameter	-
Default	N/A
Mode	all mode
Usage Guide	N/A
Example	Switch#show ptp parent

14-Debugging and Diagnosis

1 SHOW

clear history all-users

Command	clear history all-users
Parameter	none
Default	none
Mode	Admin mode
Usage	Using this command can clear the command history of all users.
Example	Switch#clear history all-users

clear logging

Command	clear logging <sdram> <nvr>				
Parameter	<table><tr><td><sdram></td><td>Sdram</td></tr><tr><td><nvr></td><td>Nvr</td></tr></table>	<sdram>	Sdram	<nvr>	Nvr
<sdram>	Sdram				
<nvr>	Nvr				
Default	none				
Mode	Admin mode				
Usage	When the old information in the log buffer zone is no longer concerned, we can use this command to clear all the information.				
Example	Clear all information in the log buffer zone sdram or nvr . Switch#clear logging sdram				

history all-users max-length

Command	history all-users max-length <count>
Parameter	<count> the command history number can be saved, ranging from 100 to 1000
Default	The system can save 100 recent command history of all users at best by default
Mode	Global mode

Usage	using this command can set the max command history number
Example	Switch#config Switch(config)#history all-users max-length 500

logging

Command	logging [vrf <WORD>]{<ipv4-addr> <ipv6-addr> } [facility<local-number> udp-port<UDP port number>] [level <severity>] logging console logging flash level <severity> no logging [vrf <WORD>] {<ipv4-addr> <ipv6-addr> } [facility<local-number> udp-port<UDP port number>] [level <severity>] no logging console no logging flash level <severity>													
Parameter	<table><tr><td><WORD></td><td>Virtual Routing and Forwarding instance name</td></tr><tr><td><ipv4-addr></td><td>IPv4 address of the host</td></tr><tr><td><ipv6-addr></td><td>IPv6 address of the host</td></tr><tr><td><local-number></td><td>recording equipment of the host with a valid range of local0 ~ local7, which is in accordance with the facility defined in the RFC3164</td></tr><tr><td><UDP port number></td><td><1-65535> UDP port number (default value: 514)</td></tr><tr><td><severity></td><td>severity threshold of the log information severity level. The rule of the log information output is explained as follows: only those with a level equal to or higher than the threshold will be outputted. For detailed description on the severity please refer to the operation manual.</td></tr></table>		<WORD>	Virtual Routing and Forwarding instance name	<ipv4-addr>	IPv4 address of the host	<ipv6-addr>	IPv6 address of the host	<local-number>	recording equipment of the host with a valid range of local0 ~ local7, which is in accordance with the facility defined in the RFC3164	<UDP port number>	<1-65535> UDP port number (default value: 514)	<severity>	severity threshold of the log information severity level. The rule of the log information output is explained as follows: only those with a level equal to or higher than the threshold will be outputted. For detailed description on the severity please refer to the operation manual.
<WORD>	Virtual Routing and Forwarding instance name													
<ipv4-addr>	IPv4 address of the host													
<ipv6-addr>	IPv6 address of the host													
<local-number>	recording equipment of the host with a valid range of local0 ~ local7, which is in accordance with the facility defined in the RFC3164													
<UDP port number>	<1-65535> UDP port number (default value: 514)													
<severity>	severity threshold of the log information severity level. The rule of the log information output is explained as follows: only those with a level equal to or higher than the threshold will be outputted. For detailed description on the severity please refer to the operation manual.													
Default	No log information output to the log host by default. The default recorder of the log host is the local0; the default severity level is warnings.													
Mode	Global mode													
Usage	The command is used to configure the output channel of the log host. The “no” form of this command will disable the output at the log host output channel. Only when the log host is configured by the logging command, this command will be available. We can configure many IPv4 and IPv6 log hosts.													
Example	Send the log information with a severity level equal to or higher than warning to the log server with an IPv4 address of 100.100.100.5, and save to the log recording equipment local1. Switch#config Switch(config)#logging 100.100.100.5 facility local1 level warnings													

logging executed-commands

Command	logging executed-commands {enable disable}
Parameter	none
Default	Disable state.
Mode	Global mode
Usage	After enable this command, the commands executed by user at the console, telnet or ssh terminal will record the log, so it should be used with the logging LOGHOST command.
Example	Enable the command and send the commands executed by user into log host (10.1.1.1) Switch#config Switch(config)#logging 10.1.1.1 Switch(config)#logging executed-commands enable

logging loghost sequence-number

Command	logging loghost sequence-number no logging loghost sequence-number
Parameter	none
Default	Do not include the sequence-number.
Mode	Global mode
Usage	Add the loghost sequence-number for the log; the no command does not include the loghost sequence-number. Use logging command to configure the loghost before this command is set.
Example	Open the loghost sequence-number Switch#config Switch(config) #logging loghost sequence-number

logging source-ip

Command	logging source-ip { <A.B.C.D> <X:X::X:X> }
Parameter	<ipv4-addr> IPv4 address of the host <ipv6-addr> IPv6 address of the host
Default	None0000
Mode	Global mode

Usage	Appoint the source IP address of the log packet which is sent to the log server, the ipv4 or ipv6 addresses can be configured. After configured this command, the log information sent to the server has the IP address; if this command is not configured, the log information does not have the IP address.
Example	Configure the source IP address of the log packet which is sent to the log server. Switch#config Switch(config)#logging source-ip 2010::10

ping

Command	ping [vrf <WORD>] [[src <source-address>] { <destination-address> host <hostname>}] [[[count <input number>] size <input number1>] timeout <Input number2>]	
	ping mpls [src <source-address>]<destination-address>	
Parameter	<WORD>	VPN Routing/Forwarding instance name
	<source-address>	<source-address> is the source IP address where the ping command is issued, with IP address in dotted decimal format.
	<destination-address>	<destination-address> is the target IP address of the ping command, with IP address in dotted decimal format
	<hostname>	<hostname> is the target host name of the ping command, which should not exceed 64 characters.
	<input number>	<1-2147483647> Input number for ping count
	<input number1>	<1-21832> Input number for ping size in bytes
	<input number2>	<100-60000> Input number for ping timeout in milliseconds
Default	5 ICMP echo requests will be sent. The default packet size and time out is 56 bytes and 2 seconds.	
Mode	Admin mode	
Usage	Issue ICMP request to remote devices, check whether the remote device can be reached by the switch. When the ping command is entered without any parameters, interactive configuration mode will be invoked. And ping parameters can be entered interactively.	
Example	Example 1: To ping with 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 the example above, the switch is made to ping the device at 10.1.128.160. The command did not receive ICMP reply packets for the first three ICMP echo requests within default 2 seconds timeout. The ping failed for the first three tries. However, the last two ping succeeded. So the success rate is 40%. It is denoted on the switch “.” for	

ping failure which means unreachable link, while "!" for ping success, which means reachable link.

Example 2: Ping with parameters entered interactively.

Switch#ping

VRF name:

Use IP Address[y]: y

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

Display Information	Explanation
VRF name	VRM name. If MPLS is not enabled, this field will be left empty.
Target IP address:	The IP address of the target device.
Use source address option[n]	Whether or not to use ping with source address.
Source IP address	To specify the source IP address for ping.
Repeat count [5]	Number of ping requests to be sent. The default value is 5.
Datagram size in byte [56]	The size of the ICMP echo requests, with default as 56 bytes.
Timeout in milli-seconds [2000]:	Timeout in milli-seconds, with default as 2 seconds.
Extended commands [n]:	Whether or to use other extended options.

ping6

Command

ping6 [vrf <WORD>] [<dst-ipv6-address> | host <hostname>] [src <src-ipv6-address>] [[[count <input number>] size <input number1>] timeout <Input number2>]

Parameter

<WORD>	VPN Routing/Forwarding instance name
<dst-ipv6-address>	target IPv6 address of the ping command
<src-ipv6-address>	source IPv6 address where the ping command is issued
<hostname>	arget host name of the ping command, which should not exceed 64 characters.
<input number>	<1-2147483647> Input number for ping count
<input number1>	<1-21832> Input number for ping size in bytes
<input number2>	<100-60000> Input number for ping timeout in milli-seconds

Default

Five ICMP6 echo request will be sent by default, with default size as 56 bytes, and default

	timeout to be 2 seconds.
Mode	Admin mode
Usage	To check whether the destination network can be reached. When the ping6 command is issued with only one IPv6 address, other parameters will be default. And when the ipv6 address is a local data link address, the name of VLAN interface should be specified. When the source IPv6 address is specified, the command will fill the icmp6 echo requests with the specified source address for ping.
Example	Example 1: To issue ping6 command with default parameters. <pre>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</pre> Example 2: To issue the ping6 command with parameters input interactively. <pre>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</pre>

Display Information	Explanation
ping6	The ping6 command
Target IPv6 address	The target IPv6 address of the command
Output Interface	The name of the VLAN interface, which should be specified when the target address is a local data link address.
Use source IPv6 address [n]:	Whether or not use source IPv6 address. Disabled by default.
Source IPv6 address	Source IPv6 address.
Repeat count[5]	Number of the ping packets.
Datagram size in byte[56]	Packet size of the ping command. 56 byte by default.
Timeout in milli-seconds[2000]	Timeout for ping command. 2 seconds by default.
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	Statistic information, success rate is 100 percent of ping packet.

show boot-files

Command	show boot-files [member <member id>]
Parameter	<member id>
Default	none
Mode	Admin and Configuration Mode.
Usage	Display the first and second IMG files and the CFG file enabled by switch. After implementing this command, the booting sequence of IMG files in the corresponding storage device, which IMG file is currently used in booting, the configuration information of the CFG file in the storage device and the CFG file currently booted.
Example	Display the first and second IMG files and the CFG file enabled by switch. <pre>Switch#show boot-files</pre> Booted files on switch The primary img file at the next boot time: flash:/nos.img The backup img file at the next boot time: flash:/nos.img Current booted img file: flash:/nos.img The startup-config file at the next boot time: flash:/startup.cfg Current booted startup-config file: flash:/startup.cfg If the CFG file of the next booting is set as NULL, the CFG part mentioned above will be displayed as follows: The startup-config file at the next boot time: NULL Current booted startup-config file: flash:/startup.cfg

show flash

Command	Show flash
Parameter	none
Default	none
Mode	Admin and Configuration Mode.
Usage	Show the size of the files which are reserved in the system flash memory.
Example	To list the files and their size in the flash. <pre>Switch#show flash</pre>

total	12227K	
-rw-	12516553	nos.img
-rw-	3224	startup.cfg

Drive : flash:

Size:30.0M	Used:13.0M	Available:17.0M	Use:43%

show history

Command	show history
Parameter	none
Default	none
Mode	Admin Mode
Usage	Display the recent user command history. The system holds up to 20 commands the user entered, the user can use the UP/DOWN key or their equivalent (ctrl+p and ctrl+n) to access the command history.
Example	<pre>Switch# show history enable config interface ethernet 1/0/3 enable dir show ftp</pre>

show history all-users

Command	show history all-users [detail]
Parameter	detail shows user name of the executing command. IP address of the user will be shown when logging in the executing command through Telnet or SSH
Default	none
Mode	Admin and configuration mode
Usage	This command is used to show the recent command history of all users, including time, logging type, executing command, etc. Notice: The user can only check the command history of other users whose purview should not be higher than oneself.
Example	<pre>Switch# 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</pre>

```

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

```

show logging buffered

Command	show logging buffered [member<Member ID>] [level {critical warnings} range <begin-index> <end-index>]
Parameter	<Member ID> <1-8> level {critical warnings} level of critical information
	<begin-index> index start value of the log message, the valid range is 1-65535 <end-index> index end value of the log message, and the valid range is 1-65535. When only display logging buffered information of the line card must be added range parameter, but the main control has not the request
Default	No parameter specified indicates all the critical log information will be displayed.
Mode	Admin and configuration mode
Usage	This command displays the detailed information in the log buffer channel. This command is not supported on low end switches. Warning and critical log information is saved in the buffer zone. When displayed to the terminal, their display format should be: index ID time <level> module ID [mission name] log information.
Example	Display the critical log information in the log buffer zone channel and related to the main control with index ID between 940 and 946. <pre>Switch# show logging buffered level critical range 940 946</pre> Current messages in SDRAM:0

show logging executed-commands state

Command	show logging executed-commands state
Parameter	none
Default	none
Mode	Admin Mode
Usage	Use this command to display the state (enable or disable).
Example	<pre>Switch#show logging executed-commands state</pre> Logging executed command state is enable

show logging source

Command	show logging source mstp
Parameter	None
Default	None
Mode	Admin and configuration mode
Usage	Show the log information source of MSTP module.
Example	Show the log information source of MSTP. Switch#show logging source mstp system module log switch status: Channel Onoff Severity logbuff on warning loghost on warning terminal on warning

show running-config

Command	show running-config
Parameter	none
Default	None
Mode	Admin Mode
Usage	Display the current active configuration parameters for the switch. When the user finishes a set of configuration and needs to verify the configuration, show running-config command can be used to display the current active parameters. 。
Example	Switch#show running-config

show running-config current-mode

Command	show running-config current-mode
Parameter	none
Default	none
Mode	All configuration modes.
Usage	Enter into any configuration mode and input this command under this mode, it can show all the configurations under the current mode.
Example	Switch(config-if-ethernet1/0/1)#show run c ! Interface Ethernet1/0/1 switchport access vlan 2 !

show startup-config

Command	show startup-config [<WORD>]
Parameter	<WORD> startup configuration filename
Default	If the configuration parameters read from the Flash are the same as the default operating parameter, nothing will be displayed.
Mode	Admin Mode
Usage	The show running-config command differs from show startup-config in that when the user finishes a set of configurations, show running-config displays the added-on configurations whilst show startup-config won't display any configurations. However, if write command is executed to save the active configuration to the Flash memory, the displays of show running-config and show startup-config will be the same.
Example	Switch#show startup-config

show switchport interface

Command	show switchport interface [Ethernet port-channel] <IFNAME>
Parameter	<IFNAME> port number
Default	none
Mode	Admin and configuration mode
Usage	Show the VLAN port mode, VLAN number and Trunk port messages of the VLAN port mode on the switch.
Example	Show VLAN messages of port ethernet 1/0/1 Switch#show switchport interface ethernet 1/0/1 Ethernet1/0/1 Type :Universal Mode :Trunk Port VID :1 Trunk allowed Vlan :1-4094

Displayed Information	Description
Ethernet1/0/1	Corresponding interface number of the Ethernet.
Type	Current interface type.
Mode: Trunk	Current interface VLAN mode.
Port VID :1	Current VLAN number the interface belongs.
Trunk allowed Vlan : ALL	VLAN permitted by Trunk

show tcp

Command
Parameter
Default

show tcp

none

none

Mode
Usage
Example

Admin Mode

Display the current TCP connection status established to the switch.

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

Displayed information	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 status of the TCP connection.

show tcp ipv6

Command
Parameter

show tcp ipv6

none

Default

none

Mode
Usage

Admin and configuration mode

Show the current TCP connection.

Example

Switch#show tcp ipv6

LocalAddress	LocalPort	RemoteAddress
RemotePort State IF VRF		
::	80	::
0 LISTEN 0 0		
::	23	::
0 LISTEN 0 0		

Displayed Information	Explanation

LocalAddress	Local IPv6 address of TCP connection
LocalPort	Local port of TCP connection
RemoteAddress	Remote IPv6 address of TCP connection
RemotePort	Remote Port of TCP connection
State	The current state of TCP connection
IF	Local port index of TCP connection
VRF	Virtual route forward instance

show telnet login

Command	show telnet login
Parameter	none
Default	none
Mode	Admin and configuration mode
Usage	This command used to list the information of currently available telnet clients which are connected to the switch
Example	Switch#show telnet login Authenticate login by local. Login user: aa

show udp

Command	show udp				
Parameter	none				
Default	none				
Mode	Admin Mode				
Usage	Display the current UDP connection status established to the switch.				
Example	Switch#show udp				
	LocalAddress	LocalPort	ForeignAddress	ForeignPort	State
	0.0.0.0	32768	0.0.0.0	0	CLOSE
	0.0.0.0	3071	0.0.0.0	0	CLOSE
	Displayed Information		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 status of the UDP connection.

show udp ipv6

Command	show udp ipv6
Parameter	none
Default	none
Mode	Admin and configuration mode
Usage	Show the current UDP connection

Example	Switch#show udp ipv6
	LocalAddress LocalPort RemoteAddress
	RemotePort State
	:: 3071 ::
	0 CLOSE

Displayed Information	Description
LocalAddress	Local IPv6 address of the UDP connection.
LocalPort	Local port number of the UDP connection.
RemoteAddress	Remote IPv6 address of the UDP connection.
RemotePort	Remote port number of the UDP connection.
State	Current status of the UDP connection.

show version

Command	show version
Parameter	none
Default	none
Mode	Admin Mode

Usage	Display the switch version. Use this command to view the version information for the switch, including hardware version and software version.
Example	Switch#show version

Traceroute

Command	traceroute [<mpls> vrf<name>] [source <ipv4-addr>] { <ip-addr> host <hostname> } [hops <hops>] [timeout <timeout>]																																		
Parameter	traceroute ethernet [<target-mac> <target-mac value> <target-mep> <Target-mep mepid>] domain <WORD> service [<WORD1> <number> <pvlan>] source <source mepid> [<fdb-only>] ttl <ttl value> <table> <tr> <td><name></td><td>VPN Routing/Forwarding instance name</td></tr> <tr> <td><ipv4-addr></td><td>assigned source host IPv4 address in dot decimal format</td></tr> <tr> <td><ip-addr></td><td>target host IP address in dot decimal format</td></tr> <tr> <td><hostname></td><td>hostname for the remote host</td></tr> <tr> <td><hops></td><td>maximum gateway number allowed by Traceroute command 1-255</td></tr> <tr> <td><timeout></td><td>timeout value for test packets in milliseconds, between 100 - 10000</td></tr> <tr> <td><target-mac></td><td>target-mac</td></tr> <tr> <td><target-mac value></td><td>XX-XX-XX-XX-XX-XX</td></tr> <tr> <td><target-mep></td><td>target-mep</td></tr> <tr> <td><Target-mep mepid></td><td><1-4094></td></tr> <tr> <td><WORD></td><td>domain name</td></tr> <tr> <td><WORD1></td><td>Service name by string configuration</td></tr> <tr> <td><number></td><td>Service name by number</td></tr> <tr> <td><pvlan></td><td>Service name by primary vlan</td></tr> <tr> <td><source mepid></td><td><1-4094> Source mepid</td></tr> <tr> <td><fdb-only></td><td>only fdb</td></tr> <tr> <td><ttl value></td><td><1-255></td></tr> </table>	<name>	VPN Routing/Forwarding instance name	<ipv4-addr>	assigned source host IPv4 address in dot decimal format	<ip-addr>	target host IP address in dot decimal format	<hostname>	hostname for the remote host	<hops>	maximum gateway number allowed by Traceroute command 1-255	<timeout>	timeout value for test packets in milliseconds, between 100 - 10000	<target-mac>	target-mac	<target-mac value>	XX-XX-XX-XX-XX-XX	<target-mep>	target-mep	<Target-mep mepid>	<1-4094>	<WORD>	domain name	<WORD1>	Service name by string configuration	<number>	Service name by number	<pvlan>	Service name by primary vlan	<source mepid>	<1-4094> Source mepid	<fdb-only>	only fdb	<ttl value>	<1-255>
<name>	VPN Routing/Forwarding instance name																																		
<ipv4-addr>	assigned source host IPv4 address in dot decimal format																																		
<ip-addr>	target host IP address in dot decimal format																																		
<hostname>	hostname for the remote host																																		
<hops>	maximum gateway number allowed by Traceroute command 1-255																																		
<timeout>	timeout value for test packets in milliseconds, between 100 - 10000																																		
<target-mac>	target-mac																																		
<target-mac value>	XX-XX-XX-XX-XX-XX																																		
<target-mep>	target-mep																																		
<Target-mep mepid>	<1-4094>																																		
<WORD>	domain name																																		
<WORD1>	Service name by string configuration																																		
<number>	Service name by number																																		
<pvlan>	Service name by primary vlan																																		
<source mepid>	<1-4094> Source mepid																																		
<fdb-only>	only fdb																																		
<ttl value>	<1-255>																																		
Default	The default maximum gateway number is 30, timeout in 2000 ms.																																		
Mode	Admin mode																																		
Usage	This command is tests the gateway passed in the route of a packet from the source device to the target device. This can be used to test connectivity and locate a failed sector. Traceroute is usually used to locate the problem for unreachable network nodes.																																		
Example	Switch#traceroute 192.168.2.36 Type ^c to abort. Traceroute to host 192.168.2.36, maxhops is 30, timeout is 2000ms. 1 0ms 192.168.2.36																																		

Traceroute completed.

traceroute6

Command	traceroute6 [vrf < WORD>] [source <addr>] {<ipv6-addr> host <hostname>} [hops <hops>] [timeout <timeout>]	
Parameter	< WORD>	VPN Routing/Forwarding instance name
	<ipv4-addr>	assigned source host IPv6 address in colonned hex notation.
	<ip-addr>	IPv6 address of the destination host, shown in colonned hex notation
	<hostname>	name of the remote host
	<hops>	max number of the gateways the traceroute6 passed through, ranging between 1-255
	<timeout>	timeout period of the data packets, shown in millisecond and ranging between 100~10000
Default	Default number of the gateways passes by the data packets is 30, and timeout period is defaulted at 2000ms.	
Mode	Admin mode	
Usage	This command is for testing the gateways passed by the data packets from the source device to the destination device, so to check the accessibility of the network and further locating the network failure. Traceroute6 is normally used to locate destination network inaccessible failures.	
Example	Switch#traceroute6 2004:1:2:3::4 Type ^c to abort. Traceroute to IPv6 host 2004:1:2:3::4, maxhops is 30, timeout is 2000ms. Traceroute6 error occurred.	

reload

Command	reload <member ID>	
Parameter	<member ID>	<1-8>
Default	none	
Mode	Admin mode	
Usage	Reloads the specified member switch in a VSF stack. The member ID ranges from 1 to 8.	
Example	Prevent the switch to automatically reboot after the specified time. Switch#reload 1	

reload after

Command	reload after {[<HH:MM:SS>] [days <days>]}	
Parameter	<HH:MM:SS>	specified time, HH (hours) ranges from 0 to 23, MM (minutes) and SS (seconds) range from 0 to 59
	<days>	specified days, unit is day, range from 1 to 30.
Default	none	
Mode	Admin mode	
Usage	With this command, users can reboot the switch without shutdown its power after a specified period of time, usually when updating the switch version. The switch can be rebooted after a period of time instead of immediately after its version being updated successfully. This command will not be reserved, which means that it only has one-time effect. After this command is configured, it will prompt the reboot information when user logging in the switch by telnet.	
Example	Set the switch to automatically reload after 2 days, 10 hours and 1 second. Switch#reload after 10:00:01 days 2 Process with reboot after? [Y/N] y	

reload cancel

Command	reload cancel	
Parameter	none	
Default	none	
Mode	Admin mode	
Usage	Cancel the specified time period to reload the switch. With this command, users can cancel the specified time period to reload the switch, that is, to cancel the configuration of command "reload after". This command will not be reserved.	
Example	Prevent the switch to automatically reboot after the specified time. Switch#reload cancel Reload cancel successful.	

show reload

Command	show reload	
Parameter	none	
Default	none	
Mode	Admin and configuration mode	

Usage	Display the user's configuration of command "reload after". With this command, users can view the configuration of command "reload after" and check how long a time is left before rebooting the switch.
Example	View the configuration of command "reload after". In the following case, the user set the switch to be rebooted in 10 hours and 1 second, and there are still 9 hours 59 minutes and 48 seconds left before rebooting it. Switch#show reload The original reload after configuration is 10:00:01. System will be rebooted after 09:59:48 from now.

clear cpu-rx-stat protocol

Command	clear cpu-rx-stat protocol [<protocol-type>] all member <Member ID>	
Parameter	<protocol-type>	type of the protocol of the packet, , including dot1x, stp, snmp, arp, telnet, http, dhcp, igmp, ssh
	<Member ID>	<1-8>
Default	none	
Mode	Admin mode	
Usage	This command clear the statistics of the CPU received packets of the protocol type, it is supposed to be used with the help of the technical support.	
Example	Clear the statistics of the CPU receives ARP packets. Switch#config Switch(config)#clear cpu-rx-stat protocol arp	

cpu-rx-ratelimit protocol

Command	cpu-rx-ratelimit protocol <protocol-type> <packets> no cpu-rx-ratelimit protocol <protocol-type>	
Parameter	<protocol-type>	type of the protocol, including dot1x, stp, snmp, arp, telnet, http, dhcp, igmp, ssh
	<packets>	max rate of CPU receiving packets of the protocol type, its range is 125-6000 pps.
Default	A different default rate is set for the different type of protocol.	
Mode	Global mode	
Usage	Set the max rate of the CPU receiving packets of the protocol type, the no command set the max rate to default. The rate limit set by this command have an effect on CPU receiving packets, so it is supposed to be used with the help of the technical support.	
Example	set the rate of the ARP packets to 500pps. Switch#config	

```
Switch(config)#cpu-rx-ratelimit protocol arp 500
```

cpu-rx-ratelimit channel-rate

Command	cpu-rx-ratelimit channel-rate <Channel id> <Pps> no cpu-rx-ratelimit protocol < Channel id >	
Parameter	<Channel id>	0-16
	<Pps>	0-500
Default		
Mode	Global mode	
Usage	Sets the rate limit for CPU receive packets on a specified channel. The channel-rate option configures the limit in packets per second (PPS) for a given channel ID. The no form removes the rate limit configuration.	
Example	set the rate of the ARP packets to 500pps. Switch#config Switch(config)#cpu-rx-ratelimit channel-rate 10 10	

cpu-rx-ratelimit channel-skb-threshold

Command	cpu-rx-ratelimit channel-skb-threshold <Channel id> <Skb threshold> no cpu-rx-ratelimit channel-skb-threshold < Channel id >	
Parameter	<Channel id>	0-16
	<Pps>	0-100
Default		
Mode	Global mode	
Usage	Sets the SKB (socket buffer) threshold for CPU receive packet rate limiting on a specified channel. The no form removes the threshold configuration for the channel.	
Example	set the rate of the ARP packets to 500pps. Switch#config Switch(config)#cpu-rx-ratelimit channel-skb-threshold 10 10	

cpu-rx-ratelimit total

Command	cpu-rx-ratelimit total <packets> no cpu-rx-ratelimit total	
Parameter	<packets>	<125-50000> Pps(integer multiple of 125)
Default	1200pps	
Mode	Global mode	
Usage	Set the total rate of the CPU receiving packets, the no command sets the total rate of the CPU receiving packets to default. The total rate set by the command have an effect on CPU receiving packets, so it is supposed to be used with the help of the technical support.	
Example	Set the total rate of the CPU receive packets to 1500pps. Switch#config Switch(config)# cpu-rx-ratelimit total 1500	

show cpu-rx protocol

Command	show cpu-rx protocol [<WORD> all member <Member ID>]	
Parameter	<WORD>	protocol nameA
	<Member ID>	all protocol member<1-8>
Default	none	
Mode	Admin and configuration mode	
Usage	Show the statistics of the CPU received packets of the specified protocol type. This command is used to debug, it is supposed to be used with the help of the technical support.	
Example	Show the statistics of CPU receiving ARP packets. Switch#show cpu-rx protocol arp Type Rate-limit TotPkts DropPkts DelayCount CurState ARP 300 0 0 0 allowed	

15-Commands for Routing Protocol

1 Commands for RIP

accept-lifetime

Command	accept-lifetime <start-time> {<end-time> duration<seconds> infinite} no accept-lifetime
	Use this command to specify a key accept on the key chain as a valid time period. The "no accept-lifetime" command deletes this configuration.
Parameter	<start-time> parameter specifies the start time of the time period, of which the form should be: <start-time>={<hh:mm:ss> <month> <day> <year> <hh:mm:ss> <day> <month> <year>} <hh:mm:ss> specify the concrete valid time of accept-lifetime in hours, minutes and second <day> specifies the date of valid, ranging between 1 -31 <month> specifies the month of valid shown with the first three letters of the month, such as Jan <year> specifies the year of valid start, ranging between 1993 - 2035 <end-time> specifies the due of the time period, of which the form should be: <end-time>={<hh:mm:ss> <month> <day> <year> <hh:mm:ss> <day> <month> <year>}<hh:mm:ss> specify the concrete valid time of accept-lifetime in hours, minutes and second <day> specifies the date of valid, ranging between 1 -31 <month> specifies the month of valid shown with the first three letters of the month, such as Jan <year> specifies the year of valid start, ranging between 1993 - 2035 <seconds> the valid period of the key in seconds, ranging between 1-2147483646 Infinite means the key will never be out of date.
Default	No default configuration.
Mode	keychain-key Mode。
Usage Guide	If only the authentication mode is configured and the key chain or password used by the interface is not configured, authentication will not work at all. If the mode is not configured before configuring this command, the mode will be set to clear text authentication after configuring this command. The no operation of this command will cancel the authentication, but it does not mean that the mode will be set to the non-authentication type, only that the authentication processing will not be performed when sending or receiving packets. You can enter ip rip authentication key-chain my key to indicate that the key chain name is my key, which is 6 characters in total.
Example	The example below shows the accept-lifetime configuration of key 1 on the keychain 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
```

clear ip rip route

Command	clear ip rip route {<A.B.C.D/M> kernel static connected rip ospf isis bgp all}
Parameter	Clear specific route in the RIP route table. <A.B.C.D/M> Clear the routes which match the destination address from the RIP route table. Specifies the IP address prefix and its length of the destination address kernel delete kernel routes from the RIP route table static delete static routes from the RIP route table connected delete direct routes from the RIP route table rip only delete RIP routes from the RIP route table ospf only delete OSPF routes from the RIP route table isis only delete ISIS routes from the RIP route table bgp only delete BGP routes from the RIP route table all delete all routes from the RIP route table
Default	No default configuration
Mode	Admin mode
Usage Guide	Use this command with the all parameter will delete all learnt route in the RIP route which will be immediately recovered except for rip route. The dynamic learnt RIP route can only be recovered by studying one more time.
Example	<pre>Switch# clear ip rip route 10.0.0.0/8 Switch# clear ip rip route ospf</pre>

default-information originate

Command	default-information originate no default-information originate
Parameter	-
Default	Disabled
Mode	Router mode and address-family mode

Usage Guide	This command tells the router to insert the default route with the destination of 0.0.0.0 into the RIP routing database, and advertise the route as other routes.
Example	<pre>Switch# config terminal Switch(config)# router rip Switch(config-router)# default-information originate</pre>

default-metric

Command	default-metric <value> no default-metric
	Set the default metric value of the introduced route. The “ no default-metric ” command restores the default value to 1.
Parameter	<value> is the metric value to be set, ranging between 1~14.
Default	Default route metric value is 1.
Mode	Router mode and address-family mode。
Usage Guide	default-metric command is used for setting the default route metric value of the routes from other routing protocols when distributed into the RIP routes. When using the redistribute commands for introducing routes from other protocols, the default route metric value specified by default-metric will be adopted if no specific route metric value is set.
Example	Set the default route metric value to 3 for introducing routes from other routing protocols into the RIP routes. <pre>Switch(config-router)#default-metric 3</pre>

distance

Command	distance <number> [<A.B.C.D/M>] [<access-list-name access-list-number >] no distance [<A.B.C.D/M>]
	Set the managing distance with this command. The “ no distance [<A.B.C.D/M>] ” command restores the default value to 120.
Parameter	<number> specifies the distance value, ranging from 1 to 255. <A.B.C.D/M> specifies the network prefix and its length. <access-list-name access-list-number > specifies the access-list number or name applied.
Default	The default managing distance of RIP is 120.

Mode	Router mode and address-family mode。
Usage Guide	In case there are routes from two different routing protocols to the same destination, the managing distance is then used for selecting routes. The less the managing distance of the route protocol is, the more reliable will be the route acquired from the protocol.
Example	<pre>Switch# config terminal Switch(config)# router rip Switch(config-router)# distance 8 10.0.0.0/8 mylist</pre>

istribute-list

Command	istribute-list{<access-list-number access-list-name> prefix<prefix-list-name>} {in out} [<ifname> tunnel<tunnel interface number> vlan<vlan port number>] no distribute-list{<access-list-number access-list-name> prefix<prefix-list-name>} {in out} [<ifname> tunnel<tunnel interface number> vlan<vlan port number>] number>] This command uses access-list or prefix-list to filter the route update packets sent and received. The “no distribute-list {<access-list-number access-list-name> prefix<prefix-list-name>} {in out} [<ifname> tunnel<tunnel interface number> vlan<vlan port number>]” command cancels this route filter function.
Parameter	<access-list-number access-list-name> is the name or access-list number to be applied. <prefix-list-name> is the name of the prefix-list to be applied. <ifname> specifies the name of interface to be applied with route filtering. <tunnel interface number> <1-200> <vlan port number> <1-4094>
Default	The function in default situation is disabled.
Mode	Router mode and address-family mode。
Usage Guide	The filter will be applied to all the interfaces in case no specific interface is set.
Example	<pre>Switch# config terminal Switch(config)# router rip Switch(config-router)# distribute-list prefix myfilter in vlan 1</pre>

ip rip aggregate-address

Command	ip rip aggregate-address A.B.C.D/M no ip rip aggregate-address A.B.C.D/M

	To configure RIP aggregation route. The no form of this command will delete this configuration.
Parameter	A.B.C.D/M: IPv4 address and mask length.
Default	Disabled.
Mode	Router Mode or Interface Configuration Mode.
Usage Guide	If to configure aggregation route under router mode, RIP protocol must be enabled. If configured under interface configuration mode, RIP protocol may not be enabled, but the aggregation router can operation after the RIP protocol be enabled on interface.
Example	To configure aggregation route as 192.168.20.0/22 globally. Switch(config)#router rip Switch(config-router)#ip rip agg 192.168.20.0/22

ip rip authentication key-chain

Command	ip rip authentication key-chain <name-of-chain> no ip rip authentication key-chain
	Use this command to enable RIPv2 authentication on an interface and further configures the adopted key chain. The “ no ip rip authentication key-chain ” command cancels the authentication.
Parameter	<name-of-chain> is the name of the adopted key chain. There may be spaces in the string. The input ends with an enter and the string should not be longer than 256 bytes.
Default	Not configured.
Mode	Interface Configuration Mode.
Usage Guide	If the authentication is only configured without configuring the key chain or password used by the interface, the authentication does no effect. If mode has not been configured prior to configuring this command, the mode will be set to plaintext authentication. The “no ip rip authentication key” command will cancel the authentication which only cancels the authentication process when sending or receiving data packet other than set non authentication mode.
Example	Switch#config terminal Switch(config)# interface vlan 1 Switch(config-if-vlan1)# ip rip authentication key-chain my key

ip rip authentication mode

Command	ip rip authentication mode {text md5} no ip rip authentication mode {text md5}
Parameter	Configure the authentication mode; the “ no ip rip authentication mode {ext md5} ” command restores the default authentication mode namely text authentication mode. text means text authentication; md5 means MD5 authentication.
Default	Not configured authentication.
Mode	Interface Configuration Mode.
Usage Guide	RIP-I do not support authentication which the RIP-II supports two authentication modes: text authentication (i.e. Simple authentication) and data packet authentication (i.e. MD5 authentication). This command should be used associating the ip rip authentication key or ip rip authentication string. Independently configuration will not lead to authentication process.
Example	Switch#config terminal Switch(config)# interface vlan 1 Switch(config-if-vlan1)# ip rip authentication mode md5

ip rip authentication string

Command	ip rip authentication string <text> no ip rip authentication string
Parameter	Set the password used in RIP authentication. The “ no ip rip authentication string ” cancels the authentication. <text> is the password used in authentication of which the length should be 1-16 characters with space available. The password should end with enter.
Default	-
Mode	Interface mode
Usage Guide	The ip rip authentication key will not be able to be configured when this command is configured, key id value is required in MD5 authentication which is 1 when use this command. The mode will be set to plaintext authentication in case no mode configuration is available. The “no ip rip authentication string” command will cancel the

authentication which only cancels the authentication process when sending or receiving data packet other than set non authentication mode. Input ip rip authentication string aaa aaa to set the password as aaa aaa which is 7 characters.

Example	Switch# config terminal Switch(config)# interface vlan 1 Switch(config-if-vlan1)# ip rip authentication string guest

ip rip authentication cisco-compatible

Command	ip rip authentication cisco-compatible no ip rip authentication cisco-compatible
	After configured this command, the cisco RIP packets will be receivable by configuring the plaintext authentication or MD5 authentication
Parameter	-
Default	Not configured
Mode	Interface mode
Usage Guide	After authentication is configured on the cisco router, the RIP packets will exceeds the length of the defined standard length of the protocol once the number of route items is greater than 25. By configuring this command the over-lengthen RIP packets will be receivable other than denied.

Example	Switch# config terminal Switch(config)# interface vlan 1 Switch(config-if-vlan1)# ip rip authentication cisco-compatible

ip rip receive-packet

Command	ip rip receive-packet no ip rip receive-packet
	Set the interface to be able to receivable RIP packets; the “ no ip rip receive-packet ” command sets the interface to be unable to receivable RIP packets.
Parameter	-
Default	Interface receives RIP packets.
Mode	Interface Configuration Mode.
Usage Guide	-

Example	Switch# config terminal Switch(config)# interface vlan 1 Switch(config-if-vlan1)# ip rip receive-packet

ip rip receive version

Command	ip rip receive version { 1 2 1 2 } no ip rip receive version
	Set the version information of the RIP packets the interface receives. The default version is 2; the “ no ip rip receive version ” command restores the value set by using the version command.
Parameter	1 and 2 respectively stands for RIP version 1 and RIP version 2, 1 2 stands for the RIP versions 1, 2.
Default	Version 2.
Mode	Interface Configuration Mode.
Usage Guide	-
Example	Switch# config terminal Switch(config)# interface vlan 1 Switch(config-if-vlan1)# ip rip receive version 1 2

ip rip send-packet

Command	ip rip send-packet no ip rip send-packet
	Set the Interface to be able to receive the RIP packets; the “ no ip rip send-packet ” sets the interface to be unable to receive the RIP packets.
Parameter	-
Default	Interface sends RIP packets.
Mode	Interface Configuration Mode.
Usage Guide	-
Example	Switch# config terminal

```
Switch(config)# interface vlan 1
Switch(config-if-vlan1)# ip rip send-packet
```

ip rip send version

Command	ip rip send version { 1 2 1-compatible 1 2 } no ip rip send version
	Set the version information of the RIP packets the interface receives. The default version is 2; the “ no ip rip send version ” command restores the value set by using the version command.
Parameter	1 and 2 respectively stands for RIP version 1 and RIP version 2, 1 2 stands for the RIP versions 1, 2.
Default	Version 2.
Mode	Interface Configuration Mode.
Usage Guide	-
Example	Switch# config terminal Switch(config)# interface vlan 1 Switch(config-if-vlan1)# ip rip send version 1

ip rip split-horizon

Command	ip rip split-horizon [poisoned] no ip rip split-horizon
	Enable split horizon. The “ no ip rip split-horizon ” disables the split horizon.
Parameter	[poisoned] means configure the split horizon with poison reverse.
Default	Split Horizon with poison reverse by default.
Mode	Interface Configuration Mode.
Usage Guide	The split horizon is for preventing the Routing Loops, namely preventing the layer 3 switches from broadcasting the routes which is learnt from the same interface on which

the route to be broadcasted.

Example

```
Switch# config terminal
Switch(config)# interface vlan 1
Switch(Config-if-Vlan1)# ip rip split-horizon poisoned
```

key

Command

key <keyid>
no key <keyid>

This command is for managing and adding keys in the key chain. The “**no key <keyid>**” command deletes one key.

Parameter

<keyid> is key ID, ranging between 0-2147483647.

Default

-

Mode

keychainMode and keychain-keyMode。

Usage Guide

The command permits entering the keychain-key mode and set the passwords corresponding to the keys.

Example

```
Switch#config terminal
Switch(config)#key chain mychain
Switch(config-keychain)#key 1
Switch(config-keychain-key)#
```

key chain

Command

key chain <name-of-chain>
no key chain < name-of-chain >

This command is for entering a keychain manage mode and configure a keychain. The “**no key chain < name-of-chain >**” deletes one keychain.

Parameter

<name-of-chain> is the name string of the keychain the length of which is not specifically limited.

Default

-

Mode	Global Mode
Usage Guide	-
Example	Switch#config terminal Switch(config)#key chain mychain Switch(config-keychain)#

key-string

Command	key-string <text> no key-string <text>
	Configure a password corresponding to a key. The “ no key-string <text> ”command deletes the corresponding password.
Parameter	<text> is a character string without length limit. However when referred by RIP authentication only the first 16 characters will be used.
Default	-
Mode	keychain-key Mode。
Usage Guide	This command is for configure different passwords for keys with different ID.
Example	Switch# config terminal Switch(config)# key chain mychain Switch(config-keychain)# key 1 Switch(config-keychain-key)# key-string prime

maximum-prefix

Command	maximum-prefix <maximum-prefix> [<threshold>] no maximum-prefix
	Configure the maximum number of RIP routes in the route table. The “ nomaximum-prefix ” command cancels the limit.
Parameter	<maximum-prefix> the maximum number of RIP route, ranging between 1-216000; a warning is given when the number rate of current route exceeds <threshold> ranging between 1-100, default at 75.

Default	-
Mode	router mode
Usage Guide	The maximum RIP route only limits the number of routes learnt through RIP but not includes direct route or the RIP static route configured by the route command. The base on which the comparison is performed is the number of route marked R in the show ip route database, and also the number of RIP routes displayed in the show ip route statistics command.
Example	Switch# config terminal Switch(config)# router rip Switch(config-router)# maximum-prefix 150

neighbor

Command	neighbor <A.B.C.D> no neighbor <A.B.C.D>
	Specify the destination address requires targeted-peer sending. The “ no neighbor <A.B.C.D> ” command cancels the specified address and restores all gateways to trustable.
Parameter	<A.B.C.D> is the specified destination address for the sending, shown in dotted decimal notation.
Default	Not sending to any targeted-peer destination address.
Mode	router mode
Usage Guide	When used accompany with passive-interface command it can be configured to only sending routing messages to specific neighbor.
Example	Switch# config terminal Switch(config)# router rip Switch(config-router)# neighbor 1.1.1.1

network

Command	network <A.B.C.D/M> <ifname> loopback<loopback-ID> tunnel<Tunnel interface number> vlan<WORD> no network <A.B.C.C/M ifname>

Parameter	Configure the RIP protocol network.
	<A.B.C.D/M> is the IP address prefix and its length in the network.
	<ifname> is the name of a interface.
	<loopback-ID> <1-1024>
	<Tunnel interface number> <1-200>
	<WORD> Vlan IDs, use '-' or ',' or ';' to specify more than one
Default	Not running RIP protocol
Mode	Router mode and address-family mode。
Usage Guide	Use this command to configure the network for sending or receiving RIP update packets. If the network is not configured, all interfaces of the network will not be able to send or receive data packets.
Example	<pre>Switch# config terminal Switch(config)# router rip Switch(config-router)# network 10.0.0.0/8 Switch(config-router)# network vlan 1</pre>

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> tunnel<tunnel number> vlan<vlan port number>]
	Add an offset value to the metric value of the routes learnt by RIP. The “ no offset-list <access-list-number access-list-name> {in out} <number > [<ifname> tunnel<tunnel number> vlan<vlan port number>]” command disables this function.
Parameter	< access-list-number access-list-name> is the access-list or name to be applied <number > is the added offset value, ranging between 0-16; <ifname> is the specific interface name; <tunnel number> Tunnel interface number <vlan port number> 1-4094
Default	Default offset value is the metric value defined by the system.
Mode	Router mode and address-family mode。
Usage Guide	-
Example	<pre>Switch# config terminal Switch(config)# router rip Switch(config-router)# offset-list 1 in 5 vlan 1</pre>

passive-interface

Command	passive-interface <ifname> tunne<tunnel-number> vlan<WORD> no passive-interface <ifname> tunne<tunnel-number> vlan<WORD>
Parameter	Set the RIP layer 3 switch blocks RIP broadcast on specified interface, on which the RIP data packets will only be sent to layer 3 switches configured with neighbor. <ifname> is the name of specific interface. <tunnel-number> 1-200 <WORD> Vlan IDs, use '-' or ',' or ';' to specify more than one
Default	Not configured
Mode	router mode
Usage Guide	Suppresses RIP broadcast updates on specified interfaces. RIP packets will only be sent to configured neighbors. The no form removes this configuration.
Example	Switch# config terminal Switch(config)# router rip Switch(config-router)# passive-interface vlan 1

recv-buffer-size

Command	recv-buffer-size<size> no recv-buffer-size
Parameter	This command configures the size of UDP receiving buffer zone of RIP; the “no recv-buffer-size” command restores the system default. <size> is the buffer zone size in bytes, ranging between 8192-1000000000.
Default	8192 bytes.
Mode	router mode
Usage Guide	Configures the UDP receive buffer size for RIP in bytes.
Example	Switch# config terminal Switch(config)# router rip Switch(config-router)# recv-buffer-size 23456789

redistribute

Command	redistribute {kernel connected static ospf [<process-id>] (isis [<WORD> is-type <level-1> <level-1-2> <level-2>]) bgp} [metric<value>] [route-map<WORD2>] no redistribute {kernel connected static ospf [<process-id>] (isis [<WORD> is-type <level-1> <level-1-2> <level-2>]) bgp} [metric<value>] [route-map<word>]
Parameter	Introduce the routes learnt from other routing protocols into RIP. kernel introduce from kernel routes; connected introduce from direct routes; static introduce from static routes; ospf introduce from OSPF routes. process-id is OSPF process ID, if there is no parameter that means the process by default, range between 1 to 65535; isis introduce from ISIS routes; bgp introduce from BGP routes; <WORD> ISO routing area tag <level-1> IS-IS level-1 routes only <level-1-2> IS-IS level-1 and level-2 routes <level-2> IS-IS level-2 routes only <value> is the metric value assigned to the introduced route, ranging between 0 to 14; < WORD2> is the probe pointing to the route map for introducing routes.
Default	-
Mode	Router mode and address-family mode。
Usage Guide	Under the address-family mode, the parameter kernel and ISIS is unavailable.
Example	Switch#config terminal Switch(config)#router rip Switch(config-router)#redistribute kernel route-map ipi To redistribute OSPFv2 routing information to RIP. Switch(config)#router rip Switch(config-router)#redistribute ospf 2

route

Command	route <A.B.C.D/M> no route <A.B.C.D/M>
	This command configures a static RIP route. The “ no route <A.B.C.D/M> ” command deletes this route.
Parameter	<A.B.C.D/M> Specifies this destination IP address prefix and its length.
Default	-
Mode	router mode
Usage Guide	The command adds a static RIP route, and is mainly used for debugging. Routes configured by this command will not appear in kernel route table but in the RIP route database.
Example	Switch# config terminal Switch(config)# router rip Switch(config-router)# route 1.0.0.0/8

router rip

Command	router rip no router rip
	Enable the RIP routing process and enter the RIP mode; the “ no router rip ” command closes the RIP routing protocol.
Parameter	-
Default	Not running RIP route.
Mode	Global mode
Usage Guide	This command is the switch for starting the RIP routing protocol which is required to be open before configuring other RIP protocol commands.
Example	Enable the RIP protocol mode Switch(config)# router rip Switch(config-router)#

send-lifetime

Command	send-lifetime <start-time> {<end-time> duration<seconds> infinite} no send-lifetime
	Use this command to specify a key on the keychain as the time period of sending keys. The "no send-lifetime" cancels this configuration.
Parameter	<start-time> parameter specifies the starting time of the time period, which is: <start-time>={<hh:mm:ss> <month> <day> <year> <hh:mm:ss> <day> <month> <year>} <hh:mm:ss> Specify the concrete valid time of accept-lifetime in hours, minutes and second; <day> Specifies the date of valid, ranging between 1 -31; <month> Specifies the month of valid shown with the first three letters of the month, such as Jan; <year> Specifies the year of valid start, ranging between 1993 - 2035; <end-time> Specifies the due of the time period, of which the form should be: <end-time>={<hh:mm:ss> <month> <day> <year> <hh:mm:ss> <day> <month> <year>} <hh:mm:ss> Specify the concrete valid time of send-lifetime in hours, minutes and second; <seconds> is the valid period of the key in seconding and ranging between 1-2147483646; infinite means the key will never be out of date.
Default	No default configuration.
Mode	keychain-key Mode。
Usage Guide	If only the authentication mode is configured and the key chain or password used by the interface is not configured, authentication will not work at all. If the mode is not configured before configuring this command, the mode will be set to clear text authentication after configuring this command. The no operation of this command will cancel the authentication, but it does not mean that the mode will be set to the non-authentication type, only that the authentication processing will not be performed when sending or receiving packets. You can enter ip rip authentication key-chain my key to indicate that the key chain name is my key, which is 6 characters in total.
Example	The example below shows the send-lifetime configuration on the keychain named mychain for key 1. 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

timers basic

Command	timers basic <update> <invalid> <garbage> no timers basic
Parameter	Adjust the RIP timer update, timeout, and garbage collecting time. The “no timers basic” command restores each parameter to their default values. <update> time interval of sending update packet, shown in seconds and ranging between 5-2147483647; <invalid> time period after which the RIP route is advertised dead, shown in seconds and ranging between 5-2147483647; <garbage> is the hold time in which the a route remains in the routing table after advertised dead, shown in seconds and ranging between 5-2147483647.
Default	<update> defaulted at 30; <invalid> defaulted at 180; <garbage> defaulted at 120
Mode	router mode
Usage Guide	The system is defaulted broadcasting RIPvng update packets every 30 seconds; and the route is considered invalid after 180 seconds but still exists for another 120 seconds before it is deleted from the routing table.
Example	Set the RIP update time to 20 seconds and the timeout period to 80 second, the garbage collecting time to 60 seconds. <pre>Switch(Config-Router)#timers basic 20 80 60</pre>

version

Command	version {1 2} no version
Parameter	Configure the version of all RIP data packets sent/received by router interfaces: the “no version” restores the default configuration. 1 is version 1 rip; 2 is version 2 rip.
Default	Sent and received data packet is version 2 by default.
Mode	Router mode and address-family mode。
Usage Guide	1 refers to that each interface of the layer 3 switch only sends/receives the RIP-I data packets. 2 refers to that each interface of the layer 3 switch only sends/receives the RIP-II data packets. The RIP-II data packet is the default version.

Example	Configure the version of all RIP data packets sent/received by router interfaces to version 2. Switch(config-router)#version 2

show ip protocols rip

Command	show ip protocols rip
Parameter	Show the RIP process parameter and statistics information. -
Default	-
Mode	Any mode.
Usage Guide	-

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 Displayed information Explanation Sending updates every 30 seconds with +/-50%, next due in 8 seconds Sending update every 30 secs Timeout after 180 seconds, garbage collect after 120 seconds The route time-out event period is 180 secs, the garbage collect time is 120 seconds Outgoing update filter list for all interface is not set Outgoing update filter list for all interface is not set Incoming update filter list for all interface is not set Incoming update filter list for all interface is not set Default redistribution metric is 1 Default redistribution metric is 1 Redistributing: static Redistributing the static route into the RIP	

	route
Default version control: send version 2, receive version 2	The configuration of interface receiving and sending packets. Receive version is 2, keychain 1 not configured.
Interface Send Recv Key-chain Ethernet1/3 2 2	
Routing for Networks: Vlan1 Vlan2	The segment running RIP is the Vlan 1 and Vlan 2
Routing Information Sources: Gateway Distance Last Update BadPackets Bad Routes 20.1.1.1 120 00:00:31 0 0 Distance: (default is 120)	Routing information sourcesThe badpacketand bad routes from the gateway 20.1.1.1 are all 0. 31 seconds have passed since the last route update. The manage distance is 120 Default manage distance is 120

show ip rip

Command	show ip rip
Parameter	Show the routes in the RIP route data base.
Default	-
Mode	Any mode.
Usage Guide	-
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 Amongst R stands for RIP route, namely a RIP route with the destination network address 12.1.1.0, the network prefix length as 24, next-hop address at 20.1.1.1. It is learnt from the Ethernet port E1/3 with a metric value of 2, and still has 2 minutes 51 seconds before time out.

show ip rip database

Command	show ip rip database [vrf <WORD>]
	show the routes in the RIP route database.
Parameter	<WORD> VRF name
Default	-
Mode	Any mode.
Usage Guide	Displays all routes in the RIP routing database. The vrf option shows routes for a specific VRF instance.
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

show ip rip interface

Command	show ip rip interface [vrf <WORD>] [<ifname> vlan<Vlan port number>]
	Show the RIP related messages.
Parameter	<WORD> VRF name <ifname> Interface name <Vlan port number> 1-4094
Default	-
Mode	Any mode.
Usage Guide	Displays RIP routing information for specified interfaces. The command can show RIP status for a specific VRF, interface name, or VLAN port. If no parameter is specified, it displays RIP information for all RIP-enabled interfaces.
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

show ip rip aggregate

Command show ip rip aggregate

To display the information of IPv4 aggregation route.

Parameter

-

Default

-

Mode

Admin and Configuration Mode.

Usage Guide

This command is used to display which interface the aggregation route be configured, Metric, Count, Suppress and so on. If configured under global mode, then the interface display "----", "Metric" is metric. "Count" is the number of learned aggregation routes. "Suppress" is the times of aggregation.

Example

To display the information of IPv4 aggregation route.

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

Displayed information

Explanation

Network

Route prefix and prefix length.

Aggregated

To configure the interface name of the aggregation route. If the route aggregated globally, then display "----".

Ifname

Metric

Metric of aggregation route.

Count

The number of learned aggregation route.

Suppress

The times of aggregated for aggregation route.

show ip rip redistribute

Command show ip rip redistribute [vrf <NAME>]

Parameter	To display the routing information introduced from external process of RIP.
	<NAME> VPN Routing/Forwarding instance name
Default	Not shown by default.
Mode	Admin Mode and Configuration Mode.
Usage Guide	-
Example	Switch#show ip rip redistribute

debug rip

Command	debug rip [events nsm packet[recv send][detail]] all mib] no debug rip [events nsm packet[recv send][detail]] all]
	Open various RIP adjustment switches and show various adjustment debugging messages. The “no debug rip [events nsm packet[recv send][detail]] all]” command closes corresponding debugging switch.
Parameter	events shows the debugging messages of RIP events nsm shows the communication messages between RIP and NSM packet shows the debugging messages of RIP data packets recv shows the messages of the received data packets send shows the messages of the sent data packets detail shows the messages of received or sent data packets mib shows the messages of the rip mib
Default	Debug switch closed.
Mode	Admin mode and global mode
Usage Guide	-
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

debug rip redistribute route receive

Command	debug rip redistribute route receive no debug rip redistribute route receive
	To enable debugging of received messages from NSM for RIP. The no form of this

	command will disable debugging of received messages from NSM for RIP.
Parameter	-
Default	Close the debug by default.
Mode	Admin mode
Usage Guide	-
Example	Switch#debug rip redistribute route receive Switch#no debug rip redistribute route receive

debug rip redistribute message send

Command	debug rip redistribute message send no debug rip redistribute message send
	To enable the debugging of sending messages for routing redistribution messages from OSPF process or BGP protocol for RIP. The no form of this command will disable the debugging messages.
Parameter	-
Default	Close the debug by default.
Mode	Admin mode
Usage Guide	-
Example	Switch#debug rip redistribute message send Switch#no debug rip redistribute message send

rip restart grace-period

Command	rip restart grace-period <1-65535> no rip restart grace-period
	When the RIP process restarts, the neighboring routers need to retain the RIP routes learned from this device for the maximum duration. If the device fails to complete the restart and re-establish the RIP neighbor relationship with the neighboring routers within the set time, the neighbors will timeout and delete these routes, and the data forwarding on the device may also be interrupted.
Parameter	<1-65535> seconds
Default	The debugging switch has been turned off.

Mode	Config mode
Usage Guide	-
Example	Switch(config)#rip restart grace-period 50 Switch(config)#no rip restart grace-period

2 Commands for OSPF

area authentication

Command	area <id> authentication [message-digest] no area <id> authentication
Parameter	Configure the authentication mode of the OSPF area; the “ no area <id> authentication ” command restores the default value. <id> is the area number which could be shown in digit, ranging from 0 to 4294967295, or in IP address message-digest is proved by MD5 authentication, or be proved by simple plaintext authentication if not choose this parameter.
Default	No authentication.
Mode	OSPF protocol mode
Usage Guide	Set the authentication mode to plaintext authentication or MD5 authentication. The authentication mode is also configurable under interface mode of which the priority is higher than those in the area. It is required to use ip ospf authentication-key to set the password while no authentication mode configured at the interface and the area is plaintext authentication, and use ip ospf message-digest key command to configure MD5 key if is MD5 authentication. The area authentication mode could not affect the authentication mode of the interface in this area.
Example	Set the authentication mode in area 0 to MD5. Switch(config-router)#area 0 authentication message-digest

area default-cost

Command	area <id> default-cost <cost> no area <id> default-cost
	Configure the cost of sending to the default summary route in stub or NSSA area; the

Parameter	“no area <id> default-cost” command restores the default value.
	<id> is the area number which could be shown as digits 0 ~ 4294967295, or as an IP address; <cost> ranges between <0-16777215>
Default	Default OSPF cost is 1.
Mode	OSPF protocol mode
Usage Guide	The command is only adaptive to the ABR router connected to the stub area or NSSA area.
Example	Set the default-cost of area 1 to 10. Switch(config-router)#area 1 default-cost 10

area filter-list

Command	[no] area <id> filter-list {access prefix } <name> {in out}
Parameter	Configure the filter broadcasting summary routing on the ABR; the “no area <id> filter-list {access prefix} {in out}” command restores the default value.
	<id> is the area number which could be shown in digits ranging between 0 ~ 4294967295, or as an IP address; access-list is appointed for use in access, so is prefix-list for prefix; <name> Name of an IP prefix-list or Name of an access-list
Default	No filter configured.
Mode	OSPF protocol mode
Usage Guide	This command is used for restraining routes from specific area from spreading between this area and other areas.
Example	Set a filter on the area 1. Switch(config)#access-list 1 deny 172.22.0.0 0.0.0.255 Switch(config)#access-list 1 permit any-source Switch(config)#router ospf 100 Switch(config-router)#area 1 filter-list access 1 in

area nssa

Command	area <id> nssa [TRANSLATOR] no-redistribution [DEFAULT-ORIGINATE no-summary] no area <id> nssa[TRANSLATOR] no-redistribution [DEFAULT-ORIGINATE no-

summary]

Parameter	Set the area to Not-So-Stubby-Area (NSSA) area.
	<id> is the area number which could be digits ranging between 0~4294967295, and also as an IP address. TRANSLATOR = translator-role {candidate never always} , specifies the LSA translation mode for routes: candidate means if the router is elected translator, Type 7 LSA can be translated to Type-5 LSA, the default is candidate . never means the router will never translate Type 7 LSA to Type 5 LSA. always means the route always translate Type 7 LSA to Type 5 LSA. no-redistribution means never distribute external-LSA to NSSA. DEFAULT-ORIGINATE=default-information-originate [metric <0-16777214>] [metric-type <1-2>] , generate the Type-7 LSA. metric <0-16777214> specifies the metric value. metric-type <1-2> specifies the metric value type of external-LSA, default value is 2. no-summary shows not injecting area route to the NSSA.
Default	No NSSA area defined by default.
Mode	OSPF protocol mode
Usage Guide	The same area can not be both NSSA and stub at the same time.
Example	Set area 3 to 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

area range

Command	area <id> range <address> [advertise not-advertise substitute cost <value>] no area <id> range <address>
Parameter	Aggregate OSPF route on the area border. The “ no area <id> range <address> ” cancels this function. <id> is the area number which could be digits ranging between 0 ~ 4294967295, and also as an IP address.; <address>=<A.B.C.D/M> , specifies the area network prefix and its length.; advertise : Advertise this area, which is the default; not-advertise : Not advertise this area;

substitute= substitute <A.B.C.D/M>: advertise this area as another prefix;
cost <value>: Set cost , <1-16777214> 24-bit cost value
<A.B.C.D/M>: Replace the network prefix to be advertised in this area.

Default	Not set.
Mode	OSPF protocol mode
Usage Guide	Use this command to aggregate routes inside an area. If the network IDs in this area are not configured continuously, a summary route can be advertised by configuring this command on ABR. This route consists of all single networks belong to specific range.

Example

```
Switch # config terminal
Switch (config)# router ospf 100
Switch (config-router)# area 1 range 192.16.0.0/24
```

area stub

Command	area <id> stub [no-summary] no area <id> stub [no-summary]
Parameter	Define an area to a stub area. The “ no area <id> stub [no-summary] ” command cancels this function. <id> is the area number which could be digits ranging between 0 ~ 4294967295, and also as an IP address; no-summary: The area border routes stop sending link summary announcement to the stub area.

Default	Not defined.
Mode	OSPF protocol mode
Usage Guide	Configure area stub on all routes in the stub area. There are two configuration commands for the routers in the stub area: stub and default-cost. All routers connected to the stub area should be configured with area stub command. As for area border routers connected to the stub area, their introducing cost is defined with area default-cost command.

Example

```
Switch # config terminal
Switch (config)# router ospf 100
Switch (config-router)# area 1 stub
```

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]

Configure a logical link between two backbone areas physically divided by non-backbone area. The “**no area <id> virtual-link A.B.C.D [AUTHENTICATION | AUTH_KEY | INTERVAL]**” command removes this virtual-link.

Parameter	<id> is the area number which could be digits ranging between 0 ~ 4294967295, and also as an IP address. AUTHENTICATION = authentication [message-digest[message-digest-key <1-255> md5 <LINE>] null AUTH_KEY]. authentication : Enable authentication on this virtual link. message-digest: Authentication with MD-5. null : Overwrite password or packet summary with null authentication. AUTH_KEY= authentication-key <key>. <key>: A password consists of less 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 seconds, ranging between 1~3600. <dead-interval>: A neighbor is considered offline for certain dead interval without its group messages which the default is 40 seconds. <hello-interval>: The time interval before the router sends a hello group message, default is 10 seconds. <message-digest-key>: Authentication key with MD-5. <retransmit-interval>: The time interval before a router retransmitting a group message, default is 5 seconds. <transmit-delay>: The time delay before a router sending a group messages, default is 1 second.
Default	No default configuration.
Mode	OSPF protocol mode
Usage Guide	In the OSPF all non-backbone areas will be connected to a backbone area. If the connection to the backbone area is lost, virtual link will repair this connection. You can configure virtual link between any two backbone area routers connected with the public non-backbone area. The protocol treat routers connected by virtual links as a point-to-point network.
Example	<pre>Switch#config terminal Switch(config) #router ospf 100 Switch(config-router) #area 1 virtual-link 10.10.11.50 hello 5 dead 20</pre>

auto-cost reference-bandwidth

Command	auto-cost reference-bandwidth <bandwidth> no auto-cost reference-bandwidth
This command sets the way in which OSPF calculate the default metric value. The “no	

auto-cost reference-bandwidth" command only configures the cost to the interface by types.

Parameter	<bandwidth> : reference bandwidth in Mbps, ranging between 1~4294967.
Default	Default bandwidth is 100Mbps.
Mode	OSPF protocol mode
Usage Guide	The interface metric value is acquired by divide the interface bandwidth with reference bandwidth. This command is mainly for differentiate high bandwidth links. If several high bandwidth links exist, their cost can be assorted by configuring a larger reference bandwidth value.
Example	Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#auto-cost reference-bandwidth 50

compatible rfc1583

Command	compatible rfc1583 no compatible rfc1583
	This command configures to rfc1583 compatible. The " no compatible rfc1583 " command close the compatibility.
Parameter	-
Default	Rfc 2328 compatible by default.
Mode	OSPF protocol mode
Usage Guide	-
Example	Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#compatible rfc1583

clear ip ospf process

Command	clear ip ospf [<process-id>] process

Use this command to clear and restart OSPF routing processes. One certain OSPF process will be cleared by specifying the process ID, or else all OSPF processes will be cleared.

Parameter	-
Default	No default configuration.
Mode	Admin mode。
Usage Guide	-
Example	Switch#clear ip ospf process

default-information originate

Command	default-information originate [always METRIC METRICTYPE ROUTEMAP] no default-information originate
Parameter	This command create a default external route to OSPF route area; the “no default-information originate” closes this feature. always: Whether default route exist in the software or not, the default route is always advertised. METRIC = metric <value>: Set the metric value for creating default route, <value> ranges between 0~16777214, default metric value is 0. METRICTYPE = metric-type {1 2}set the OSPF external link type of default route. 1 Set the OSPF external type 1 metric value. 2 Set the OSPF external type 2 metric value. ROUTEMAP = route-map <WORD> <WORD> specifies the route map name to be applied.
Default	Default metric value is 10; default OSPF external link type is 2.
Mode	OSPF protocol mode
Usage Guide	When introducing route into OSPF route area with this command, the system will behaves like 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

default-metric

Command	default-metric <value> no default-metric
	The command set the default metric value of OSPF routing protocol; the “ no default-metric ” returns to the default state.
Parameter	<value> , metric value, ranging between 0~16777214.
Default	Built-in, metric value auto translating.
Mode	OSPF protocol mode
Usage Guide	When the default metric value makes the metric value not compatible, the route introducing still goes through. If the metric value can not be translated, the default value provides alternative option to carry the route introducing on. This command will result in that all introduced route will use the same metric value. This command should be used associating redistribute.
Example	Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#default-metric 100

distance

Command	distance {<value> ROUTEPARAMETER} no distance ospf
	Configure OSPF manage distance base on route type. The “ no distance ospf ” command restores the default value.
Parameter	<value> , OSPF routing manage distance, ranging between 1~255 ROUTEPARAMETER= ospf {ROUTE1 ROUTE2 ROUTE3} ROUTE1= external <external-distance> , Configure the distance learnt from other routing area. <external-distance> distance value, ranging between 1~255. ROUTE2= inter-area <inter-distance> , configure the distance value from one area to another area. <inter-distance> manage distance value, ranging between 1~255. ROUTE3= intra-area <intra-distance> Configure all distance values in one area. <intra-distance> Manage distance value, ranging between 1~255.
Default	Default distance value is 110.
Mode	OSPF protocol mode
Usage Guide	Manage distance shows the reliability of the routing message source. The distance value

may range between 1~255. The larger the manage distance value is, the lower is its reliability.

Example

```
Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#distance ospf inter-area 20 intra-area 10 external 40
```

istribute-list

Command

```
istribute-list prefix <access-list-name> {in (<IFNAME> | vlan <vlan-value>)} |
{out (kernel |connected| static| rip| isis| bgp)}
istribute-list <WORD> {in (<IFNAME> | vlan <vlan-value>)} | {out (kernel
|connected| static| rip| isis| bgp)}
istribute-list <gateway> <WORD1> in {<IFNAME> | vlan <vlan-value>}
istribute-list <route-map> <WORD2> in {<IFNAME> | vlan <vlan-value>}
```

```
no istribute-list prefix <access-list-name> {in (<IFNAME> | vlan <vlan-value>)} |
{out (kernel |connected| static| rip| isis| bgp)}
no istribute-list <WORD> {in (<IFNAME> | vlan <vlan-value>)} | {out (kernel
|connected| static| rip| isis| bgp)}
no istribute-list <gateway> <WORD1> in {<IFNAME> | vlan <vlan-value>}
no istribute-list <route-map> <WORD2> in {<IFNAME> | vlan <vlan-value>}
```

Parameter

< access-list-name> is the access-list name to be applied.

out: filter the sent route update.

kernel kernel route.

connected direct route;

static static route;

rip RIP route;

isis ISIS route;

bgp BGP route.

<WORD> access-list name

<IFNAME> interface name

<vlan-value> <1-4094>Vlan port number

<gateway> filter incoming updates based on gateway

<WORD1> prefix-list name

<route-map> route map reference

<WORD2> Pointer to route-map entries

Default

No default configuration.

Mode

OSPF protocol mode

Usage Guide

When distributing route from other routing protocols into the OSPF routing table, we can use this command.

Example

Example below is the advertisement based on the access-list list 1 of the BGP route.

```
Switch#config terminal
Switch(config)#access-list 11 permit 172.10.0.0 0.0.255.255
Switch(config)#router ospf 100
Switch(config-router)#redistribute rip
Switch(config-router)#distribute-list 1 out rip
```

host area

Command	host <host-address> area <area-id> <ip-address> [cost <cost>] no host <host-address> area <area-id> <ip-address> [cost <cost>]
Parameter	Use this command to set a stub host entire belongs to certain area. The “[no] host <host-address> area <area-id> [cost <cost>]” command cancels this configuration. <host-address> is host IP address show in dotted decimal notation. <area-id> area ID shown in dotted decimal notation or integer ranging between 0~4294967295. <ip-address> OSPF area ID in IP address format <cost> specifies the entire cost, which is a integer ranging between 0~65535 and defaulted at 0.
Default	No entire set.
Mode	OSPF protocol mode
Usage Guide	With this command you can advertise certain specific host route out as stub link. Since the stub host belongs to special router in which setting host is not important.
Example	<pre>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</pre>

ip ospf authentication

Command	ip ospf [<ip-address>] authentication [message-digest null key-chain <LINE>] no ip ospf [<ip-address>] authentication
Parameter	Specify the authentication mode required in sending and receiving OSPF packets on the interfaces; the “no ip ospf [<ip-address>] authentication” command cancels the authentication. <ip-address> is the interface IP address, shown in dotted decimal notation. message-digest: Use MD5 authentication. null: no authentication applied, which resets the password or MD5 authentication

	applied on the interface. < LINE > name of key-chain
Default	Authentication not required in receiving OSPF packets on the interface.
Mode	Interface Configuration Mode.
Usage Guide	-
Example	Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf authentication message-digest

ip ospf authentication-key

Command	ip ospf authentication-key [0 <WORD1> 7 <WORD2> <WORD3>] no ip ospf authentication-key
	Specify the authentication key required in sending and receiving OSPF packet on the interface; the no command cancels the authentication key.
Parameter	<WORD1> The UNENCRYPTED user key (1--8 character(s)) <WORD2> The UNENCRYPTED user key (16 character(s)) <WORD3> The OSPF password key (1--8 character(s))
Default	Authentication not required in receiving OSPF packets on the interface.
Mode	Interface Configuration Mode.
Usage Guide	Sets the OSPF authentication key for the interface. The key can be specified as plain text (0) or encrypted type 7 (7). The no form removes the authentication key.
Example	Switch#config terminal Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)# ip ospf authentication-key 0 1 Switch(Config-if-Vlan1)# no ip ospf authentication-key

ip ospf cost

Command	ip ospf [<ip-address>] cost <cost> no ip ospf [<ip-address>] cost
	Specify the cost required in running OSPF protocol on the interface; the “ no ip ospf [<ip-address>] cost ” command restores the default value.
Parameter	<ip-address> is the interface IP address shown in dotted decimal notation.

<cost > is the cost of OSPF protocol ranging between 1~65535.

Default Default OSPF cost on the interface is auto-figure out based bandwidth.

Mode Interface Configuration Mode.

Usage Guide -

Example Switch#config terminal
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#ip ospf cost 3

ip ospf database-filter

Command ip ospf [<ip-address>] database-filter all out
no ip ospf [<ip-address>] database-filter

The command opens LSA database filter switch on specific interface; the “**no ip ospf [<ip-address>] database-filter**” command closes the filter switch.

Parameter **<ip-address>** is the interface IP address shown in dotted decimal notation;
all: All LSAs.
out: Sent LSAs.

Default Filter switch Closed.

Mode Interface Configuration Mode.

Usage Guide -

Example Switch#config terminal
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#ip ospf database-filter all out

ip ospf dead-interval

Command ip ospf [<ip-address>] dead-interval <time >
no ip ospf [<ip-address>] dead-interval

Specify the dead interval for neighboring layer 3 switch; the “**no ip ospf [<ip-address>] dead-interval**” command restores the default value.

Parameter **<ip-address>** is the interface IP address shown in dotted decimal notation;
<time > is the dead interval length of the neighboring layer 3 switches, shown in seconds and ranging between 1~235926000.

Default	The default dead interval is 40 seconds (normally 4 times of the hello-interval).
Mode	Interface Configuration Mode.
Usage Guide	If no Hello data packet received after the dead-interval period then this layer 3 switch is considered inaccessible and invalid. This command modifies the deadinterval value of neighboring layer 3 switch according to the actual link state. The set dead-interval value is written into the Hello packet and transmitted. To ensure the normal operation of the OSPF protocol, the dead-interval between adjacent layer 3 switches should be in accordance or at least 4 times of the hello-interval value.
Example	Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf dead-interval 80

ip ospf disable all

Command	ip ospf disable all no ip ospf disable all
Parameter	Stop OSPF group process on the interface. -
Default	-。
Mode	Interface Configuration Mode.
Usage Guide	This command resets the network area command and stops group process on specific interface.
Example	Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf disable all

ip ospf hello-interval

Command	ip ospf [<ip-address>] hello-interval <time> no ip ospf [<ip-address>] hello-interval
Parameter	Specify the hello-interval on the interface; the “no ip ospf [<ip-address>] hello-interval” restores the default value. <ip-address> is the interface IP address shown in dotted decimal notation; <time> is the interval sending HELLO packet, shown in seconds and ranging between

Default	The hello-interval on the interface is 10 seconds.
Mode	Interface Configuration Mode.
Usage Guide	HELLO data packet is the most common packet which is periodically sent to adjacent layer 3 switch to discover and maintain adjacent relationship, elect DR and BDR. The user set hello-interval value will be written into the HELLO packet and transmitted. The less the hello-interval value is, the sooner the network topological structure is discovered as well larger the cost. To ensure the normal operation of OSPF protocol the hello-interval parameter between the layer 3 switches adjacent to the interface must be in accordance.

Example	Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf hello-interval 20

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>
Parameter	Specify the key id and value of MD5 authentication on the interface; the no command restores the default value. <ip-address> is the interface IP address show in dotted decimal notation; <key_id> ranges between 1-255; <LINE> is OSPF key. If key option is 0, specify plaintext key. If key option is 7, specify encrypted string. If no option, specify plaintext key by default.
Default	MD5 key is not configured.
Mode	Interface Configuration Mode.
Usage Guide	MD5 key encrypted authentication is used to ensure the safety between the OSPF routers on the network. Same key id and key should be configured between neighbors when using this command, or else no adjacent relationship will not be created.
Example	Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf message-digest-key 2 MD5 0 yourpassword

ip ospf mtu

Command	ip ospf mtu <mtu> no ip ospf mtu
	Specify the mtu value of the interface as the OSPF group structure according; the “no ip ospf mtu” command restores the default value.
Parameter	<mtu > is the interface mtu value ranging between 576~65535
Default	Use the interface mtu acquired from the kernel.
Mode	Interface Configuration Mode.
Usage Guide	The interface value configured by this command is only used by OSPF protocol other than updated into kernel.
Example	Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf mtu 1480

ip ospf mtu-ignore

Command	ip ospf <ip-address> mtu-ignore no ip ospf <ip-address> mtu-ignore
	Use this command so that the mtu size is not checked when switching DD; the “ no ip ospf <ip-address> mtu-ignore ” will ensure the mtu size check when performing DD switch.
Parameter	<ip-address> is the interface IP address show in dotted decimal notation.
Default	Check mtu size in DD switch.
Mode	Interface Configuration Mode.
Usage Guide	-
Example	Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf mtu-ignore

ip ospf network

Command	ip ospf network {broadcast non-broadcast point-to-point point-to-multipoint} no ip ospf network
Parameter	This command configures the OSPF network type of the interface; the “no ip ospf network” command restores the default value. broadcast: Set the OSPF network type to broadcast. non-broadcast: Set the OSPF network type to NBMA. point-to-point: Set the OSPF network type to point-to-point. point-to-multipoint: Set the OSPF network type to point-to-multipoint.
Default	The default OSPF network type is broadcast.
Mode	Interface Configuration Mode.
Usage Guide	-
Example	The configuration below set the OSPF network type of the interface vlan 1 to point-to-point. <pre>Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf network point-to-point</pre>

ip ospf priority

Command	ip ospf [<ip-address>] priority <priority> no ip ospf [<ip-address>] priority
Parameter	Configure the priority when electing “Defined layer 3 switch” at the interface. The “no ip ospf [<ip-address>] priority” command restores the default value. <ip-address> is the interface IP address show in dotted decimal notation. <priority> is the priority of which the valid value ranges between 0 ~ 255.
Default	The default priority when electing DR is 1.
Mode	Interface Configuration Mode.
Usage Guide	When two layer 3 switches connected to the same segments both want to be the “Defined layer 3 switch”, the priority will decide which one should be chosen. Normally the one with higher priority will be elected, or the one with larger router-id number if the priorities are the same. A layer 3 switch with a priority equal to 0 will not be elected as “Defined layer 3 switch” or “Backup Defined layer 3 switch”.
Example	Configure the priority of DR electing. Configure the interface vlan 1 to no election right,

namely set the priority to 0.
Switch#config terminal
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#ip ospf priority 0

ip ospf retransmit-interval

Command	ip ospf [<ip-address>] retransmit-interval <time> no ip ospf [<ip-address>] retransmit-interval
Parameter	Specify the retransmit interval of link state announcements between the interface and adjacent layer 3 switches. The “no ip ospf [<ip-address>] retransmit-interval” command restores the default value. <ip-address> is the interface IP address shown in dotted decimal notation. <time> is the retransmit interval of link state announcements between the interface and adjacent layer 3 switches, shown in seconds and ranging between 1 ~ 3600.
Default	Default retransmit interval is 5 seconds.
Mode	Interface Configuration Mode.
Usage Guide	When a layer 3 switch transmits LSA to its neighbor, it will maintain the link state announcements till confirm from the object side is received. If the confirm packet is not received within the interval, the LSA will be retransmitted. The retransmit interval must be larger than the time it takes to make a round between two layer 3 switches.
Example	Configure the LSA retransmit interval of interface vlan 1 to 10 seconds. <pre>Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf retransmit-interval 10</pre>

ip ospf transmit-delay

Command	ip ospf [<ip-address>] transmit-delay <time> no ip ospf [<ip-address>] transmit-delay
Parameter	Set the transmit delay value of LSA transmitting; the “no ip ospf [<ip-address>] transmit-delay” restores the default value. <ip-address> is the interface IP address shown in dotted decimal notation. <time> is the transmit delay value of link state announcements between the interface and adjacent layer 3 switches, shown in seconds and ranging between 1 ~ 3600.
Default	Default transmit delay value of link state announcements is 1 second.

Mode	Interface Configuration Mode.
Usage Guide	The LSA ages with time in the layer 3 switches, but not in the network transmitting process. By adding the transit-delay prior to sending the LSA, the LSA will be sent before aged.
Example	Set the LSA transmit delay of interface vlan1 to 3 seconds. Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf transmit-delay 3

ispf enable

Command	ispf enable no ispf enable
Parameter	Enable or disable the ISPF incremental algorithm. -
Default	Default to disabling the ISPF incremental algorithm
Mode	OSPF Protocol Configuration Mode
Usage Guide	After enabling the ISPF incremental algorithm, when the OSPF network topology changes, a local incremental SPF calculation will be performed.
Example	Switch#config terminal Switch(config)#router ospf 1 Switch(config-if-vlan1)#ispf enable

key

Command	key <keyid> no key <keyid>
Parameter	This command is for managing and adding keys in the key chain. The “ no key <keyid> ” command deletes one key. <keyid> is key ID, ranging between 0-2147483647.
Default	-。
Mode	keychainMode and keychain-keyMode。

Usage Guide	The command permits entering the keychain-key mode and set the passwords corresponding to the keys.
Example	<pre>Switch#config terminal Switch(config)#key chain mychain Switch(config-keychain)#key 1 Switch(config-keychain-key)#</pre>

key chain

Command	key chain <name-of-chain> no key chain < name-of-chain >
Parameter	This command is for entering a keychain manage mode and configure a keychain. The “no key chain < name-of-chain >” command deletes one keychain. <name-of-chain> is the name string of the keychain the length of which is not specifically limited.
Default	-。
Mode	Global Mode and keychain Mode。
Usage Guide	-
Example	<pre>Switch#config terminal Switch(config)#key chain mychain Switch(config-keychain)#</pre>

log-adjacency-changes detail

Command	log-adjacency-changes detail no log-adjacency-changes detail
Parameter	Configure to keep a log for OSPF adjacency changes or not. -
Default	Don't I keep a log for OSPF adjacency changes by default.
Mode	OSPF Protocol Configuration Mode
Usage Guide	When this command is configured, the OSPF adjacency changes information will be recorded into a log.
Example	<pre>Switch#config terminal</pre>

```
Switch(config)#router ospf 100
Switch(config-router)# log-adjacency-changes detail
```

max-concurrent-dd

Command	max-concurrent-dd <value> no max-concurrent-dd
Parameter	This command set the maximum concurrent number of dd in the OSPF process; the “no max-concurrent-dd” command restores the default. <value> ranges between <1-65535>, which is the capacity of processing the concurrent dd data packet.
Default	Not set, no concurrent dd limit.
Mode	OSPF protocol mode
Usage Guide	Specify the max concurrent number of dd in the OSPF process.
Example	Set the max concurrent dd to 20. <pre>Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#max-concurrent-dd 20</pre>

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>]
Parameter	This command configures the OSPF router connecting NBMA network. The “no neighbor A.B.C.D [<cost> priority <value> poll-interval <value>]” command removes this configuration. <cost>, OSPF neighbor cost value ranging between 1-65535; priority <value>, neighbor priority defaulted at 0 and ranges between 0-255; poll-interval <value>, 120s by default, which the polling time before neighbor relationship come into shape, ranging between 1-65535.
Default	No default configuration.
Mode	OSPF protocol mode
Usage Guide	Use this command on NBMA network to configure neighbor manually. Every known non-broadcasting neighbor router should be configured with a neighbor entry. The configured neighbor address should be the main address of the interface. The poll-

interval should be much larger 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
```

network area

Command

network NETWORKADDRESS area <area-id>
no network NETWORKADDRESS area <area-id>

This command enables OSPF routing function on the interface with IP address matched with the network address. The “**no network NETWORKADDRESS area <area-id>**” command removes the configuration and stop OSPF on corresponding interface.

Parameter

NETWORKADDRESS = A.B.C.D/M | A.B.C.D X.Y.Z.W, Shown with the network address prefix or the mask. Wildcast mask if shown in mask;
<area-id> is the ip address or area number shown in point divided decimal system, if shown in decimal integer, it ranges between 0~4294967295.

Default

No default configuration

Mode

OSPF protocol mode

Usage Guide

When certain segment belongs to certain area, interface the segment belongs will be in this area, starting hello and database interaction with the connected neighbor.

Example

```
Configuration 10.1.1.0/24 is in area 1.
Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#network 10.1.1.0/24 area 1
```

ospf abr-type

Command

ospf abr-type {cisco|ibm|shortcut|standard}
no ospf abr-type

Use this command to configure an OSPF ABR type. The “**no ospf abr-type**” command restores the default value.

Parameter

cisco , Realize through cisco ABR;
ibm , Realize through ibm ABR;
shortcut , Specify a shortcut-ABR;
standard , Realize with standard(RFC2328)ABR.

Default	Cisco by default.
Mode	OSPF protocol mode
Usage Guide	For Specifying the realizing type of abr. This command is good for interactive operation among different OSPF realizing method and is especially useful in the multiple host environment.
Example	Configure abr as standard. Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#ospf abr-type standard

ospf router-id

Command	ospf router-id <address> no ospf router-id
	Specify a router ID for the OSPF process. The “ no ospf router-id ” command cancels the ID number.
Parameter	<address> , IPv4 address format of router-id.
Default	No default configuration
Mode	OSPF protocol mode
Usage Guide	The new router-id takes effect immediately.
Example	Configure router-id of ospf 100 to 2.3.4.5. Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#ospf router-id 2.3.4.5

overflow database

Command	overflow database <maxdbsize > [{hard soft}] no overflow database
	This command is for configuring the max LSA number. The “no overflow database” command cancels the limit.
Parameter	< maxdbsize > Max LSA numbers, ranging between 0~4294967294. soft : Soft limit, warns when border exceeded. hard : Hard limit, directly close ospf instance when border exceeded. If there is not soft or hard configured, the configuration is taken as hard limit.

Default	Not configured
Mode	OSPF protocol mode
Usage Guide	-
Example	<pre>Switch#config terminal Switch(config)#router ospf Switch(config-router)#overflow database 10000 soft</pre>

overflow database external

Command	overflow database external [<maxdbsize> <maxtime>] no overflow database external [<maxdbsize> <maxtime>]
Parameter	The command is for configuring the size of external link database and the waiting time before the route exits overflow state. The “no overflow database external [<maxdbsize> <maxtime>]” restores the default value. < maxdbsize > size of external link database, ranging between 0~2147483647, defaulted at 4294967294. < maxtime > the seconds the router has to wait before exiting the database overflow, ranging between 0~65535.
Default	Configures the maximum number of external LSAs allowed in the OSPF link-state database and the timeout period before the router exits the overflow state. The no form restores the default values.
Mode	OSPF protocol mode
Usage Guide	-
Example	<pre>Switch#config terminal Switch(config)#router ospf Switch(config-router)#overflow database external 5 3</pre>

passive-interface

Command	passive-interface [vlan <WORD> <IFNAME>] <ip-address> passive-interface <default> no passive-interface [vlan <WORD> <IFNAME>] <ip-address> no passive-interface <default>
Parameter	Configure that the hello group not sent on specific interfaces. <WORD> Vlan port number <IFNAME> Vlan IDs, use '-' or ',' or ';' to specify more than one <ip-address> Address of interface

<default>	Suppress routing updates on all interfaces

Default	Not configured
Mode	OSPF protocol mode
Usage Guide	Suppresses OSPF hello packets on specified interfaces to prevent adjacencies from forming. The default option applies this to all interfaces. The no form removes the configuration.
Example	Switch#config terminal Switch(config)#router ospf Switch(config-router)#passive-interface vlan1

redistribute

Command	redistribute {kernel connected static rip bgp isis [<WORD>] is-type <level-1 level-1-2 level-2>} [metric<value> metric-type {1 2} route-map <word> tag <tag-value>] no redistribute {kernel connected static rip bgp isis [<WORD>] is-type <level-1 level-1-2 level-2>} [metric<value> metric-type {1 2} route-map <word> tag <tag-value>]
Parameter	Introduce route learnt from other routing protocols into OSPF. kernel introduce from kernel route. connected introduce from direct route. static introduce from static route. rip introduce from the RIP route. bgp introduce from BGP route. isis introduce from ISIS route. <WORD> ISO routing area tag is-type level of IS-IS level-1 IS-IS level-1 routes only level-1-2 IS-IS level-1 and level-2 routes level-2 IS-IS level-2 routes only metric <value> is the introduced metric value, ranging between 0-16777214. metric-type {1 2} is the metric value type of the introduced external route, which can be 1 or 2, and it is 2 by default. route-map <word> point to the probe of the route map for introducing route. tag<tag-value> external identification number of the external route, ranging between 0~4294967295, defaulted at 0.
Default	-
Mode	OSPF protocol mode

Usage Guide	Learn and introduce other routing protocol into OSPF area to generate AS-external_LSAs.
Example	<pre>Switch#config terminal Switch(config)#router ospf Switch(config-router)#redistribute bgp metric 12</pre>

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>]		
	To redistribute of process ID routing to this process. The no form of command deletes the redistribution of process ID routing to this process. When input the optional parameters of metric, metric type and routemap, then restores default configuration.		
Parameter	process-id	<1-65535>	is OSPF process ID, 0 by default.
	metric <value>	<0-16777214>	is the metric for redistributed routing, range between 0 to 16777214.
	metric-type {1 2}		Set OSPF External Type 1/2 metrics
	route-map <word>		Pointer to route-map entries
Default	Not redistributed any OSPF routing by default.		
Mode	OSPF protocol mode		
Usage Guide	When process-id is not input, that means OSPF routing will be redistributed by default (Process-id is 0).		
Example	Switch(config-router)#redistribute ospf		

router ospf

Command	router ospf <process_id> no router ospf <process_id>		
Parameter	This command is for relating the OSPF process. <table> <tr> <td><process_id></td><td>specifies the ID of the OSPF process to be created, the ranging from 1 to 65535.</td></tr> </table>	<process_id>	specifies the ID of the OSPF process to be created, the ranging from 1 to 65535.
<process_id>	specifies the ID of the OSPF process to be created, the ranging from 1 to 65535.		
Default	-		

Mode	OSPF protocol mode
Usage Guide	-
Example	Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#network 10.1.1.0/24 area 0

refresh timer

Command	refresh timer <timer-value> no refresh timer <timer-value>
Parameter	Set the OSPF refresh timer. <timer-value> Timer refresh time, value range is 10 to 1800, in seconds. The default value is 1800.
Default	-
Mode	OSPF protocol mode
Usage Guide	-
Example	Switch#config Switch(config)# Switch(config)#router ospf 1 Switch(config-router)#refresh timer ? <10-1800> Timer value in seconds Switch(config-router)#refresh timer 20 Switch(config-router)#

summary-address

Command	summary-address <A.B.C.D/M> [cost <1-16777214> not-advertise tag <tag-value>]
Parameter	Summarize or restrain external route with specific address scope. <A.B.C.D/M> address scope, shown in dotted decimal notation IPv4 address plus mask length.

<1-16777214>	24-bit cost value
not-advertised	restrain the external routes.
tag<tag-value>	is the identification label of the external routes, which ranges between 0~4294967295, and is defaulted at 0.

Default	-
Mode	OSPF protocol mode
Usage Guide	When routes are introduced into OSPF from other routing protocols, it is required to advertise every route in a external LSA. This command is for advertise one summary route for those introduced routes contained in specific network address and masks, which could greatly reduces 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

timers

Command	timers spf <spf-delay> <spf-holdtime> timers lsa arrival <WORD> timers throttle [lsa <WORD1> spf <WORD2>] no timers [spf lsa arrival throttle <lsa spf>]		
	Adjust the value of the route calculating timer. The " no timers spf " command restores relevant values to default.		
Parameter	<spf-delay>	<0-4294967295>	Delay between receiving a change to SPF calculation in seconds, 5 seconds by default.
	<spf-holdtime>	<0-4294967295>	Hold time between consecutive SPF calculations in seconds, 10 seconds by default.
	<WORD>	<0-600000>	Minimum Delay in acceptance of same LSA in milliseconds
	<WORD1>	<0-600000>	Starting Delay for LSA Generation calculation in milliseconds
	<WORD2>	<1-600000>	Delay between receiving a change to SPF calculation in milliseconds
Default	-		
Mode	OSPF protocol mode		
Usage Guide			
Example	Switch#config terminal Switch(config)#router ospf		

Switch(config-router)#timers spf 5 10

show ip ospf

Command	show ip ospf [<process-id>]
Parameter	Display OSPF main messages. <process-id> is the process ID, ranging between 0~65535.
Default	Not displayed
Mode	Admin and Configuration Mode.
Usage Guide	-
Example	Switch#show ip ospf Routing Process "ospf 0" with ID 192.168.1.1 Process bound to VRF default 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

show ip ospf border-routers

Command	show ip ospf [<process-id>] border-routers
	Display the intra-domain route entries for the switch to reach ABR and ASBR of all instances.
Parameter	<process-id> is the process ID, ranging between 0~65535.
Default	Not displayed
Mode	Admin and Configuration Mode.
Usage Guide	-
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

show ip ospf database

Command	<pre>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>}] external [{<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 }</pre>
Parameter	Display the OSPF link state data base messages. <process-id> is the process ID, ranging between 0~65535 <linkstate_id> Link state ID, shown in point divided demical system <advertiser_router> is the ID of Advertising router, shown in point divided demcial IP address forma
Default	Not displayed
Mode	Admin and Configuration Mode.
Usage Guide	According to the output messages of this command, we can view the OSPF link state database messages.
Example	<pre>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 0x800000031 0xec21 1 192.168.1.3 192.168.1.3 236 0x800000033 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 0x80000002b 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 0x80000002b 0x5757 6.1.0.0/22 6.1.1.0 192.168.1.2 879 0x80000002a 0xf8bc 6.1.1.0/24 22.1.1.0 192.168.1.2 308 0x80000000c 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 0x80000002a 0x89c7</pre>

```

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]

```

show ip ospf interface

Command	show ip ospf interface [<IFNAME> vlan <1-4094>]	
	Display the OSPF interface messages.	
Parameter	<IFNAME>	interface name
	<1-4094>	vlan port number
Default	Not displayed	
Mode	Admin and Configuration Mode.	
Usage Guide	-	
Example	<pre> 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 </pre>	

show ip ospf ispf status

Command	show ip ospf ispf status	
	Display the incremental algorithm execution status of ISPF for each area of the OSPF instance.	
Parameter	-	
Default	Not Displayed	
Mode	Admin and Configuration Mode.	

Usage Guide	-
Example	<pre>Switch#show ip ospf ispf status OSPF process 1: Incremental SPF Status: Enable Hold Timer: 5 secs Area 0 Total iSPF Runs: 1 (Last runtime: 0.002784 secs) ISPF Last time: 2025-06-16 19:07:36</pre>

show ip ospf neighbor

Command	show ip ospf [<process-id>] neighbor [{<neighbor_id> all detail all] [interface<ifaddress>}]														
Parameter	Display the OSPF adjacent point messages. <process-id> is the process ID ranging between 0~65535 <neighbor_id> is the dotted decimal notation neighbor ID all: Display messages of all neighbors detail: Display detailed messages of all neighbors <ifaddress> Interface IP address														
Default	Not displayed														
Mode	Admin and Configuration Mode.														
Usage Guide	OSPF neighbor state can be checked by viewing the output of this command.														
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 <table><tr><td>Displayed information</td><td>Explanation</td></tr><tr><td>Neighbor ID</td><td>ID Neighbor ID</td></tr><tr><td>Priority</td><td>Priority</td></tr><tr><td>State</td><td>Neighbor relation state</td></tr><tr><td>Dead time</td><td>Neighbor dead time</td></tr><tr><td>Address</td><td>Interface Address</td></tr><tr><td>Interface</td><td>Interface name</td></tr></table>	Displayed information	Explanation	Neighbor ID	ID Neighbor ID	Priority	Priority	State	Neighbor relation state	Dead time	Neighbor dead time	Address	Interface Address	Interface	Interface name
Displayed information	Explanation														
Neighbor ID	ID Neighbor ID														
Priority	Priority														
State	Neighbor relation state														
Dead time	Neighbor dead time														
Address	Interface Address														
Interface	Interface name														

show ip ospf redistribute

Command	show ip ospf [<process-id>] redistribute
Parameter	To display the routing message redistributed from external process of OSPF. <process-id> is the process ID ranging between 0~65535.
Default	-
Mode	Admin Mode and Configuration Mode.
Usage Guide	-
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

show ip ospf route

Command	show ip ospf {route [process-id (<route> <fast-reroute>)]}
Parameter	Display the OSPF routing table messages. <process-id> is the process ID ranging between 0~65535
Default	-
Mode	Admin and Configuration Mode.
Usage Guide	-
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

```

show ip ospf virtual-links

Command	show ip ospf [<process-id>] virtual-links
Parameter	Display the OSPF virtual link message. <process-id> is the process ID ranging between 0~65535.
Default	-
Mode	Admin and Configuration Mode.
Usage Guide	-
Example	<pre> 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 </pre>

show ip route process-detail

Command	show ip route [database] process-detail
Parameter	Display the IP routing table with specific process ID or Tag. The parameter of database means displaying all the routers, no parameter means only displaying effective routers.
Default	Not importing any router of OSPF process by default.
Mode	Admin and Configuration Mode.
Usage Guide	-
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

show ip protocols

Command	show ip protocols
Parameter	Display the running routing protocol messages.
Default	-
Mode	Admin and Configuration Mode.
Usage Guide	-
Example	Switch#show ip protocols Use "show ip protocols" command will show the messages of the routing protocol running on current layer 3 switch For example, the displayed messages are: 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:

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]
Parameter	Open debugging switches showing various OSPF events messages; the “no debug ospf events [abr asbr lsa nssa os router vlink]” command closes the debugging switch. -
Default	Closed.
Mode	Admin and global mode
Usage Guide	-
Example	Switch#debug ospf events router

debug ospf ifsm

Command	debug ospf ifsm [status events timers] no debug ospf ifsm [status events timers]
	To enable debugging of received messages from NSM for RIP. The no form of this command will disable debugging of received messages from NSM for RIP.

Parameter	-
Default	Closed.
Mode	Admin mode and global mode
Usage Guide	-
Example	Switch#debug ospf ifsm events

debug ospf lsa

Command	debug ospf lsa [generate flooding install maxage refresh] no debug ospf lsa [generate flooding install maxage refresh]
	Open debugging switches showing showing link state announcements; the “ no debug ospf lsa [generate flooding install maxage refresh] ” closes the debugging switches.
Parameter	-
Default	Closed.
Mode	Admin mode and global mode
Usage Guide	-
Example	Switch#debug ospf lsa generate

debug ospf nfsm

Command	debug ospf nfsm [status events timers] no debug ospf nfsm [status events timers]
	Open debugging switches showing OSPF neighbor state machine; the “ no debug ospf nfsm [status events timers] ” command closes this debugging switch.
Parameter	-
Default	Closed.
Mode	Admin mode and global mode

Usage Guide	-
Example	Switch#debug ospf nsm events
debug ospf nsm	
Command	debug ospf nsm [interface redistribute] no debug ospf nsm [interface redistribute]
	Open debugging switches showing OSPF NSM, the “ no debug ospf nsm [interface redistribute] ” command closes this debugging switch.
Parameter	-
Default	Closed.
Mode	Admin mode and global mode
Usage Guide	-
Example	Switch#debug ospf nsm interface

debug ospf packet

Command	debug ospf packet [dd detail hello ls-ack ls-request ls-update rcv] no debug ospf packet [dd detail hello ls-ack ls-request ls-update rcv]	
	Open debugging switches showing OSPF packet messages; the “ no debug ospf packet [dd detail hello ls-ack ls-request ls-update rcv] ” command closes this debugging switch.	
Parameter	dd detail hello ls-ack ls-request ls-update rcv send	OSPF Database Description Detail information OSPF Hello OSPF Link State Acknowledgment OSPF Link State Request OSPF Link State Update Packet received Packet sent

Default	Closed.
Mode	Admin mode and global mode
Usage Guide	Enables debugging of OSPF packet messages for specified packet types. Supported options include dd (Database Description), hello (Hello packets), ls-ack (Link State Acknowledgment), ls-request (Link State Request), ls-update (Link State Update), rcv (received packets), send (sent packets), and detail (verbose information). If no option is specified, all packet types are debugged. The no form disables the specified debugging.
Example	Switch#debug ospf packet hello

debug ospf route

Command	debug ospf route [ase ia install spf] no debug ospf route [ase ia install spf]
Parameter	Open debugging switches showing OSPF related routes; the “ no debug ospf route [ase ia install spf] ” command closes this debugging switch.
Default	Closed.
Mode	Admin mode and global mode
Usage Guide	-
Example	Switch#debug ospf route spf

debug ospf redistribute message send

Command	debug ospf redistribute message send no debug ospf redistribute message send

To enable debugging of sending command from OSPF process redistributed to other OSPF process routing. The no form of command disables debugging of sending command from OSPF process redistributed to other OSPF process routing.

Parameter	-
Default	Disabled.
Mode	Admin Mode
Usage Guide	-
Example	To enable debugging of sending command from OSPF process redistributed to other OSPF process routing. Switch#debug ospf redistribute message send

debug ospf redistribute route receive

Command	debug ospf redistribute route receive no debug ospf redistribute route receive
	To enable/disable debugging switch of received routing message from NSM for OSPF process.
Parameter	-
Default	Disabled.
Mode	Admin Mode
Usage Guide	-
Example	To enable debugging switch of received routing message from NSM for OSPF process. Switch# debug ospf redistribute route receive

capability

Command	capability [<cspf> <te> <vrf-lite>] no capability [<cspf> <te> <vrf-lite>]

	Enable GR of specified OSPF process, no command disables this function.
Parameter	<csf> Constrained Shortest Path First <te> OSPF Traffic Engineering extension <vrf-lite> VRF-lite
Default	Enable OSRF GR function.
Mode	OSPF protocol configuration mode
Usage Guide	Enables OSPF capabilities for the specified feature. The csf option enables Constrained Shortest Path First computation. The te option enables OSPF Traffic Engineering extensions. The vrf-lite option enables VRF-lite support. The no form disables the specified capability.
Example	Enable OSPF GR function. Switch(config)#router ospf Switch(config-router)#capability csf

debug ospf events gr

Command	debug ospf events gr no debug ospf events gr
	Enable the debugging for displaying relevant event of OSPF GR, no command disables the debugging.
Parameter	-
Default	Disabled.
Mode	Admin Mode
Usage Guide	-
Example	Enable the debugging for displaying relevant event of OSPF GR. Switch#debug ospf events gr

3 Commands for BGP

aggregate-address

Command	aggregate-address <ip-address/M> [summary-only] [as-set]

no aggregate-address <ip-address/M> [summary-only] [as-set]

Configure the aggregate-address. The "**no aggregate-address <ip-address/M> [summary-only] [as-set]**" command deletes the aggregate-address.

Parameter	<ip-address/M> : IP address, length of mask. [summary-only] : Send summary only ignoring specific route. [as-set] : Show AS on the path in list, each AS is shown once.
Default	No aggregate configuration.
Command Mode	BGP route mode
Usage Guide	Address aggregation reduces spreading routing messages outside. Use summary-only option so to spread aggregate route to the neighbors without spreading specific route. as-set option will list AS from each route covered by the aggregation only once without repeat.
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

bgp aggregate-nexthop-check

Command	bgp aggregate-nexthop-check no bgp aggregate-nexthop-check
	Configures whether BGP checks all the route next-hop in aggregating. The " no bgp aggregate-nexthop-check " command cancels this configuration, namely not check the next-hop accordance of aggregate route.
Parameter	-
Default	No nexthop checked during aggregating.
Command Mode	Global mode
Usage Guide	When check is enabled, the aggregate will not be performed if the next-hop of the covered routes are not in accordance. When checking is disabled, all covered route will be aggregated into the aggregate route.
Example	Switch(config)#bgp aggregate-nexthop-check

bgp always-compare-med

Command	bgp always-compare-med no bgp always-compare-med
	Configures If MED comparison is always performed. The “ no bgp always-compare-med ” command cancels this configuration.
Parameter	-
Default	-
Command Mode	BGP route mode
Usage Guide	Normally the BGP compares the MED only when the AS is the same. By using this configuration, MED of routes from different AS source will also be compared.
Example	The AS (200) receives the same route prefix form the two AS (100 and 300) carrying different MED, configure the MED comparison is always performed. Switch(config-router)#bgp always-compare-med

bgp asnotation asdot

Command	bgp asnotation asdot no bgp asnotation asdot
	Show AS number and match the regular expression with ASDOT method. The no command cancels this method.
Parameter	-
Default	ASPLAIN method.
Command Mode	BGP route mode
Usage Guide	To change the method that show AS number and match the regular expression, it must configure “clear ip bgp *” to rebuild all BGP neighbor relationships after this command is configured.
Example	Show AS number and match the regular expression with ASDOT method. Switch(config)#router bgp 200 Switch(config-router)#bgp asnotation asdot

bgp bestpath as-path ignore

Command	bgp bestpath as-path ignore no bgp bestpath as-path ignore
	Set to ignore the AS-PATH length. The “ no bgp bestpath as-path ignore ” command cancels this configuration.
Parameter	-
Default	-
Command Mode	BGP route mode
Usage Guide	Length of AS-PATH will be compared in BGP pathing, and its length can be ignored by using this configuration.
Example	Set to ignore the AS-PATH length: Switch(config)#router bgp 200 Switch(config-router)#bgp bestpath as-path ignore

bgp bestpath compare-confed-aspath

Command	bgp bestpath compare-confed-aspath no bgp bestpath compare-confed-aspath
	Set to concern the confederation AS-PATH length. The “ no bgp bestpath compare-confed-aspath ” command cancels this configuration.
Parameter	-
Default	-
Command Mode	BGP route mode
Usage Guide	Normally only the length of external AS-PATH will be compared in BGP pathing. By using this configuration, lengths of AS inner confederation AS-PATH will be compared at the same time.
Example	Configure confederation AS-PATH length. Switch(config-router)#bgp bestpath compare-confed-aspath

bgp bestpath compare-routerid

Command	bgp bestpath compare-routerid no bgp bestpath compare-routerid
Parameter	Compare route ID; the “ no bgp bestpath compare-routerid ” command cancels this configuration.
Default	-
Command Mode	BGP route mode
Usage Guide	Normally the first arrived route from the same AS (with other conditions equal) will be chosen as the best route. By using this command, source router ID will also be compared.
Example	Device (10.1.1.66, AS200) receives the same route prefix from two devices (10.1.1.64 and 10.1.1.68) of the same AS (100), configure the device to compare route ID. Switch(config-router)#bgp bestpath compare-routerid

bgp bestpath med

Command	bgp bestpath med {[confed] [missing-as-worst]} no bgp bestpath med {[confed] [missing-as-worst]}
Parameter	Configure to compare the MED attributes in the confederation path and to consider the value is the largest when MED is unavailable . The “ no bgp bestpath med {[confed] [missing-as-worst]} ” command cancels this configuration.
Default	-
Command Mode	BGP route mode
Usage Guide	Choose whether MED is compared among confederations by this command. If MED is missing, it is considered max when missing-is-worst or else 0.
Example	Configure to compare the MED attributes in the confederation path and to consider the value is the largest when MED is unavailable.

bgp client-to-client reflection

Command	bgp client-to-client reflection no bgp client-to-client reflection
	Configures whether the route reflection is performed. The “ no bgp client-to-client reflection ” cancels this configuration.
Parameter	-
Default	Reflection defaulted when client is configured.
Command Mode	BGP route mode
Usage Guide	After configured reflection client with neighbor {<ip-address> <WORD>} route-reflector-client, the router performs routing reflection in default condition. The NO form of this command cancels the route reflection among CLIENT, (reflection among Clients and non-CLIENT is not disturbed).
Example	Configure to cancel the route reflection. Switch(config-router)#no bgp client-to-client reflection

bgp cluster-id

Command	bgp cluster-id {<ip-address> <01-4294967295>} no bgp cluster-id {<[<ip-address>] <0-4294967295>}
	Configure the route reflection ID during the route reflection. The “ no bgp cluster-id {<[<ip-address>] <0-4294967295>} ” command cancels this configuration.
Parameter	<ip-address> <1-4294967295> : cluster-id which is shown in dotted decimal notation or a 32 digit number.
Default	-
Command Mode	BGP route mode
Usage Guide	A cluster consists of one routing reflector and its clients in an area. However in order to increase the redundancy level, sometime more than one routing reflectors may be deployed in one area. Router-id is for identifying the router exclusively in an area, and

cluster-id is required for two or more reflector identification.

Example	Configure the route reflection cluster-id is 1.1.1.1. Switch(config-router)#bgp cluster-id 1.1.1.1

bgp confederation identifier

Command	bgp confederation identifier <as-id> no bgp confederation identifier [<as-id>]
	Create a confederation configuration. The “ no bgp confederation identifier [<as-id>] ” command deletes a confederation.
Parameter	<as-id> : ID number of the confederation AS, ranging from 1 to 4294967295, it can be shown in decimal notation (such as 6553700) or delimiter method (such as 100.100).
Default	-
Command Mode	BGP route mode
Usage Guide	Confederation is for divide large AS into several smaller AS, while still identified as the large AS. Create large AS number with this command.

Example	Switch(config-router)# bgp confederation identifier 600

bgp confederation peers

Command	bgp confederation peers <as-id> [<as-id>..] no bgp confederation peers <as-id> [<as-id>..]
	Add/delete one or several AS to a confederation.
Parameter	<as-id> : ID numbers of the AS included in the confederation, ranging from 1 to 4294967295, it can be shown in decimal notation (such as 6553700) or delimiter method (such as 100.100), which could be multiple.
Default	-
Command Mode	BGP route mode

Usage Guide	Confederation is for divide large AS into several smaller AS, while still identified as the large AS. Use this command to add/delete confederation members.
Example	Create a confederation, ID is 600, add 100, 200, 100.300 members. Switch(config-router)# bgp confederation identifier 600 Switch(config-router)#bgp confederation peers 100 200 100.300

bgp dampening

Command	bgp dampening {<1-45> [<1-20000> [<1-20000>[<1-255> [<1-45>]]]] route-map} no bgp dampening
	Configure the route dampening.The “no bgp dampening” command cancels the route dampening function
Parameter	<1-45>: Respectively the penalty half-lives of accessible and inaccessible route, namely the penalty value is reduced to half of the previous value, in minutes. <1-20000>: Respectively the penalty reuse border and restrain border. <1-255>: Maximum restrain route time, in minutes. route-map: route-map name.
Default	Half-life of accessible route is 15 minutes, 15 minutes for inaccessible. The restrain border is 2000, reuse border is 750, and maximum restrain time is 60 minutes
Command Mode	BGP route mode
Usage Guide	Abundant route update due to unstable route could be reduced with route dampening technology, of which the algorithm is lay penalty on the route when the route fluctuates, and when penalty exceeds the restrain border this route will no longer be advertised. The penalty value will be reduced by time by the half-life index regulation if the route keeps stable and finally be advertised again when the penalty falls below the border or the restrain time exceeds the maximum restrain time. This command is for enabling/disabling the route dampening and configuring its parameters.
Example	Enable the route dampening and use the parameter configuration by default. Switch(config-router)# bgp dampening

bgp default

Command	bgp default {ipv4-unicast local-preference <0-4294967295>} no bgp default {ipv4-unicast local-preference [<0-4294967295>]}
Parameter	Set the BGP defaults, the “ no bgp default {ipv4-unicast local-preference [<0-4294967295>]} ” command cancels this configuration. ipv4-unicast : Configure the default using IPv4-unicast to set up neighbor connection. local-preference<0-4294967295> : Configure the default local priority.
Default	The IPv4 unicast is default enabled when BGP is enabled. The default priority is 100.
Command Mode	BGP route mode
Usage Guide	IPv4 unicast address-family is default enabled in BGP. Cancel this setting with no bgp default ipv4-unicast command so to not enable this address-family in default. Default local priority can be configured through bgp default local-preference command.
Example	Configure the default local priority to be 500. Configure in 10.1.1.66: Switch(config)#router bgp 200 Switch(config-router)# bgp default local-preference 500

bgp deterministic-med

Command	bgp deterministic-med no bgp deterministic-med
Parameter	Use the best MED for the same prefix in the AS to compare with other AS. The “ no bgp deterministic-med ” cancels this configuration. -
Default	-
Command Mode	BGP route mode
Usage Guide	Normally if same prefix routes from several paths, each path will be compared. With this configuration, the system will only use the path with the smallest MED in the AS (when other main attributes equal) to compare with other AS. After the best one is elected, select the path among AS with no regard to MED value.
Example	Set BGP to use the best MED for the same prefix in the AS to compare with other AS. Switch(config-router)#bgp deterministic-med

bgp enforce-first-as

Command	bgp enforce-first-as no bgp enforce-first-as
	Enforces the first AS position of the route AS-PATH contain the neighbor AS number or else disconnect this peer when the BGP is reviving the external routes. The " no bgp enforce-first-as " command cancels this configuration.
Parameter	-
Default	-
Command Mode	BGP route mode
Usage Guide	This command is usually for avoiding unsafe or unauthenticated routes.
Example	Switch(config-router)#bgp enforce-first-as

bgp fast-external-failover

Command	bgp fast-external-failover no bgp fast-external-failover
	Fast reset when the BGP neighbor connection varies at the interface other than wait for TCP timeout. The " no bgp fast-external-failover " command cancels this configuration.
Parameter	-
Default	Configured
Command Mode	BGP route mode。
Usage Guide	This command is for immediately cutting of the neighbor connection when the interface is down
Example	Switch(config-router)# bgp fast-external-failover

bgp inbound-route-filter

Command	bgp inbound-route-filter no bgp inbound-route-filter

	The bgp do not install the RD routing message which does not exist locally. The no command means the RD will be installed with no regard to the local existence of the RD.
Parameter	-
Default	-
Command Mode	BGP route mode
Usage Guide	Normally when the switch plays as PE, whether the route bgp acquired from VPN is saved in BGP depends on if the VRF configured in this PE has got matched information. With the no command the BGP will save the routing message with no regard to the matched information.
Example	Switch(config)#router bgp 100 Switch(config-router)#no bgp inbound-route-filter

bgp inbound-max-route-num

Command	bgp inbound-max-route-num <0-216000> no bgp inbound-max-route-num
Parameter	Set the number limit of routers learnt by the bgp process from its neighbors. The number limit of routers, ranging from 0 to 216000.
Default	The number limit is 216000by default.
Command Mode	BGP route mode
Usage Guide	Limit the number of routers learnt by the bgp process from its neighbors with this command.
Example	The following configuration will limit max number of routers that the bgp process receives from its neighbors as 20000. Switch(config-router)#bgp inbound-max-route-num 20000

bgp log-neighbor-changes

Command	bgp log-neighbor-changes no bgp log-neighbor-changes
Parameter	Output log message when BGP neighbor changes. The “ no bgp log-neighbor-changes ” command cancels this configuration.

Default	-
Command Mode	BGP route mode
Usage Guide	Can display neighbor change messages on the monitor.
Example	Switch(config-router)# bgp log-neighbor-changes

bgp network import-check

Command	bgp network import-check no bgp network import-check
	Set whether check the IGP accessibility of the BGP network route or not. The “ no bgp network import-check ” command sets to not checking the IGP accessibility.
Parameter	-
Default	-
Command Mode	BGP route mode
Usage Guide	Checking the IGP accessibility of the route advertised by BGP is to check the existence of next-hop and its IGP accessibility.
Example	Set to check the IGP accessibility of BGP network route. Switch(config-router)# bgp network import-check

bgp rfc1771-path-select

Command	bgp rfc1771-path-select no bgp rfc1771-path-select
	After this attribute is set, path selecting will follow the way defined in rfc 1771, namely not checking the AS internal metric, or comparing the internal METRIC.
Parameter	-
Default	-
Command Mode	Global mode
Usage Guide	After this attribute is set, path selecting will follow the way defined in rfc 1771, namely not checking the AS internal metric, when different AS exist, which should be perform without this attribute set.

Example	Configure to follow the rfc1771 path selecting. Switch(config)# bgp rfc1771-path-select
bgp rfc1771-strict	
Command	bgp rfc1771-strict no bgp rfc1771-strict
	Set whether strictly follows the rfc1771 restrictions. The “ no bgp rfc1771-strict ” command set to not strictly following.
Parameter	-
Default	Not following rfc 1771 restrictions.
Command Mode	Global mode
Usage Guide	With this attribute set, generation types of routes from protocols such as RIP, OSPF, ISIS, etc will be regarded as IGP (internal generated), or else as incomplete.Example: Configure to stricly follow the rfc1771 restrictions.
Example	Configure to stricly follow the rfc1771 restrictions. Switch(config)#bgp rfc1771-strict

bgp router-id

Command	bgp router-id <A.B.C.D> no bgp router-id [<A.B.C.D>]
	Configure the router ID manually. The no operation cancels this configuration.
Parameter	<A.B.C.D> : Router ID.
Default	Automatically acquire router ID.
Command Mode	BGP route mode
Usage Guide	Manually set the router ID with this command.

Example	Set the Router ID to be 1.1.1.1. Switch(config-router)#bgp router-id 1.1.1.1
bgp scan-time	
Command	bgp scan-time <0-60> no bgp scan-time [<0-60>]
	Set the time interval of the periodical next-hop validation; the “ no bgp scan-time [<0-60>] ” command restores to the default value.
Parameter	<0-60> : Validation time interval.
Default	Default interval is 60s.
Command Mode	BGP route mode
Usage Guide	Validate the next-hop of BGP route, this command is for configuring the interval of this check. Set the parameter to 0 if you don't want to check.
Example	Set the time interval of periodical next-hop validation to be 30s. Switch(config-router)# bgp scan-time 30

clear ip bgp

Command	clear ip bgp { * <1-4294967295> A.B.C.D X:X::X:X dampening external flap-statistics ipv4 ipv6 peer-group view } { in [prefix-filter] ipv4 [labeled-unicast multicast unicast] ipv6 [multicast unicast] l2vpn [evpn] out soft vpnv4 [unicast] vrf <vrf-name> } { soft in out }
	Reboot the connection between BGP of vrf-name and all peers.
Parameter	*: Clear all peers. <1-4294967295>: Clear peers with the AS number. A.B.C.D: BGP neighbor address to clear. X:X::X:X: BGP IPv6 neighbor to clear. dampening: Clear route flap dampening information. external: Clear all external peers. flap-statistics: Clear route flap statistics. ipv4: Address family ipv6: Address family peer-group: Clear all members of peer-group view: BGP view <vrf-name>: Configure the instance name of VPN, the ranging from 1 to 64; in: The in soft configuration is updated; out: The out soft configuratin is updated;

	soft: The soft reboot.
Default	-
Command Mode	Admin mode
Usage Guide	Reboot BGP when configuring clear ip bgp * command; send the requestment message to neighbor when configuring in parameter; sent the route to neighbor when configuring out parameter. If configure soft, BGP will not be reseted.
Example	Switch#clear ip bgp * vrf VRF-A Switch#

clear ip bgp dampening

Command	clear ip bgp [<address-family>] dampening [<ip-address> <ip-address/M>]
	Used for resetting BGP routing dampening.
Parameter	<address-family>: address-family, such as "ipv4 unicast". <ip-address>: IP address. <ip-address/M>: IP address and mask.
Default	-
Command Mode	Admin mode
Usage Guide	It is possible to clear BGP routing dampening messages and state by different parameters (such as address-family or IPv4 address).
Example	Clear BGP routing dampening and state of IPv4 unicast cluster. Switch# clear ip bgp ipv4 unicast dampening

clear ip bgp flap-statistics

Command	clear ip bgp [<address-family>] flap-statistics [<ip-address> <ip-address/M>]
	For resetting BGP routing dampening statistics messages.
Parameter	<address-family>: address-family such as "ipv4 unicast". <ip-address>: IP address. <ip-address/M>: IP address and mask.
Default	-
Command Mode	Admin mode

Usage Guide	It is possible to clear BGP routing dampening statistic messages and state by different parameters (such as address-family or IPv4 address).
Example	Clear the BGP dampening statistic messages of IPv4 unicast cluster. Switch#clear ip bgp ipv4 unicast flap-statistics

distance

Command	distance <1-255> <ip-address/M> [<WORD>] no distance <1-255> <ip-address/M> [<WORD>]
Parameter	Set the manage distance of the routing prefix. The “ no distance <1-255> <ip-address/M> [<WORD>] ” command restores to the default value. <1-255> : Manage distance. <ip-address/M> : Routing prefix. <WORD> : Access-list name.
Default	-
Command Mode	BGP route mode
Usage Guide	Set the manage distance for specified BGP route as the path selecting basis.
Example	Set the manage distance for route 90 10.1.1.64/32 to be 90. Switch(config-router)# distance 90 10.1.1.64/32

distance bgp

Command	distance bgp <1-255> <1-255> <1-255> no distance bgp [<1-255> <1-255> <1-255>]
Parameter	Set the BGP protocol management distance. The “ no distance bgp [<1-255> <1-255> <1-255>] ” command restores the manage distance to default value. <1-255> : Respectively the EBGp, IBGP and LOCAL manage distance of the BGP.
Default	Default EBGp is 20, others are 200.
Command Mode	BGP route mode
Usage Guide	: Set the manage distance for BGP routing as the NSM path selecting basis.
Example	Set the manage distance for BGP routing as 15, the manage distance for IBGP and local routing as 150. Switch(config-router)# distance bgp 15 150 150

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>
Parameter	Configure the AS-PATH access-list. The “ no ip as-path access-list <.LINE>{<permit> <deny>} <LINE>” command deletes this access-list. <.LINE> : name of access-list. <LINE> : matched strings in the AS-PATH.
Default	-
Command Mode	Global mode
Usage Guide	Use this command to configure the access-list related to AS-PATH, so to supply the conditions for pass/filter.
Example	Configure the access-list named ASPF, filter the AS-PATH contained route 100. Switch(config)#ip as-path access-list ASPF deny ^100\$

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>]
Parameter	Configure the community-list. The “ no ip community-list {<LISTNAME> <1-199>}[expanded <WORD>][standard <WORD>] [{deny permit} <.COMMUNITY>]” command deletes the community list. <LISTNAME> : name of community list. <1-199> : Standard or extended community number. <WORD> : Standard or extended community number. <.COMMUNITY > : Members of the community list, which may be the combination of aa:nn, or internet, local-AS, no-advertise, and no-export. It can be shown in regular expressions under extended conditions.
Default	-
Command Mode	Global mode
Usage Guide	With this command we can configure the community-list so to supply terms for the pass/filter/search.

Example	Configure the ip community-list named LN, permit community attribute as 100:10. <pre>Switch(config)# ip community-list LN permit 100:10</pre>
ip extcommunity-list	
Command	<pre>ip extcommunity-list {<LISTNAME> <1-199> [expanded <WORD>]][standard <WORD>]} {deny permit} <.COMMUNITY> no ip extcommunity-list {<LISTNAME> <1-199> [expanded <WORD>]][standard <WORD>]} {deny permit} <.COMMUNITY></pre> Configure the extended community-list. The “no ip extcommunity-list {<LISTNAME> <1-199> [expanded <WORD>]][standard <WORD>]} {deny permit} <.COMMUNITY>” command is for deleting the extended community list.
Parameter	<LISTNAME>: name of community-list. <1-199>: Standard or extended community number. <WORD>: Standard or extended community number. <.COMMUNITY>: Members of the community list, which may be the combination of aa:nn, or internet, local-AS, no-advertise, and no-export. It can be shown in regular expressions under extended conditions.
Default	-
Command Mode	Global mode
Usage Guide	With this command we can configure the community-list so to supply terms for the pass/filter/search.
Example	Configure the excommunity-list named LN, permit community attribute as 100:10. <pre>Switch(config)#ip extcommunity-list LN permit 100:10</pre>

neighbor activate

Command	<pre>neighbor {<ip-address> <WORD>} activate no neighbor {<ip-address> <WORD>} activate</pre> Configure the address family routing which do or do not switch specific address-family with BGP neighbors. The “no neighbor {<ip-address> <WORD>} activate” command is for setting the route which do not switch the specified address family.
Parameter	<ip-address>: IP address of the neighbor. <WORD>: Name of peer group.
Default	Enable the routing switch of IP unicast address-family, and disable other address-families.
Command Mode	BGP route mode

Usage Guide	IP unicast is configured under BGP route mode. Configure whether specific address-family is switched under address-family mode. If this option on any side between local side and partner is not enabled, the address-family route will not be acquired by the partner even if the corresponding address family routes acquired before will be cancelled after this option is disabled.
Example	Configure to exchange the unicast route with neighbor 2002::2. Switch(config-router)#neighbor 2002::2 activate

neighbor advertisement-interval

Command	neighbor {<ip-address> <WORD>} advertisement-interval <0-600> no neighbor {<ip-address> <WORD>} advertisement-interval [<0-600>]
	Configure the update interval of specific neighbor route. The “ no neighbor {<ip-address> <WORD>} advertisement-interval [<0-600>] ” command restores to default.
Parameter	<ip-address> : IP address of the neighbor. <WORD> : Name of the peer group. <0-600> : Advertise interval, in seconds.
Default	Default IBGP is 5s, default EBGP is 30s.
Command Mode	BGP route mode
Usage Guide	Reduce this value will improve the route updating speed while also consumes more bandwidth.
Example	Set the route update interval as 20s with neighbor 10.1.1.64. Switch(config-router)#neighbor 10.1.1.64 advertisement-interval 20

neighbor allowas-in

Command	neighbor {<ip-address> <WORD>} allowas-in [<1-10>] no neighbor {<ip-address> <WORD>} allowas-in
	Configure the counts same AS is allowed to appear in the neighbor route AS table. The

Parameter	“no neighbor {<ip-address> <WORD>} allowas-in” restores to not allow any repeat.
	<ip-address> : IP address of the neighbor.
	<WORD> : Name of the peer group.
	<1-10> : Allowed count of same AS number.
Default	In default conditions AS is not allowed repeating in the same route, and when set the repeat count it is defaulted at 3 when <1-10> parameters not set.
Command Mode	BGP route mode
Usage Guide	Normally BGP will not allow same AS number appears in the route more than one time. The system will deny a route when its AS number appears in the AS-PATH. However to support some special needs, especially the VPN support, the extended BGP allows the AS re-appear counts by configuration. This command is for configure the re-appear counts.
Example	Allow the same AS to appear in the route three times for neighbor 10.1.1.66. Switch(config-router)#neighbor 10.1.1.66 allowas-in

neighbor attribute-unchanged

Command	neighbor {<ip-address> <WORD>} attribute-unchanged [as-path][med][next-hop] no neighbor {<ip-address> <WORD>} attribute-unchanged [as-path] [med] [next-hop]
	Configure certain attributes which is kept unchanged for transmitting, namely the attribute transparent transmission. The “no neighbor {<ip-address> <WORD>} attribute-unchanged [as-path] [med] [next-hop]” command means the attribute transparent transmission is not performed.
Parameter	<ip-address> : IP address of the neighbor. <WORD> : Name of the peer group.
Default	-
Command Mode	BGP route mode
Usage Guide	With this configuration specified route attributes will not change when transmitted to the specified neighbor. The BGP route mode is the IPv4 unicast address mode configuration. No parameter refers to above three parameter are configured together.
Example	Set the attribute of route as-path, med, next-hop unchanged for neighbor 10.1.1.64. Switch(config-router)#neighbor 10.1.1.64 attribute-unchanged

neighbor capability

Command	<pre>neighbor {<ip-address> <WORD>} capability {<dynamic> <route-refresh> <graceful-restart>} no neighbor {<ip-address> <WORD>} capability {<dynamic> <route-refresh> <graceful-restart>}</pre> Configure dynamic update between neighbors and the route refresh capability negotiation. The “no neighbor {<ip-address> <WORD>} capability {dynamic route-refresh}” command do not enable the specific capability negotiation.
Parameter	<ip-address>: Neighbor IP address. <WORD>: Name of peer group. <dynamic>: Advertise dynamic capability to this neighbor <route-refresh>: Advertise route-refresh capability to this neighbor <graceful-restart>: the graceful-restart capability
Default	Not configure the dynamic update capability but the route refresh capability.
Command Mode	BGP route mode
Usage Guide	This is an extended BGP capability. With this configuration supported capabilities by both side will be negotiated in the OPEN messages, and the partner will respond if this capability is supported by the partner and send NOTIFICATION if not. The originating side will then send an OPEN excluded the capability to reestablish the connection. The dynamic capability refers to when the address family negotiation changes, the connection don't have to be restarted. Route refresh refers to sending refresh request when configuring some soft reconfigurable attributes and the partner will retransmit the existing route to the originating side. With route refresh attribute, the connection will not have to be restarted but be refreshed with the clear ip bgp * soft in command.
Example	<pre>Switch(config-router)#neighbor 10.1.1.64 capability dynamic Switch(config-router)# no neighbor 10.1.1.64 capability route-refresh</pre>

neighbor capability orf prefix-list

Command	<pre>neighbor {<ip-address> <WORD>} capability orf prefix-list {<both> <send> <receive>} no neighbor {<ip-address> <WORD>} capability orf prefix-list {<both> <send> <receive>}</pre> Configure the out route filter capability negotiation between neighbors. The “no neighbor {<ip-address> <WORD>} capability orf prefix-list {<both> <send> <receive>}” command set to not perform the negotiation.
Parameter	<ip-address>: Neighbor IP address. <WORD>: Name of peer group.

Default	-
Command Mode	BGP route mode
Usage Guide	This is an extended BGP capability. With this configuration supported capabilities by both side will be negotiated in the OPEN messages, and the partner will respond if this capability is supported by the partner and send NOTIFICATION if not. The originating side will then send an OPEN excluded the capability to reestablish the connection. With this capability, the side configured with in prefix-list filter rules will transmit its own filter rules to the peer, the peer group will apply this rule as its own out rules, so to avoid sending route which will be denied by the partner.
Example	Set to perform the out route filter capability negotiation with neighbor 10.1.1.66. Switch(config-router)#neighbor 10.1.1.66 capability orf prefix-list both

neighbor collide-established

Command	neighbor {<ip-address> <WORD>} collide-established no neighbor {<ip-address> <WORD>} collide-established
	Enable the collision check and settlement in the TCP connection collision. The “ no neighbor {<ip-address> <WORD>} collide-established ” command disables the TCP connection collision settlement.
Parameter	<ip-address> : Neighbor IP address. <WORD> : Name of the peer.
Default	-
Command Mode	BGP route mode
Usage Guide	This command is for settling the problem that multi-connection among peers due to TCP connection collision. Connections created with this option on will always be check even at established state. And it will be checked if local side IP is larger than partner IP when collides. If yes, the original connection will be deleted, and if not the option will be configured to only checks when the connection originated from local side at open sent and open confirm state.
Example	Set to perform the TCP connection collision check and settlement with neighbor 10.1.1.64. Switch(config-router)#neighbor 10.1.1.64 collide-established

neighbor default-originate

Command	neighbor {<ip-address> <WORD>} default-originate [route-map <WORD>] no neighbor {<ip-address> <WORD>} default-originate [route-map <WORD>]
Parameter	Configures whether enables transmitting default route to the specific neighbor. The “ no neighbor {<ip-address> <WORD>} default-originate [route-map <WORD>] ” command configures not sending default route to neighbors. <ip-address> : IP address of the neighbor. <WORD> : Name of the peer. <WORD> : Name of route map.
Default	-
Command Mode	BGP route mode
Usage Guide	With this option, the default route of local side will be transmitted to partner, or else not. It supplies with options of which one to supply the default route. if several neighbors of the partner supply default route, the best one will be elected according to path selecting principles. According to route mirror, it can be chosen when to send the default route.
Example	Set to transmit the local default route to neighbor 10.1.1.64. Switch(config-router)#neighbor 10.1.1.64 default-originate Switch(config-router)# Then the default route from BGP will appear in partner route list.

neighbor description

Command	neighbor {<ip-address> <WORD>} description <LINE> no neighbor {<ip-address> <WORD>} description
Parameter	Configure the description string of the peer or peer group. The “ no neighbor {<ip-address> <WORD>} description ” command deletes the configurations of this string. <ip-address> : Neighbor IP address. <WORD> : Name of peer group. <.LINE> : Description string consists of displayable characters less than 80.
Default	Description string is empty.
Command Mode	BGP route mode
Usage Guide	Configure the introduction of the peer or peer group.
Example	Set the description string as tester with neighbor 10.1.1.64. Switch(config-router)#neighbor 10.1.1.64 description tester Switch(config-router)#

neighbor distribute-list

Command	neighbor {<ip-address> <WORD>} distribute-list {<1-199> <1300-2699> <WORD>} {in out} no neighbor {<ip-address> <WORD>} distribute-list {<1-199> <1300-2699> <WORD>} {in out}
Parameter	Configure the policy applied in partner route update transmission. The “ no neighbor {<ip-address> <WORD>} distribute-list {<1-199> <1300-2699> <WORD>} {in out} ” command cancels the policy configuration. <ip-address> : Neighbor IP address. <WORD> : Name of peer group. <1-199> <1300-2699> <WORD> : Number or name of the access-list.
Default	Policy not applied.
Command Mode	BGP route mode
Usage Guide	Configure the policies with access-list command and apply this command on route sending and receiving. It will filter the update route from partner when use in mode, and will filter the route from local side to partner with out mode.
Example	Send into neighbor route 10.1.1.66, to filter the route with the aim 100.1.0.0. 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)# neighbor 10.1.1.66 distribute-list 101 in

neighbor dont-capability-negotiate

Command	neighbor {<ip-address> <WORD>} dont-capability-negotiate no neighbor {<ip-address> <WORD>} dont-capability-negotiate
Parameter	Set to not perform capability negotiate in creating connections. The “ no neighbor {<ip-address> <WORD>} dont-capability-negotiate ” command cancels this configuration. <ip-address> : Neighbor IP address. <WORD> : Name of the peer group.
Default	Capability negotiation performed.

Command Mode	BGP route mode
Usage Guide	As the negotiation is the default, it can be disabled with this configuration when it is known that the partner BGP version is old which don't support capabilitynegotiation.
Example	Last addition capability negotiation will not be realized in the connection by configuring as follows. <pre>Switch(config-router)#neighbor 10.1.1.64 dont-capability-negotiate</pre>

neighbor ebgp-multihop

Command	neighbor {<ip-address> <WORD>} ebgp-multihop [<1-255>] no neighbor {<ip-address> <WORD>} ebgp-multihop [<1-255>]
	Configures the EBGp neighbors can existing in different segment as well as its hop count (TTL). The " no neighbor {<ip-address> <WORD>} ebgp-multihop [<1-255>] " set that the EBGp neighbors must be in the same segment.
Parameter	<ip-address> : Neighbor IP address. <WORD> : Name of the peer group. <1-255> : Allowed hop count.
Default	Must be in the same segment.
Command Mode	BGP route mode
Usage Guide	Without this command, EBGp peers are required to be in the same segment and after this command is configured, peer addresses may from different segments. The allowed hop count can be configured and will be 255 if not.
Example	Three device 10.1.1.64(AS100) and 11.1.1.120(AS300) connected respectively to the two interface 10.1.1.66 and 10.1.1.100 of another device. IGP accessibilities of 10.1.1.64 and 11.1.1.120 on both side routes are ensured through static configuration. The neighbor relationship is established only after both side are configured as follows: <pre>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</pre> After this, switches in different segments will be able to create BGP neighbor relationship.

neighbor enforce-multihop

Command	neighbor {<ip-address> <WORD>} enforce-multihop no neighbor {<ip-address> <WORD>} enforce-multihop
Parameter	Enforce the multihop connection to the neighbor. The “ no neighbor {<ip-address> <WORD>} enforce-multihop ” command cancels this configuration. <ip-address> : Neighbor IP address <WORD> : Name of peer group.
Default	Not enforced
Command Mode	BGP route mode
Usage Guide	In fact the direct route can not be enforced to multihop, however will be treated as a multihop connection with this configuration, namely the check originally only performed on IBGP and EBGP of non-direct routes will be performed on all after this attribute set. The nexthop direct connected check will not be performed at exit in enforce multihop conditions.
Example	Enforce neighbor 10.1.1.66 as multihop connection. Switch(config-router)#neighbor 10.1.1.66 enforce-multihop

neighbor filter-list

Command	neighbor {<ip-address> <WORD>} filter-list <.LINE> {<in> <out>} no neighbor {<ip-address> <WORD>} filter-list <.LINE> {<in> <out>}
Parameter	Access-list control for AS-PATH. The “ no neighbor {<ip-address> <WORD>} filter-list <.LINE> {<in> <out>} ” cancels the AS-PATH access-list control. <ip-address> : Neighbor IP address. <WORD> : Name of peer group. <.LINE> : AS-PATH access-list name configured through ip as-path access-list <.LINE> <permit deny> <LINE>.
Default	Not configured
Command Mode	BGP route mode
Usage Guide	After first configured the IP AS-PATH access-list, apply this option to specified neighbor will be able to send/receive routes with specified AS numbers in the AS list. Accepting or denying depends on the configuration of the access-list, while sending and receiving are configured by this command.
Example	Configure the AS-PATH access control list, “ASPF” is the name of the access-list. The route with AS number of 100 will not be able to update to the partner due to the filter

```

table control.
Switch(config)#ip as-path access-list ASPF deny 100
Switch(config)#router bgp 100
Switch(config-router)# redistribute static
Switch(config-router)neighbor 10.1.1.66 filter-list aspf out

```

neighbor interface

Command	neighbor {<ip-address>}interface{<IFNAM> <loopback>[<1-1024>]}<vlan>[<1-4094>]} no neighbor {<ip-address>}interface Specify the interface to the neighbor. The “ no neighbor <ip-address>interface <IFNAM> ” of the command cancels this configuration.
Parameter	<ip-address> : Neighbor IP address. <IFNAME> : Interface name, e.g. “Vlan 2”. <loopback> : loopback <vlan> : vlan <1-1024> : Loopback ID <1-1024> <1-4094> : Vlan port number
Default	-
Command Mode	BGP route mode
Usage Guide	Specifies the exit interface to the neighbor with this command. Interface destination accessibility should be ensured.
Example	Set the interface to neighbor 10.1.1.64 as interface vlan 2 Switch(config-router)# neighbor 10.1.1.64 interface vlan2

neighbor maximum-prefix

Command	neighbor {<ip-address> <WORD>} maximum-prefix <1-4294967295> [<1-100> <warning-only>]} no neighbor {<ip-address> <WORD>} maximum-prefix <1-4294967295> [<1-100> <warning-only>]}
Parameter	Control the number of route prefix from the neighbor. The “ no neighbor {<ip-address> <WORD>} maximum-prefix <1-4294967295> [<1-100> <warning-only>]} ” command cancels this configuration.
Parameter	<ip-address> : Neighbor IP address. <WORD> : Name of the peer. <1-4294967295> : Max prefix value allowed. <1-100> : Percentage of the max value at which it warns.

<warning-only>: Warning only or not.

Default	Not limited.
Command Mode	BGP route mode
Usage Guide	Due to concerns of too much route updates from neighbors (e.g. attack), the max number of prefix acquired from a neighbor is limited, and will warns when the number hits certain rate. If the warning-only option is set, then there will be warning only, if not, the connection to the neighbor will be cut till clear the records with clear ip bgp command.

Example	Configure the maximum number of route prefix from neighbor 10.1.1.64 is 12, and it warns when the number of route prefix reaches 6, and the connection will be cut when the number hit 13. Switch(config-router)#neighbor 10.1.1.64 maximum-prefix 12 50

neighbor next-hop-self

Command	neighbor {<ip-address> <WORD>} next-hop-self no neighbor {<ip-address> <WORD>} next-hop-self
	Ask the neighbor to point the route nexthop sent by the local side to local side. The “ no neighbor {<ip-address> <WORD>} next-hop-self ” command cancels this configuration.
Parameter	<ip-address> : Neighbor IP address. <WORD> : Name of peer group.

Default	-
Command Mode	BGP route mode
Usage Guide	In the EBGP environment, the nexthop will automatically point to the source neighbor. However in IBGP environment, the nexthop remains the same for route in the same segment. If it is not broadcast network, errors will be encountered. This command is for force self as the nexthop of the neighbor under IBGP.

Example	Switch(config-router)#neighbor 10.1.1.66 next-hop-self

neighbor override-capability

Command	neighbor {<ip-address> <WORD>} override-capability

no neighbor {<ip-address>|<WORD>} override-capability

Whether enable overriding capability negotiation. The “**no neighbor {<ip-address>|<WORD>} override-capability**” command restores the capability negotiation.

Parameter	<ip-address> : Neighbor IP address. <WORD> : Name of the peer group.
Default	-
Command Mode	BGP route mode
Usage Guide	With this attribute, error notify due to unsupported capability negotiation the neighbors required will not be sent.
Example	Switch(config-router)#neighbor 10.1.1.64 override-capability

neighbor passive

Command	neighbor {<ip-address> <WORD>} passive no neighbor {<ip-address> <WORD>} passive
Parameter	Configure whether the connecting request is positively sent in the connection with specified neighbor; the “ no neighbor {<ip-address> <WORD>} passive ” command restores to positively send the connecting request. <ip-address> : Neighbor IP address. <WORD> : Name of peer group.
Default	Positively send the connecting request.
Command Mode	BGP route mode
Usage Guide	With this attribute set, the local side will not positively send the TCP connecting request after the neighbors are configured, but stays in listening mode waiting for the connecting request from partners.
Example	Switch(config-router)#neighbor 10.1.1.64 passive After configured with this attribute and reestablishing the connection , the local side do not attempt to create connection but stays in ACTIVE state waiting for the TCP connection request from the partner.

neighbor peer-group (Creating)

Command	neighbor < TAG> peer-group no neighbor < TAG> peer-group
	Create/delete a peer group. The “ no neighbor < TAG> peer-group ” command deletes a peer group.
Parameter	<WORD> : Name of the peer group of which the largest length contains 256 characters.
Default	No peer group.
Command Mode	BGP route mode
Usage Guide	By configuring the peer group, a group of peers with the same attributes will be configured at the same time so to reduce the configuration staff labor. Assign members to the peer group with neighbor <ip-address> peer-group <WORD> 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

neighbor peer-group(Configuring group members)

Command	neighbor <ip-address> peer-group <WORD> no neighbor <ip-address> peer-group <WORD>
	Assign/delete peers in the group. The “ no neighbor <ip-address>peer-group <WORD> ”command deletes the peers from the peer group.
Parameter	<ip-address> : Neighbor IP address. <WORD> : Name of peer group.
Default	No peer group.
Command Mode	BGP route mode
Usage Guide	By configuring the peer group, a group of peers with the same attributes will be configured at the same time so to reduce the configuration staff labor. Create peer group with above command and assign members into the group with this command.
Example	Refer to above examples.

neighbor port

Command	neighbor {<ip-address> <WORD>} port <0-65535> no neighbor {<ip-address> <WORD>} port [<0-65535>]
	Specify the TCP port number of the partner through which the communication carries. The “ no neighbor <ip-address> port [<0-65535>]” command restores the port number to default value.
Parameter	<ip-address>: Neighbor IP address. < WORD >: Name of the peer group. <0-65535>: TCP port number.
Default	Default port number is 179.
Command Mode	BGP route mode
Usage Guide	This is a configuration when the partner may connect through ports not specified by BGP.
Example	Switch(config-router)#neighbor 10.1.1.64 port 1023

neighbor prefix-list

Command	neighbor {<ip-address> <WORD>} prefix-list <LISTNAME number> {<in out>} no neighbor {<ip-address> <WORD>} prefix-list <LISTNAME number>{<in> <out>}
	Configure the prefix restrictions applied in sending or receiving routes from specified neighbors. The “ no neighbor {<ip-address> <WORD>} prefix-list <LISTNAME number> {<in> <out>}” command cancels this configuration.
Parameter	<ip-address>: Neighbor IP address. <WORD>: Name of the peer group. <LISTNAME number>: Name or sequence number of the prefix-list. <in out>: Direction on which the restrictions applied.
Default	No prefix restrictions applied.
Command Mode	BGP route mode

Usage Guide	Specify the prefix and its scope by configuring ip prefix-list and determines whether this scope is permitted or denied. Only the route with permitted prefix will be sent or received.
Example	<pre>Switch(config)#ip prefix-list prw permit 100.1.0.0/22 ge 23 le 25 Switch(config)#router bgp 200 Switch(config-router)#redistribute static Switch(config-router)#neighbor 10.1.1.66 prefix-list prw out</pre>

neighbor remote-as

Command	neighbor {<ip-address> < WORD >} remote-as <as-id> no neighbor {<ip-address> < WORD >} [remote-as <as-id>]
Parameter	Configure the BGP neighbor. The no command is used for deleting BGP neighbors. <ip-address>: Neighbor IP address < WORD >: Name of peer group <as-id>: Neighbor AS number, ranging from 1 to 4294967295, it can be shown in decimal notation (such as 6553700) or delimiter method (such as 100.100).
Default	No neighbors
Command Mode	BGP route mode
Usage Guide	The BGP neighbors are completely generated through command configurations. A neighbor relationship can only be really established by mutual configuring. Partner AS number should be specified in configuration. The neighbor relationship can not be established when the AS number is incorrect. The partner AS number is the same with that of local side inside the AS.
Example	<pre>Configure 2 neighbor AS as 100 and 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</pre>

neighbor remove-private-AS

Command	neighbor {<ip-address> <WORD>} remove-private-AS no neighbor {<ip-address> <WORD>} remove-private-AS
Parameter	Configures whether remove the private AS number when sending to the neighbor. The “no neighbor {<ip-address> <WORD>} remove-private-AS” command cancels this configuration. <ip-address>: Neighbor IP address <WORD>: Name of peer group

Default	Not configured
Command Mode	BGP route mode
Usage Guide	Configure this attribute to avoid assigning the internal AS number to the external AS sometimes. The internal AS number ranges between 64512-65535, which the AS number could not be sent to the INTERNET since it is not a valid external AS number. What removed here is private AS numbers of the totally private AS routes. Those who have private AS numbers while also have public AS numbers are not processed.
Example	Switch(config-router)#neighbor 10.1.1.64 remove-private-AS

neighbor route-map

Command	neighbor {<ip-address> <WORD>} route-map <NAME> {<in out>} no neighbor {<ip-address> <WORD>} route-map <NAME> {<in out>}
Parameter	Configure the route mapping policy when sending or receiving route. The “ no neighbor {<ip-address> <WORD>} route-map <NAME> {<in out>} ” command cancels this configuration. <ip-address> : Neighbor IP address <WORD> : Name of peer group <NAME> : Name of route mapping <in out> : Direction of route mapping
Default	Not set
Command Mode	BGP route mode
Usage Guide	First it has to configure route mapping under global mode by creating a route map with route-map command and configure the match condition and actions, then the command can be applied.
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)#neighbor 10.1.1.64 route-map test out

neighbor route-reflector-client

Command	neighbor {<ip-address> <WORD>} route-reflector-client

no neighbor {<ip-address>|<WORD>} route-reflector-client

Configure the route reflector client. The “**no neighbor {<ip-address>|<WORD>}route-reflector-client**” command cancels this configuration

Parameter	<ip-address> : Neighbor IP address <WORD> : Name of peer group
Default	Not configured.
Command Mode	BGP route mode
Usage Guide	The route reflection is used for reducing the peers when the internal IBGP routers inside AS are too much. The client only exchanges messages with route reflector while the reflector deals with message exchange among each client and other IBGP, EBGp routers. This command configures itself as the route reflector, while specific peer group is as its client. Note: this configuration is only available inside AS.
Example	Switch(config)#router bgp 100 Switch(config-router)#neighbor 10.1.1.66 remote 100 Switch(config-router)#neighbor 10.1.1.66 route-reflector-client Switch(config-router)#neighbor 10.1.1.68 remote 100 Switch(config-router)#neighbor 10.1.1.68 route-reflector-client

neighbor route-server-client

Command	neighbor {<ip-address> <WORD>} route-server-client no neighbor {<ip-address> <WORD>} route-server-client
Parameter	Configure the route server client. The “ no neighbor {<ip-address> <WORD>} route-server-client ” command cancels this configuration. <ip-address> : Neighbor IP address <WORD> : Name of peer group
Default	Not configured
Command Mode	BGP route mode
Usage Guide	The route service is for reducing the peers when the router between AS is too much under EBGp environment. The server transparently transforms the routing messages to other clients with its client exchanges messages through route server.
Example	Three routers : 10.1.1.64 (AS100) and 10.1.1.68 (AS300) respectively creates neighbor relationship with the connected 10.1.1.66 (AS200) , the configuration is as follows: Switch(config)#router bgp 200 Switch(config-router)#neighbor 10.1.1.64 remote-as 100 Switch(config-router)#neighbor 10.1.1.64 route-server-client Switch(config-router)# neighbor 10.1.1.68 remote-as 300

Switch(config-router)# neighbor 10.1.1.68 route-server-client

neighbor send-community

Command	neighbor {<ip-address> <WORD>} send-community [both extended standard] no neighbor {<ip-address> <WORD>} send-community [both extended standard]
	Configures whether sending the community attribute to the neighbors. The “ no neighbor {<ip-address> <WORD>} send-community [both extended standard] ” command set to not sending.
Parameter	<ip-address> : IP address of the neighbor <WORD> : Name of peer group [both extended standard] : Standard community only, extended community or both.
Default	Sending the community attributes.
Command Mode	BGP route mode
Usage Guide	The community attributes can be sent to the outside or not. By default of our company we set to sending while the default in standard protocol is not sending. By configuring this attribute community attributes will be carried when sending routing information's to the neighbors, or else not. Omission of the following choice will be equal to standard.
Example	Switch(config-router)#no neighbor 10.1.1.66 send-community Switch(config-router)#neighbor 10.1.1.66 send-community

neighbor shutdown

Command	neighbor {<ip-address> <WORD>} shutdown no neighbor {<ip-address> <WORD>} shutdown
	Disconnect the neighbor connection. The “ no neighbor {<ip-address> <WORD>} shutdown ” cancels this configuration
Parameter	<ip-address> : Neighbor IP address <WORD> : Name of peer group
Default	Not disconnecting.
Command Mode	BGP route mode
Usage Guide	Directly disconnect/connect to a peer (group) without canceling the neighbor configuration.
Example	Switch(config-router)#neighbor 10.1.1.64 shutdown

neighbor soft-reconfiguration inbound

Command	neighbor {<ip-address> <WORD>} soft-reconfiguration inbound no neighbor {<ip-address> <WORD>} soft-reconfiguration inbound
	Configures whether perform inbound soft reconfiguration; the “ no neighbor {<ip-address> <WORD>} soft-reconfiguration inbound ” command set to not perform the inbound soft reconfiguration.
Parameter	<ip-address> : Neighbor IP address <WORD> : Name of peer group
Default	Not perform inbound soft reconfiguration.
Command Mode	BGP route mode
Usage Guide	The system saves the inbound messages in the buffer after the soft reconfiguration is set, will applies as soon as it restarts so to reduce consumptions of switching with other routers. The command is only available when the route refresh capability is not enabled
Example	Switch(config-router)#neighbor 11.1.1.120 soft-reconfiguration inbound

neighbor strict-capability-match

Command	neighbor {<ip-address> <WORD>} strict-capability-match no neighbor {<ip-address> <WORD>} strict-capability-match
	Configure whether strict capability match is required when establishing connections. The “ no neighbor {<ip-address> <WORD>} strict-capability-match ” command set to not requiring strict match.
Parameter	<ip-address> : Neighbor IP address <WORD> : Name of peer group
Default	No strict capability match configured.
Command Mode	BGP route mode
Usage Guide	This command takes effect to MP-BGP only. With this command, neighbor can be established when MP-BGP capabilities of the both side are matched, or else it can not be established. However, whether other capabilities are matched will not affect to establish neighbor.
Example	Switch(config-router)#neighbor 10.1.1.64 strict-capability-match

neighbor timers

Command	neighbor {<ip-address> <WORD>} timers <0-65535> <0-65535> no neighbor {<ip-address> <WORD>} timers <0-65535> <0-65535>
Parameter	Configure the KEEPALIVE interval and hold time; the “ no neighbor {<ip-address> <WORD>} timers <0-65535> <0-65535> ” command restores the defaults. <ip-address> : Neighbor IP address <WORD> : Name of peer group <0-65535> : Respectively the KEEPALIVE and HOLD TIME
Default	Default KEEPALIVE time is 60s, while HOLD TIME is 240s
Command Mode	BGP route mode
Usage Guide	Send KEEPALIVE interval and HOLD TIME intervals sent in the peer connection. The hold time is the time period for maintain the connection when no message is received from the partner (such as KEEPALIVE). And the connection will be closed after this hold time.
Example	Switch(config-router)#neighbor 10.1.1.64 timers 50 200

neighbor timers connect

Command	neighbor {<ip-address> <WORD>} timers connect <0-65535> no neighbor {<ip-address> <WORD>} timers connect [<0-65535>]
Parameter	Configure the connecting retry time interval. The “ no neighbor {<ip-address> <WORD>} timers connect [<0-65535>] ” command restores the default value. <ip-address> : Neighbor IP address <WORD> : Name of peer group <0-65535> : Retry interval
Default	120s
Command Mode	BGP route mode
Usage Guide	Configure the connecting time interval when connecting a peer. The NO form restores the default value.
Example	Switch(config-router)#neighbor 10.1.1.64 timers connect 100

neighbor unsuppress-map

Command	neighbor {<ip-address> <WORD>} unsuppress-map <WORD> no neighbor {<ip-address> <WORD>} unsuppress-map <WORD>
	Configure or cancel the unsurprising to conditions meet the specified route map. The “ no neighbor {<ip-address> <WORD>} unsuppress-map <WORD> ” command cancels this configuration.
Parameter	<ip-address> : Neighbor IP address. <WORD> : Name of peer group. <WORD> : Name of route-map.
Default	Not set.
Command Mode	BGP route mode
Usage Guide	This command is generally for route suppressed by the aggregated and summary-only conditions. Routes meet the route map conditions will still be send separately other than suppressed.
Example	Switch(config-router)#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 Route with nexthop as 10.1.1.100 will not be restrained.

neighbor update-source

Command	neighbor {<ip-address> <WORD>} update-source <IFNAME> no neighbor {<ip-address> <WORD>} update-source <IFNAME>
	Configure the update source. The “ no neighbor {<ip-address> <WORD>} update-source <IFNAME> ” cancels this configuration
Parameter	<ip-address> : Neighbor IP address <WORD> : Name of peer group <IFNAME> : Name or IP of the interface
Default	Not configured, namely use nearest interface.
Command Mode	BGP route mode
Usage Guide	Specified update source is allowed to connect with any available interface which

normally is the loop back interface. The NO forms restores to the nearest interface update source. Improper update source use may lead to neighbor connection unavailable, while the invalid interface causes problem which is also the reasons we use loop back interfaces. Note: the loop back interface should be maintained with its address accessibility to be able to establish connections when as the update source.

Example	Switch(config-router)#neighbor 10.1.1.66 update-source 192.168.0.1

neighbor version 4

Command	neighbor {<ip-address> <WORD>} version 4
Parameter	Configure the BGP version of the partner. <ip-address> : Neighbor IP address <WORD> : Name of the peer group 4 : Allowed BGP version, 4 only
Default	4
Command Mode	BGP route mode
Usage Guide	Only version 4 is supported so far, so whatever the configuration is the version remains at 4.

Example	Switch(config-router)#neighbor 10.1.1.66 version 4 Switch(config-router)#

neighbor weight

Command	neighbor {<ip-address> <WORD>} weight <0-65535> no neighbor {<ip-address> <WORD>} weight [<0-65535>]
Parameter	Configure the route weight sent from the partner. The “ no neighbor {<ip-address> <WORD>} weight [<0-65535>] ” command restores the default value. <ip-address> : Neighbor IP address. <WORD> : Name of IP address. <0-65535> : Weight.
Default	The default weight acquired from other routers is 0. The default weight on the local static configuration is 32768.
Command Mode	BGP route mode
Usage Guide	The path selecting can be affected through the configuration of the weight. The weight

is only relevant to the router which is not an attribute transmittable to outside.

Example	Switch(config-router)#neighbor 10.1.1.66 weight 500

network (BGP)

Command	network <ip-address/M> [route-map <WORD>] [backdoor] no network <ip-address/M> [route-map <WORD>] [backdoor]
Parameter	Configure the BGP managed network, the route map specified in network application, or set the “back door” for the network. The “no network <ip-address/M>[route-map <WORD>] [backdoor]” command cancels this configuration. <ip-address/M>: Network prefix identifier <WORD>: Name of route-map
Default	-
Command Mode	BGP route mode
Usage Guide	As for BGP routes, specify the route through which the BGP advertisements go. With the network defined by this command, the peer will be spreaded into the route map of the neighbor even if there is no route locally. Using the attribute specified in the network application through route map, when specifying the route comes from EBGP or inside the network through back door parameters, the inside route will be the optimized route even if the external route is of shorter distance.
Example	Switch(config-router)# network 172.16.0.0/16

redistribute (BGP)

Command	redistribute <ROUTES> [route-map <WORD>] no redistribute <ROUTES> [route-map <WORD>]
	redistribute isis: redistribute isis [<WORD>] [<is-type> <level-1> <level-1-2> <level-2>] {[<metric> <NUM>]][<route-map> <NAME>]}
	Set the BGP to redistribute route from other modes into BGP. The “ no redistribute

Parameter	<ROUTES> [route-map <WORD>]" command cancels this configuration.
	<ROUTES>: Route source or protocol, including: connected, ISIS, kernel, OSPF, RIP, static, etc.
	<WORD>: Name of route map.
	<is-type>: level of IS-IS.
	<metric>: Default metric
	<NUM>: <0-4294967295> BGP metric
	<route-map>: Route map reference
Default	<NAME>: route-map name
	-
	-
	-
	-
	-
	-
Command Mode	BGP route mode
Usage Guide	Route from other ways will be distributed into the BGP route table with this command and transmitted to the neighbors.
Example	The static route is introduced into BGP with this configuration and advertised to the neighbors. <pre>Switch(config-router)# redistribute static Switch(config-router)#redistribute isis is-type level-1-2 metric 10</pre>

redistribute ospf

Command	redistribute ospf [<process-id>] [route-map<word>]
	no redistribute ospf [<process-id>]
Parameter	To redistribute routing information form OSPF to BGP. The no form of this command will remove the configuration.
	process-id is the process ID of the OSPF, limited between 1 and 65535. If no process id is specified, the default process id will be used. route-map <word> is the pointer to the introduced routing map.
Default	Not redistributed by default.
Command Mode	BGP route mode
Usage Guide	-
Example	To redistribute routing of OSPF v2 to BGP (as number is 1). <pre>Switch(config)#router bgp 1 Switch(config-router)#redistribute ospf 2</pre>

router bgp

Command	router bgp [<as-id> <WORD>] no router bgp [<as-id> <WORD>]
Parameter	Enable BGP instance. The “no router bgp <as-id>” command deletes BGP instance. <as-id>: AS number, ranging from 1 to 4294967295, it can be shown in decimal notation (such as 6553700) or delimiter method (such as 100.100). <WORD>: AS number in asdot notation
Default	BGP not enabled.
Command Mode	Global mode
Usage Guide	Enable BGP by specified AS, and then enter the config-router state, the protocol can be configured at this prompt.
Example	Enable BGP, AS number is 4294967295 in decimal notation. <pre>Switch(config)#router bgp 4294967295 Switch(config-router)#exit</pre> Enable BGP, AS number is 4294967295 in delimiter method. <pre>Switch(config)#router bgp 65535.65535 Switch(config-router)#exit</pre>

timers bgp

Command	timers bgp <0-65535> <0-65535> no timers bgp [<0-65535> <0-65535>]
Parameter	Configure all neighbor time in BGP. The “no timers bgp [<0-65535> <0-65535>]” command restores these times to default value. <0-65535>: Respectively the KEEPALIVE interval and the hold time.
Default	KEEPALIVE is 60s, HOLD TIME is 180s.
Command Mode	Admin and Configuration Mode.
Usage Guide	Similar to neighbor time configuration which just performed on all neighbors
Example	<pre>Switch(config-router)# timers bgp 50 200</pre>

show ip bgp

Command	show ip bgp [<ADDRESS-FAMILY>] [<ip-address> <ip-address/M>] [<cidr-only>]
Parameter	For displaying the routing messages permitted by BGP. <ADDRESS-FAMILY>: address-family such as "ipv4 unicast"; <ip-address>: IP address; <ip-address/M>: IP address and the mask <cidr-only>: only routes with non-natural netmasks
Default	-
Command Mode	Admin and Configuration Mode.
Usage Guide	We can display BGP routing messages by different parameters (such as address-family or IPv4 address), or a route covered by a prefix, or only the routing message don't match the earliest IP address-family (namely the route is not A or B or C type address.)
Example	<pre>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</pre>

show ip bgp attribute-info

Command	show ip bgp attribute-info
Parameter	Display the BGP attributes messages. -
Default	-
Command Mode	Admin and Configuration Mode.
Usage Guide	For displaying the attribute messages permitted by BGP.
Example	<pre>Switch#show ip bgp attribute-info attr[1] nexthop 0.0.0.0 attr[1] nexthop 10.1.1.64</pre>

```
attr[3] nexthop 10.1.1.64
attr[1] nexthop 10.1.1.121
attr[2] nexthop 10.1.1.200
```

show ip bgp community

Command	show ip bgp [<ADDRESS-FAMILY>] community <TYPE> [exact-match]
Parameter	For displaying route permitted by BGP with community information. <ADDRESS-FAMILY>: Address-family, such as "ipv4 unicast" <TYPE>: Community attributes number show in AA:NN form or combination of local-AS, no-advertise, and no-export.
Default	-
Command Mode	Admin and Configuration Mode.
Usage Guide	We can choose several communities at a time, exact-match shows only the perfect match entries will be 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, 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

show ip bgp community-info

Command	show ip bgp community-info
Parameter	For displaying the community messages permitted by BGP.
Default	-
Command Mode	Admin and Configuration Mode.
Usage Guide	Messages in the same community multiply closable at the same time.

Example	<pre>Switch#show ip bgp community-info Address Refcnt Community [0x3312558] (3) 100:50</pre>
show ip bgp community-list	
Command	show ip bgp [<ADDRESS-FAMILY>] community-list <NAME> [exact-match]
Parameter	For displaying the routes containing the community list messages and permitted by BGP <ADDRESS-FAMILY>: Address-family such as "ipv4 unicast" <NAME>: Community list
Default	-
Command Mode	Admin and Configuration Mode.
Usage Guide	Configure the community list with ip community-list command and the contained community as well. When displayed with its name, communities included in all the lists are contained.
Example	<pre>Switch(config)#ip community-list commu per 100:50 Switch#show 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</pre>

show ip bgp dampening

Command	show ip bgp [<ADDRESS-FAMILY>] dampening {<dampened-paths> <flap-statistics> <parameters>}
Parameter	Display the routes permitted by BGP and relevant to the route dampening. <ADDRESS-FAMILY>: Address-family, such as "ipv4 unicast".
Default	-

Command Mode	Admin and Configuration Mode.
Usage Guide	Only the surged routes will be displayed. The Parameters shows the display configuration other than specific routes. The other two options will respectively show the restrained route and the dampening (recently recovered from invalid) routing messages.
Example	<pre> Switch#show 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#show 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#show ip bgp dampening parameters dampening 15 750 2000 60 15 (route-map rmp) Reachability Half-Life time : 15 min Reuse penalty : 750 Suppress penalty : 2000 Max suppress time : 60 min Un-reachability Half-Life time : 15 min Max penalty (ceil) : 11999 Min penalty (floor) : 375 Total number of prefixes 1 </pre>

show ip bgp filter-list

Command	show ip bgp [<ADDRESS-FAMILY>]filter-list [<WORD >]
Parameter	For displaying the routes in BGP meeting the specific AS filter list. <ADDRESS-FAMILY>: address-family such as "ipv4 unicast" < WORD >: AS-PATH access-list name
Default	-

Command Mode	Admin and Configuration Mode.
Usage Guide	Configure AS access-list with ip as-path access-list command. This command can show the routes passed the access-list.
Example	<pre>Switch#show 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</pre>

show ip bgp inconsistent-as

Command	show ip bgp [<ADDRESS-FAMILY>] inconsistent-as
Parameter	For displaying routes with inconsistent BGP AS. <ADDRESS-FAMILY> : address family such as "ipv4 unicast".
Default	-
Command Mode	Admin and Configuration Mode.
Usage Guide	If same prefix comes from different origin AS, the AS will be regarded as inconsistent. This command is for displaying this kind of routes.
Example	<pre>Switch#show 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</pre>

show ip bgp neighbors

Command	show ip bgp [<ADDRESS-FAMILY>] neighbors [IP-ADDRESS] [advertised-routes received-prefix-filter received-routes routes]

	For displaying the BGP neighbor related messages.
Parameter	<ADDRESS-FAMILY> : Address-family, such as "ipv4 unicast" <ip-address> : Neighbor IP address
Default	-
Command Mode	Admin and Configuration Mode.
Usage Guide	Display detailed messages of all neighbors by this command without parameters. Specifying IP address will show the detailed information of the neighbors with specified IP address. The advertised-routes、received prefix-filter、received routes、routes parameters will respectively displays the routes broadcast on local side, the received prefix filter, received routes (soft reconfiguration enabled) and the routing message from specific neighbor.
Example	<pre>Switch#show 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, keepalive 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</pre>

show ip bgp paths

Command	show ip bgp [<ADDRESS-FAMILY>] paths

Parameter	Display the path message permitted by BGP.
	<ADDRESS-FAMILY> : Address-family such as "ipv4 unicast".
Default	-
Command Mode	Admin and Configuration Mode.
Usage Guide	Display the BGP path message includes the utilization state.
Example	<pre>Switch#show ip bgp paths Address Refcnt Path [0x331dad0:0] (1) [0x331d850:93] (1) 600 [0x331d8d8:249] (2) 200 300</pre>

show ip bgp prefix-list

Command	show ip bgp [<ADDRESS-FAMILY>] prefix-list [<NAME>]
	For displaying the route meet the specific prefix-list in BGP.
Parameter	<ADDRESS-FAMILY>: Address family such as “ipv4 unicast” <NAME>: Name of prefix-list
Default	-
Command Mode	Admin and Configuration Mode.
Usage Guide	We can select the required BGP route by regular expression.
Example	Switch(config)#ip prefix-list PL permit any Switch(config)# Switch#show 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

show ip bgp quote-regexp

Command	show ip bgp [<ADDRESS-FAMILY>] quote-regexp [<WORD>]
Parameter	For displaying the BGP route meets the specific AS related regular expression. <ADDRESS-FAMILY > : address-family such as "ipv4 unicast" <WORD> : Regular expression
Default	-
Command Mode	Admin and Configuration Mode.
Usage Guide	Selecting the required route through regular expressions.
Example	Switch#show 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

show ip bgp redistribute

Command	show ip bgp redistribute show ip bgp redistribute vrf < WORD >
Parameter	To display redistributed routing information from external processes to BGP < WORD > : Name of vrf
Default	-
Command Mode	Admin mode and Command Mode。
Usage Guide	Displaying the redistribution configuration and the routes injected into BGP from protocols.

Example	Switch#show ip bgp redistribute Switch# show ip bgp redistribute vrf abc

show ip bgp neighbors

Command	show ip bgp neighbors
Parameter	Show neighbor information of specified BGP or total BGP processes.
Default	-
Command Mode	Admin mode and Command Mode.
Usage Guide	-。
Example	Switch#show ip bgp neighbors

show ip bgp regexp

Command	show ip bgp [<ADDRESS-FAMILY>] regexp [<LINE>]
Parameter	For displaying the BGP routes meets specific AS related normal expressions. <ADDRESS-FAMILY > : address-family such as "ipv4 unicast" <LINE> : Regular expression
Default	-
Command Mode	Admin and Configuration Mode.
Usage Guide	We can select BGP route of the required AS with normal expression.
Example	Switch#show 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

show ip bgp route-map

Command	show ip bgp [<ADDRESS-FAMILY>] route-map [<NAME>]
Parameter	For displaying the BGP routes meets the specific related route map. <ADDRESS-FAMILY > : such as "ipv4 unicast" <NAME> : Name of route map
Default	-
Command Mode	Admin and Configuration Mode.
Usage Guide	Configure the route map with the route-map command, through which it can be displayed that process routes with route map. The command will display the routes meet specific route map.
Example	Switch#show 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

show ip bgp scan

Command	show ip bgp scan
Parameter	For displaying BGP scan messages.
Default	-
Command Mode	Admin and Configuration Mode.
Usage Guide	Scan regularly the nexthop messages. The command can show the current 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:

show ip bgp summary

Command	show ip bgp [<ADDRESS-FAMILY>] summary																													
	For displaying the BGP summary information.																													
Parameter	<ADDRESS-FAMILY>: Address-family such as "ipv4 unicast".																													
Default	-																													
Command Mode	Admin and Configuration Mode.																													
Usage Guide	Display some basic summary information of BGP																													
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 <table><tr><th>Display Contents</th><th>Explanation</th></tr><tr><td>identifier</td><td>Local identifier</td></tr><tr><td>local AS number</td><td>The number of AS of local router</td></tr><tr><td>table version</td><td>the version number of BGP interior database</td></tr><tr><td>AS-PATH entries</td><td>The tabulation of the AS-PATH entries</td></tr><tr><td>community entries</td><td>The property of the community entries</td></tr><tr><td>Neighbor</td><td>Neighbor address</td></tr><tr><td>V</td><td>The BGP version of neighbor running</td></tr><tr><td>AS</td><td>The AS number of neighbor what is affiliated with</td></tr><tr><td>MsgRcvd</td><td>The amount of message received from neighbor</td></tr><tr><td>MsgSent</td><td>The amount of message sent to the neighbor</td></tr><tr><td>TblVer</td><td>the version of route table</td></tr><tr><td>Up/Down</td><td>It will display the conversation time length if the state with neighbor was established, otherwise display the present status.</td></tr><tr><td>State/PfxRcd</td><td>If the state is established, display the amount of the prefix received of the router.otherwise,display the state of the neighbor at present.</td></tr></table>		Display Contents	Explanation	identifier	Local identifier	local AS number	The number of AS of local router	table version	the version number of BGP interior database	AS-PATH entries	The tabulation of the AS-PATH entries	community entries	The property of the community entries	Neighbor	Neighbor address	V	The BGP version of neighbor running	AS	The AS number of neighbor what is affiliated with	MsgRcvd	The amount of message received from neighbor	MsgSent	The amount of message sent to the neighbor	TblVer	the version of route table	Up/Down	It will display the conversation time length if the state with neighbor was established, otherwise display the present status.	State/PfxRcd	If the state is established, display the amount of the prefix received of the router.otherwise,display the state of the neighbor at present.
Display Contents	Explanation																													
identifier	Local identifier																													
local AS number	The number of AS of local router																													
table version	the version number of BGP interior database																													
AS-PATH entries	The tabulation of the AS-PATH entries																													
community entries	The property of the community entries																													
Neighbor	Neighbor address																													
V	The BGP version of neighbor running																													
AS	The AS number of neighbor what is affiliated with																													
MsgRcvd	The amount of message received from neighbor																													
MsgSent	The amount of message sent to the neighbor																													
TblVer	the version of route table																													
Up/Down	It will display the conversation time length if the state with neighbor was established, otherwise display the present status.																													
State/PfxRcd	If the state is established, display the amount of the prefix received of the router.otherwise,display the state of the neighbor at present.																													

debug bgp

Command	debug bgp [<MODULE> all] no debug bgp [<MODULE> all]
Parameter	For BGP debugging. The “ no debug bgp [<MODULE> all] ” command closes the BGP debugging messages <MODULE> : BGP module names, including dampening、events、filters、fsm、keepalives、nsm、updates, etc.
Default	None.
Mode	Admin Mode
Usage Guide	For monitoring BGP events and the encountered errors, warning messages.
Example	Display the debugging messages of all bgp modules. Switch#debug bgp all

debug bgp redistribute message send

Command	debug bgp redistribute message send no debug bgp redistribute message send
Parameter	To enable debugging switch of sending messages for redistribution of routing information from external process such as OSPF and RIP to BGP. The no command will disable the debugging switch. -
Default	Close the debug by default.
Mode	Admin Mode
Usage Guide	-
Example	Switch# debug bgp redistribute message send Switch# no debug bgp redistribute message send

debug bgp redistribute route receive

Command	debug bgp redistribute route receive no debug bgp redistribute route receive

	To enable debugging switch of received messages from NSM for BGP. The no form of this command will disable debugging switch of received messages from NSM for BGP.
Parameter	-
Default	Close the debug by default.
Mode	Admin Mode
Usage Guide	-
Example	Switch#debug bgp redistribute route receive Switch#no debug bgp redistribute route receive

bgp graceful-restart

Command	bgp graceful-restart no bgp graceful-restart
	Enable BGP to support GR and set restart-time and stale-path-time as the default value, no command disables GR.
Parameter	-
Default	Do not enable BGP to support GR.
Mode	BGP router configuration mode
Usage Guide	-
Example	Configure GR. Switch(config-router)# bgp graceful-restart

bgp graceful-restart restart-time

Command	bgp graceful-restart restart-time <1-3600> no bgp graceful-restart restart-time <1-3600>
	Configure BGP GR's restart-time (Receiving Speaker enables a timeout timer for a neighbor, it uses the restart-time as the timeout). A restart-time specifies the longest waiting time from Receiving Speaker finds restarting to the received OPEN messages. If Receiving Speaker does not receive OPEN messages after exceed the time, it can delete SATLE route saved by neighbor. No command restores restart-time as the default value of 120 seconds.
Parameter	<1-3600>: time in seconds.

Default	restart-time uses the default value of 120s.
Mode	BGP router configuration mode
Usage Guide	-
Example	Configure restart-time as 60s for BGP GR Switch(config-router)# bgp graceful-restart restart-time 60

bgp graceful-restart stale-path-time

Command	bgp graceful-restart stale-path-time <1-3600> no bgp graceful-restart stale-path-time <1-3600>
	Configure stale-path-time for BGP GR. Specify the longest waiting time that delete stale route from the received OPEN messages to the received EOR for Receiving Speaker. No command restores stale-path-time as the default value of 360 seconds.
Parameter	<1-3600>: time in seconds
Default	stale-path-time uses the default value of 360s.
Mode	BGP router configuration mode
Usage Guide	-
Example	Configure stale-path-time as 460s for BGP GR. Switch(config-router)# bgp graceful-restart stale-path-time 460

bgp selection-deferral-time

Command	bgp selection-deferral-time <1-3600> no bgp selection-deferral-time <1-3600>
	Configure selection-deferral-time for BGP GR. Specify the longest waiting time that start to count selection route from the received OPEN messages to the received EOR for

Restarting Speaker. If Restarting Speaker does not receive EOR after exceed the time, it can count selection route. No command restores selection-deferral-time as the default value of 120 seconds.

Parameter	<1-3600>: time in seconds
Default	selection-deferral-time uses the default value of 120s.
Mode	BGP router configuration mode
Usage Guide	-
Example	Configure selection-deferral-time as 240s for BGP GR. Switch(config-router)# bgp selection-deferral-time 240

neighbor restart-time

Command	neighbor (<ip-address> <WORD>) restart-time <1-3600> no neighbor (<ip-address> <WORD>) restart-time <1-3600>
Parameter	Configure restart-time for neighbors, no command restores the default time. (<ip-address> <WORD>): name of neighbor address or neighbor group for BGP <1-3600>: time in seconds.
Default	The default restart-time is 120s for neighbor.
Mode	BGP protocol unicast address family mode
Usage Guide	Configures the restart time for a BGP neighbor or neighbor group. The restart time specifies the maximum time (in seconds) the local BGP speaker waits for the neighbor to re-establish a BGP session after a restart. The no form restores the default value.
Example	Configure restart-time as 60s for neighbor 1.1.1.1. Switch(config-router)# neighbor restart-time 60

maximum-paths

Command	maximum-paths ebgp <1-32> maximum-paths eibgp <1-32> maximum-paths ibgp <1-32>
Parameter	Configure the maximum number of multipaths in the BGP routing table. <1-32> Path type
Default	

Mode	BGP route mode
Usage Guide	-
Example	The maximum number of paths configured for the ebgp type is 3. Switch(config-router)# maximum-paths ebgp 3

load-balancing

Command	load-balancing eibgp ignore no load-balancing eibgp ignore
Parameter	Configure load balancing. none
Default	
Mode	BGP route mode
Usage Guide	Configures BGP load balancing. The load-balancing eibgp ignore command ignores the EBGp/IBGP distinction when selecting multipath routes. The no form restores the default behavior.
Example	Configure to ignore EIBGP load balancing. Switch(config-router)# load-balancing eibgp ignore

neighbor password

Command	neighbor (A.B.C.D X:X::X:X WORD) password (0 LINE 7 WORD LINE) no neighbor (A.B.C.D X:X::X:X WORD) password
Parameter	Configure the neighbor password. A.B.C.D : The IP address of the neighbor. X:X::X:X : The IPv6 address of the neighbor. WORD : Neighborhood group marking.
Default	
Mode	BGP route mode
Usage Guide	Neighbors can be created by configuring the neighbor password. If both sides have the same password, neighbors can be created.
Example	Switch(config-router)# neighbor 1.1.1.4 password 444

4 Commands for RIPng

clear ipv6 rip route

Command	<code>clear ipv6 rip route { <ipv6-address > kernel static connected rip ospf isis bgp all }</code>
Parameter	Clear specific route from the RIPng route table. Clears the route exactly match with the destination address from the RIP route table. <ipv6-address > is the destination address shown in hex notation with prefix length. kernel delete kernel route from the RIPng route table static delete static route from the RIPng route table connected delete direct route from the RIPng route table rip delete RIPng route from the RIPng route table only ospf delete IPv6 OSPF route from the RIPng route table only bgp delete IPv6 BGP route from the RIPng route table only ISIS delete ipv6 isis route from the RIPng route table only all delete all routes from the RIPng route table
Default	No default configuration
Mode	Admin mode
Usage Guide	All routes in the RIPng route table will be deleted by using this command with all parameters.
Example	<pre>Switch#clear ipv6 rip route 2001:1:1::/64 Switch#clear ipv6 rip route ospf</pre>

default-information originate

Command	<code>default-information originate</code> <code>no default-information originate</code>
Parameter	Permit redistributing the network 0:: into RIPng. The “no default-information originate” disables this function. -
Default	Disabled

Mode	Router mode
Usage Guide	-
Example	Switch# config terminal Switch(config)# router ipv6 rip Switch(config-router)# default-information originate

default-metric

Command	default-metric <value> no default-metric
	Set the default metric route value of the introduced route; the “ no default-metric ” restores the default value.
Parameter	<value> is the route metric value to be set, ranging between 1 ~ 16.
Default	Default route metric value is 1.
Mode	Router mode
Usage Guide	default-metric command is used for setting the default route metric value of the routes from other routing protocols when distributed into the RIPv6 routes. When using the redistribute commands for introducing routes from other protocols, the default route metric value specified by default-metric will be adopted if no specific route metric value is set.
Example	Set the default route metric value of the routes from other routing protocols when distributed into the RIPv6 routes as 3. Switch(config)# router ipv6 rip Switch(config-router)# default-metric 3

distance

Command	distance <number> [<ipv6-address>] [<access-list-name access-list-number >] no distance [<ipv6-address >]
	Set the managing distance with this command. The “no distance [<A.B.C.D/M>]” command restores the default value to 120.
Parameter	<number> specifies the distance value, ranging between 1-255. < ipv6-address > is the local link address or its prefix. <access-list-name access-list-number > specifies the access-list number or name applied.
Default	The default managing distance of RIPv6 is 120.

Mode	Router mode and address-family mode.
Usage Guide	In case there are routes from two different routing protocols to the same destination, the managing distance is then used for selecting routes. The less the managing distance of the route protocol is, the more reliable will be the route acquired from the protocol.
Example	<pre>Switch# config terminal Switch(config)# router ipv6 rip Switch(config-router)# distance 8 fe80:1111::4200:21ff:fe00:11 mylist</pre>

distribute-list

Command	<pre>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>]</pre>
Parameter	This command uses access-list or prefix-list to filter the route renews messages sent and received. The “no distribute-list {access-list-name> prefix<prefix-list-name>} {in out} [<ifname> vlan <vlan-id>]” command cancels this filter function. <access-list-number access-list-name> is the name or access-list number to be applied. <prefix-list-name> is the name of the prefix-list to be applied. <ifname> specifies the name of interface to be applied with route filtering.
Default	Function disabled by RIPng by default.
Mode	Router mode
Usage Guide	The filter will be applied to all interfaces if no specific interface is set.

Example	<pre>Switch# config terminal Switch(config)# router ipv6 rip Switch(config-router)# distribute-list prefix myfilter in vlan 1</pre>

debug ipv6 rip

Command	<pre>debug ipv6 rip [events nsm packet[recv send][detail]] all] no debug ipv6 rip [events nsm packet[recv send][detail]] all]</pre>
	For opening various debugging switches of RIPng, showing various debugging messages. The “no debug ipv6 rip [events nsm packet [recv send][detail]] all]”

	command closes the corresponding debugging switch.
Parameter	events shows the debugging message of RIPng events nsm shows the communication messages between RIPng and NSM. packet shows the debugging messages of RIPng data packets recv shows the messages of the received data packets send shows the messages of the sent data packets detail shows the messages of the data packets received or sent.
Default	Not enabled
Mode	Admin mode
Usage Guide	-
Example	<pre>Switch#debug ipv6 rip packet Switch#1970/01/01 21:15:08 IMI: SEND[Ethernet1/4]: Send to [ff02::9]:521 1970/01/01 21:15:08 IMI: SEND[Ethernet1/2]: Send to [ff02::9]:521 1970/01/01 21:15:09 IMI: RECV[Ethernet1/4]: Receive from [fe80::20b:46ff:fe57:8e60]:521 1970/01/01 21:15:09 IMI: RECV[Ethernet1/4]: 3000:1:1::/64 is filtered by access-list dclist 1970/01/01 21:15:09 IMI: RECV[Ethernet1/4]: 3ffe:1:1::/64 is filtered by access-list dclist 1970/01/01 21:15:15 IMI: RECV[Ethernet1/2]: Receive from [fe80::203:fff:fe01:257c]:521</pre>

debug ipv6 rip redistribute message send

Command	debug ipv6 rip redistribute message send no debug ipv6 rip redistribute message send
	To enable the debugging of sending messages for routing redistribution messages from OSPFv3 or other external process for RIPng. The no form of this command will disable the debugging messages.
Parameter	None.
Default	Close the debug by default.
Mode	Admin mode
Usage Guide	-
Example	<pre>Switch#debug ipv6 rip redistribute message send Switch#no debug ipv6 rip redistribute message send</pre>

debug ipv6 rip redistribute route receive

Command	debug ipv6 rip redistribute route receive no debug ipv6 rip redistribute route receive
Parameter	To enable the debugging switch received from NSM for redistribution of routing information for RIPng. The no form of this command will disable the debugging switch. None.
Default	Close the debug by default.
Mode	Admin mode
Usage Guide	-
Example	Switch#debug ipv6 rip redistribute route receive Switch#no debug ipv6 rip redistribute route receive

ipv6 rip aggregate-address

Command	ipv6 rip aggregate-address X:X::X:X/M no ipv6 rip aggregate-address X:X::X:X/M
Parameter	To configure IPv6 aggregation route. The no form of this command deletes the IPv6 aggregation route. X:X::X:X/M : IPv6 address and prefix length.
Default	No aggregation route configured.
Mode	Router mode or Interface Configuration Mode.
Usage Guide	If to configure aggregation route under router mode, RIPng protocol must be enabled. If configured under interface configuration mode, RIPng protocol may not be enabled, but the aggregation route can operation after the RIPng protocol be enabled on interface.
Example	Switch(config)#router ipv6 rip Switch(config-router)#ipv6 rip agg 2001:3f:ed8::99/64

ipv6 rip split-horizon

Command	ipv6 rip split-horizon [poisoned] no ipv6 rip split-horizon

Parameter	Permit the split horizon. The “ no ipv6 rip split-horizon ” disables the split horizon.
	[poisoned] configures split horizon with poison reverse.
Default	Split horizon with poison reverse.
Mode	Interface Configuration Mode.
Usage Guide	The split horizon is for preventing the routing loops, namely preventing the layer 3 switch from broadcasting a route at the interface from which the very route is learnt. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.
Example	Switch#config terminal Switch(config)#interface Vlan1 Switch(Config-if-Vlan1)#ipv6 rip split-horizon poisoned

ipv6 router rip

Command	ipv6 router rip
	no ipv6 router rip
	Enable RIPng on the interface. The “no ipv6 router rip” command disables RIPng on the interface.
Parameter	-
Default	Not configured
Mode	Interface Configuration Mode.
Usage Guide	The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.
Example	Switch#config terminal Switch(config)#interface Vlan1 Switch(Config-if-Vlan1)#ipv6 router rip

neighbor

Command	neighbor <ipv6-address> {<ifname> vlan <vlan-id>} no neighbor <ipv6-address> {<ifname> vlan <vlan-id>}
	Specify the destination address for fixed sending. The “ no neighbor <ipv6-address> <ifname> vlan <vlan-id>” cancels the specified address defined and restores all trusted gateways.
Parameter	<ipv6-address> is the IPv6 Link-local address specified for sending and shown in colon hex notation without the prefix length. <ifname> is the name of interface.
Default	Not sending to any fixed destination address.
Mode	Router mode
Usage Guide	When used associating passive-interface command it would be able to send routing messages to specified neighbor only.
Example	Switch#config terminal Switch(config)#router ipv6 rip Switch(config-router)#neighbor FE80:506::2 Vlan1

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>]
	Add an offset value on the routing metric value learnt by RIPv2. The “ no offset-list <access-list-number>[access-list-name] {in out} <number >[<ifname> vlan <vlan-id>]” command disables this function.
Parameter	< access-list-number [access-list-name]> is the access-list or name to be applied. <number > is the additional offset value, ranging between 0-16; <ifname> is the name of specific interface.
Default	The default offset value is the metric value of the interface defined by the system.
Mode	Router mode.
Usage Guide	-

Example	Switch#config terminal Switch(config)#router ipv6 rip Switch(config-router)#offset-list 1 in 5 Vlan1
passive-interface	
Command	passive-interface[<ifname>] vlan <vlan-id>] no passive-interface[<ifname>] vlan <vlan-id>]
Parameter	Set the RIPng layers 3 switches to block RIPng broadcast on the specified interfaces, and only send the RIPng data packet to the layer 3 switch which is configured with neighbor <ifname> is the specific interface name.
Default	Not configured
Mode	Router mode。
Usage Guide	-
Example	Switch#config terminal Switch(config)#router ipv6 rip Switch(config-router)#passive-interface Vlan1

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>]
Parameter	Introduce the routes learnt from other routing protocols into RIPng. kernel introduce from kernel routes connected introduce from direct routes static introduce from static routes ospf introduce from IPv6 OSPF routes isis introduce from IPv6 ISIS routes bgp introduce from IPv6 BGP routes <value> is the metric value assigned to the introduced route, ranging between 0-16

<word> is the probe pointing to the route map for introducing routes

Default

-

Mode

Router mode and address-family mode。

Usage Guide

Under the address-family mode, the parameter kernel and ISIS is unavailable.

Example

```
Switch#config terminal
Switch(config)#router rip
Switch(config-router)#redistribute kernel route-map ipi
To redistribute OSPFv2 routing information to RIP.
Switch(config)#router rip
Switch(config-router)#redistribute ospf 2
```

redistribute ospf

Command

redistribute ospf [<process-tag>] [metric<value>] [route-map<word>]
no redistribute ospf [<process-tag>]

To redistribute routing information from external OSPFv3 processes to RIPng process.
The no form of this command will remove the introduced OSPFv3 routing entries.

Parameter

process-tag is the string tag for OSPFv3 process with maximum length limited within 15 characters. If not specified, the default process will be used.
metric <value> is the metric for the introduced routing entries, limited between 0 and 16.
route-map <word> is the pointer to the introduced routing map.

Default

Not redistributed by default.

Mode

RIPng Configuration Mode.

Usage Guide

-

Example

```
To redistribute OSPFv3 ABC routing ro RIPng.
Switch(config)#router ipv6 rip
Switch(config-router)#redistribute ospf abc
```

route

Command

route <ipv6-address>
no route <ipv6-address>

This command configures a static RIPng route. The “**no route <ipv6-address>**” command deletes this route.

Parameter	<ipv6-address> Specifies this destination IPv6 address prefix and its length show in colon hex notation.
Default	-
Mode	Router mode。
Usage Guide	The command adds a static RIPng route, and is mainly used for debugging. Routes configured by this command will not appear in kernel route table but in the RIPng route database, however it could be located by using the show ipv6 rip command.
Example	Switch#config terminal Switch(config)#router ipv6 rip Switch(config-router)#route 3ffe:1234:5678::1/64

router ipv6 rip

Command	router ipv6 rip no router ipv6 rip
	Enable RIPng routing process and entering RIPng mode; the “ no router ipv6 rip ” of this command disables the RIPng routing protocol.
Parameter	
Default	RIPng routing not running.
Mode	Global mode
Usage Guide	This command is for enabling the RIPng routing protocol, this command should be enabled before performing other global configuration of the RIPng protocol.
Example	Enable the RIPng protocol mode. Switch(config)#router ipv6 rip

show debugging ipv6 rip

Command	show debugging ipv6 rip
	Show RIPng debugging status for following debugging options: nsm debugging, RIPng

event debugging, RIPng packet debugging and RIPng nsm debugging.

Parameter	
Default	-
Mode	Admin mode
Usage Guide	-
Example	Switch#show debugging ipv6 rip RIPng debugging status: RIPng event debugging is on RIPng packet send detail debugging is on RIPng NSM debugging is on

show ipv6 rip interface

Command	show ipv6 rip interface [<IFNAME> vlan <WORD>]	
	Make sure the interface and line protocols is up.	
Parameter	<IFNAME>	Interface information
	<WORD>	vlan
Default	-	
Mode	Admin mode	
Usage Guide	-	
Example	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	

Displayed information	Explanations
Vlan1 is up, line protocol is up	Interface is Up
Routing Protocol: RIP	The routing protocol running on the interface is RIPng
Passive interface: Disabled	Passive-interface disabled
Split horizon: Enabled with Poisoned Reversed	The split horizon is enabled with poisoned reversed on the interface.
IP interface address: 3000:1:1::1/64 fe80::203:fff:fe01:429e/64	IPv6 address of the interface

show ipv6 rip redistribute

Command	show ipv6 rip redistribute
Parameter	Show the configuration information of redistributed other out routing to RIPv6. -
Default	Not shown by default.
Mode	Admin mode
Usage Guide	-
Example	Switch#show ipv6 rip redistribute

show ipv6 protocols rip

Command	show ipv6 protocols rip
Parameter	Show the RIPv6 process parameters and statistic messages. -
Default	-
Mode	Admin mode
Usage Guide	-
Example	Switch(config)#show ipv6 protocols rip Routing Protocol is "ripng" Sending updates every 30 seconds with +/-50%, next due in 1 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 Ethernet1/4 filtered by dclist Default redistribute metric is 1 Redistributing: static Interface Vlan10 Vlan2 Routing for Networks:

Displayed information	Explanations
Sending updates every 30 seconds with +/-50%, next due in 1 seconds	Sending updates every 30 seconds

Timeout after 180 seconds, garbage collect after 120 seconds	The route timeout time is 180 seconds, the garbage collect time is 120 seconds
Outgoing update filter list for all interface is not set	Outgoing update filter list for all interface is not set
Incoming update filter list for all interface is not set	Incoming update filter list for all interface is not set
Default redistribution metric is 1	Default redistribution metric is 1
Redistributing: static	Redistricting the static route into the RIP routes
Interface Vlan10 Vlan2	The interfaces running RIP is Vlan 10 and Vlan 2

show ipv6 rip

Command	show ipv6 rip																														
	Show RIPng Routing.																														
Parameter	-																														
Default	-																														
Mode	Admin mode																														
Usage Guide	-																														
Example	Switch#show ipv6 rip Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP, a - aggregate, s - suppressed <table><thead><tr><th>Network</th><th>Next Hop</th><th>If</th><th>Met</th><th>Tag</th><th>Time</th></tr></thead><tbody><tr><td>R 2000:1:1::/64</td><td>::</td><td>Vlan2</td><td>1</td><td></td><td>0</td></tr><tr><td>R 2001:1:1::/64</td><td>fe80::203:fff:fe01:257c</td><td>Vlan2</td><td>2</td><td>0</td><td>02:40</td></tr><tr><td>R 3000:1:1::/64</td><td>::</td><td>Vlan10</td><td>1</td><td></td><td>0</td></tr><tr><td>R 3010:1:1::/64</td><td>::</td><td>--</td><td>1</td><td></td><td>0</td></tr></tbody></table> Amongst R stands for RIP route, namely a RIP route with the destination network address 2001:1:1::/64, next-hop address at fe80::203:fff:fe01:257c. It is learnt from the Ethernet port VLAN2 with a metric value of 2, and still has 2 minutes 40 seconds before time out.	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
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																										

show ipv6 rip database

Command	show ipv6 rip database
Parameter	Show messages related to RIPng database.
Default	-
Mode	Admin mode
Usage Guide	-
Example	Switch#show ipv6 rip database

show ipv6 rip aggregate

Command	show ipv6 rip aggregate																									
Parameter	To display the information of IPv6 aggregation route.																									
Default	-																									
Mode	Admin mode																									
Usage Guide	This command is used to display which interface the aggregation route be configured, Metric, Count, Suppress and so on, if configured under global mode, then the interface display "----". "Metric" is metric. "Count" is the number of learned aggregation routes. "Suppress" is the times of aggregation.																									
Example	To display the information of IPv6 aggregation route. Switch(config-router)#show ipv6 rip agg Aggregate information of ripng <table><tr><th>Network</th><th>Aggregated Ifname</th><th>Metric</th><th>Count</th><th>Suppress</th></tr><tr><td>2001::/16</td><td>Vlan1</td><td>1</td><td>2</td><td>0</td></tr><tr><td>2001:1::/32</td><td>----</td><td>1</td><td>2</td><td>0</td></tr><tr><td>2001:1:2::/60</td><td>Vlan1</td><td>1</td><td>1</td><td>1</td></tr><tr><td></td><td>----</td><td>1</td><td>1</td><td>1</td></tr></table>	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
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																						

timers basic

Command	timers basic <update> <invalid> <garbage> no timers basic
Parameter	Adjust the RIP timer update, timeout, and garbage collecting time. The “no timers basic” command restores each parameter to their default values. <update> time interval of sending update packet, shown in seconds and ranging between 5-2147483647; <invalid> time period after which the RIP route is advertised dead, shown in seconds and ranging between 5-2147483647; <garbage> is the hold time in which the a route remains in the routing table after advertised dead, shown in seconds and ranging between 5-2147483647.
Default	<update> defaulted at 30; <invalid> defaulted at 180; <garbage> defaulted at 120
Mode	Router mode。
Usage Guide	The system is defaulted broadcasting RIPv6 update packets every 30 seconds; and the route is considered invalid after 180 seconds but still exists for another 120 seconds before it is deleted from the routing table.
Example	Set the RIP update time to 20 seconds and the timeout period to 80 seconds, the garbage collecting time to 60 seconds. <pre>Switch(config)#router ipv6 rip Switch(config-router)#timers basic 20 80 60</pre>

5 Commands for OSPFv3

area default-cost

Command	area <id> default-cost <cost> no area <id> default-cost
Parameter	Configure the cost of sending to the default summary route in stub or NSSA area; the “ no area <id> default-cost ” command restores the default value. <id> is the area number which could be shown as digits 0 ~ 4294967295, or as an IP address; <cost> ranges between <0-16777215>
Default	Default OSPFv3 cost is 1.
Mode	OSPFv3 Configuration Mode.
Usage Guide	The command is only adaptive to the ABR router connected to the stub area.
Example	Set the default-cost of area 1 to 10 Switch(config)#router ipv6 ospf Switch(config-router)#area 1 default-cost 10

area range

Command	area <id> range <ipv6address> [advertise not-advertise] no area <id> range < ipv6address> Aggregate OSPF route on the area border. The “ no area <id> range <address> ” cancels this function.
Parameter	<id> is the area number which could be digits ranging between 0 ~ 4294967295, and also as an IP address. <ipv6address> = <X:X::X:X/M> , Specifies the area ipv6 network prefix and its length; advertise : Advertise this area not-advertise : Not advertise this area If both are not set, this area is defaulted for advertising
Default	Function not configured.
Mode	OSPFv3 Configuration Mode.

Usage Guide	Use this command to aggregate routes inside an area. If the network IDs in this area are not configured continuously, a summary route can be advertised by configuring this command on ABR. This route consists of all single networks belong to specific range.

Example	Switch #config terminal Switch (config)# router ipv6 ospf Switch (config-router)# area 1 range 2000::/3

area stub

Command	area <id> stub [no-summary] no area <id> stub [no-summary]
	Define an area to a stub area. The “ no area <id> stub [no-summary] ” command cancels this function.
Parameter	<id>is the area number which could be digits ranging between 0 ~ 4294967295, and also as an IPv4 address. no-summary: The area border routes stop sending link summary announcement to the stub area
Default	Not defined
Mode	OSPFv3 Configuration Mode.
Usage Guide	Configure area stub on all routes in the stub area. There are two configuration commands for the routers in the stub area: stub and default-cost. All routers connected to the stub area should be configured with area stub command. As for area border routers connected to the stub area, their introducing cost is defined with area default-cost command.

Example	Switch # config terminal Switch (config)# router ipv6 ospf Switch (config-router)# area 1 stub

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]
	Configure a logical link between two backbone areas physically divided by non-backbone area. The “ no area <id> virtual-link A.B.C.D [instance-id <instance-id> INTERVAL] ” command removes this virtual-link.
Parameter	<id> is the area number which could be digits ranging between 0 ~ 4294967295, and

also as an IP address.

<instance-id> is the interface instance ID ranging between 0~255 and defaulted at 0

INTERVAL= [dead-interval|hello-interval|retransmit-interval|transmit-delay]

<value>:The delay or interval seconds, ranging between 1~65535

<dead-interval>: A neighbor is considered offline for certain dead interval without its group messages which the default is 40 seconds.

<hello-interval>: The time interval before the router sends a hello group message, default is 10 seconds

<retransmit-interval>: The time interval before a router retransmitting a group message, default is 5 seconds

<transmit-delay>: The time delay before a router sending a group messages, 1 second by default

Default

No default configuration

Mode

OSPFv3 Configuration Mode.

Usage Guide

In the OSPF all non-backbone areas will be connected to a backbone area. If the connection to the backbone area is lost, virtual link will repair this connection. You can configure virtual link between any two backbone areas routers connected with the public non-backbone area. The protocol treat routers connected by virtual links 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
```

abr-type

Command

abr-type {cisco|ibm| standard}
no abr-type [cisco|ibm| standard]

Configure an OSPF ABR type with this command. The “**no abr-type [cisco|ibm| standard]**” command restores the default.

Parameter

cisco, realize by cisco ABR;
ibm, realize by ibm ABR;
shortcut, specify a shortcut-ABR;
standard, realize with standard (RFC2328) ABR.

Default

Cisco configured by default

Mode

OSPFv3 Configuration Mode.

Usage Guide

For Specifying the realizing type of abr. This command is good for interactive operation among different OSPF realizing method and is especially useful in the multiple host

environment.

Example

```
Configure ABR as standard.  
Switch#config terminal  
Switch(config)#router ipv6 ospf  
Switch(config-router)#abr-type standard
```

default-metric

Command

default-metric <value>
no default-metric

Parameter

The command set the default metric value of OSPF routing protocol; the “**no default-metric**” returns to the default state.

<value>, metric value, ranging between 1~16777214.

Default

Built-in, metric value auto translating.

Mode

OSPFv3 Configuration Mode.

Usage Guide

When the default metric value makes the metric value not compatible, the route introducing still goes through. If the metric value can not be translated, the default value provides alternative option to carry the route introducing on. This command will result in that all introduced route will use the same metric value. This command should be used associating redistribute.

Example

```
Switch#config terminal  
Switch(config)#router ipv6 ospf  
Switch(config-router)#default-metric 100
```

debug ipv6 ospf events

Command

[no]debug ipv6 ospf events [abr|asbr|os|router|vlink]

Open debugging switches showing OSPF events. The “**no debug ipv6 ospf events [abr|asbr|os|router|vlink]**” command closes this debugging switch.

Parameter	
Default	Closed.
Mode	Admin mode
Usage Guide	-
Example	Switch#debug ipv6 ospf events 1970/01/01 01:10:35 IMI: ROUTER[Process:(null)]: GC timer expire

debug ipv6 ospf ifsm

Command	[no]debug ipv6 ospf ifsm [status events timers]
	Open debugging switches showing the OSPF interface states; the “ [no] debug ospf ifsm [status events timers] ” command closes this debugging switches.
Parameter	
Default	Closed.
Mode	Admin mode
Usage Guide	-
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

debug ipv6 ospf lsa

Command	[no]debug ipv6 ospf lsa [generate flooding install maxage refresh]
	Open debugging switches showing showing link state announcements; the “ no debug ospf lsa [generate flooding install maxage refresh] ” closes the debugging switches.
Parameter	Closed.

Default	-
Mode	Admin mode
Usage Guide	-
Example	-

debug ipv6 ospf nfsm

Command	[no]debug ipv6 ospf nfsm [status events timers]
Parameter	Open debugging switches showing showing OSPF neighbor state machine; the “ no debug ipv6 ospf nfsm [status events timers] ” command closes this debugging switch. Closed.
Default	-
Mode	Admin mode
Usage Guide	-
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)

debug ipv6 ospf nsm

Command	[no]debug ipv6 ospf nsm [interface redistribute]
	Open debugging switches showing showing OSPF NSM, the “ no debug ipv6 ospf nsm [interface redistribute] ” command closes this debugging switch.
Parameter	
Default	Closed.
Mode	Admin mode
Usage Guide	-
Example	

debug ipv6 ospf packet

Command	[no]debug ipv6 ospf packet [dd detail hello ls-ack ls-request ls-update recv send]
	Open debugging switches showing OSPF packet messages; the “ no debug ipv6 ospf packet [dd detail hello ls-ack ls-request ls-update recv send] ” command closes this debugging switch.
Parameter	
Default	Closed.
Mode	Admin mode
Usage Guide	-
Example	

debug ipv6 ospf redistribute message send

Command	debug ipv6 ospf redistribute message send no debug ipv6 ospf redistribute message send
	To enable/disable debugging of sending command from IPv6 OSPF process redistributed to other IPv6 OSPF process routing.
Parameter	-
Default	Disabled.
Mode	Admin mode
Usage Guide	-
Example	Switch#debug ipv6 ospf redistribute message send

debug ipv6 ospf redistribute route receive

Command	debug ipv6 ospf redistribute route receive no debug ipv6 ospf redistribute route receive
	To enable/disable debugging of received routing message from NSM for IPv6 OSPF process.
Parameter	-
Default	Disabled.
Mode	Admin mode
Usage Guide	-
Example	Switch#debug ipv6 ospf redistribute route receive

debug ipv6 ospf route

Command	[no]debug ipv6 ospf route [ase ia install spf]
Parameter	Open debugging switches showing OSPF related routes; the " [no]debug ipv6 ospf route [ase ia install spf] " command closes this debugging switch.
Default	Closed.
Mode	Admin mode
Usage Guide	-
Example	Switch#debug ipv6 ospf route spf

ipv6 ospf cost

Command	ipv6 ospf cost <cost> [instance-id <id>] no ipv6 ospf cost [instance-id <id>]
Parameter	Specify the cost required in running OSPF protocol on the interface; the " no ipv6 ospf cost [instance-id <id>] " command restores the default value. <id> is the interface instance ID ranging between 0~255 and defaulted at 0 <cost > is the cost of OSPF protocol ranging between 1~65535.
Default	Default OSPF cost on the interface is 10.
Mode	Interface Configuration Mode.
Usage Guide	The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.
Example	Switch#config terminal Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ipv6 ospf cost 3

ipv6 ospf dead-interval

Command	ipv6 ospf dead-interval <time> [instance-id <id>] no ipv6 ospf dead-interval [instance-id <id>] Specify the dead interval for neighboring layer 3 switch; the " no ipv6 ospf dead-interval [instance-id <id>] " command restores the default value.
Parameter	<id> is the interface instance ID ranging between 0~255 and defaulted at 0 <time> is the length of the adjacent layer 3 switch, in seconds, ranging between 1 ~ 65535
Default	The default dead interval is 40 seconds (normally 4 times of the hello-interval).
Mode	Interface Configuration Mode.
Usage Guide	If no HELLO data packet received after the dead-interval period then this layer 3 switch is considered inaccessible and invalid. This command modifies the dead interval value of neighboring layer 3 switch according to the actual link state. The set dead-interval value is written into the Hello packet and transmitted. To ensure the normal operation of the OSPF protocol, the dead-interval between adjacent layer 3 switches should be in accordance or at least 4 times of the hello-interval value. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.
Example	Switch#config terminal Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ipv6 ospf dead-interval 80

ipv6 ospf display route single-line

Command	[no] ipv6 ospf display route single-line show ipv6 ospf route change the display results of show ipv6 ospf route command. The " no ipv6 ospf display route single-line " restores to default display mode.
Parameter	-
Default	Not configured
Mode	Global Mode
Usage Guide	The show ipv6 ospf route command displays the same route in several lines. This command will strict that one route will be displayed in one line.

Example	Switch#config terminal Switch(config)#ipv6 ospf display route single-line

ipv6 ospf hello-interval

Command	ipv6 ospf hello-interval <time> [instance-id <id>] no ipv6 ospf hello-interval [instance-id <id>]
Parameter	Specify the hello-interval on the interface; the “ no ipv6 ospf hello-interval [instance-id <id>] ” restores the default value. <id> is the interface instance ID ranging between 0~255 and defaulted at 0 <time> is the length of the adjacent layer 3 switch, in seconds, ranging between 1 ~ 65535
Default	Default HELLO packet sending interval is 10 seconds.
Mode	Interface Configuration Mode.
Usage Guide	HELLO data packet is the most common packet which is periodically sent to adjacent layer 3 switch to discover and maintain adjacent relationship, elect DR and BDR. The user set hello-interval value will be written into the HELLO packet and transmitted. The less the hello-interval value is, the sooner the network topological structure is discovered as well larger the cost. To ensure the normal operation of OSPF protocol the hello-interval parameter between the layer 3 switches adjacent to the interface must be in accordance. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example	Switch#config terminal Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ipv6 ospf hello-interval 20

ipv6 ospf network

Command	ipv6 ospf network [broadcast non-broadcast point-to-multipoint point-to-point] no ipv6 ospf network								
Parameter	Specify the OSPFv3 network type. <table> <tr> <td>Broadcast</td><td>Specify the OSPF broadcast multi-point access network</td></tr> <tr> <td>non-broadcast</td><td>Specify the OSPF NBMA network</td></tr> <tr> <td>point-to-multipoint</td><td>Specify an OSPF P2MP network</td></tr> <tr> <td>point-to-point</td><td>Specify the OSPF P2P network</td></tr> </table>	Broadcast	Specify the OSPF broadcast multi-point access network	non-broadcast	Specify the OSPF NBMA network	point-to-multipoint	Specify an OSPF P2MP network	point-to-point	Specify the OSPF P2P network
Broadcast	Specify the OSPF broadcast multi-point access network								
non-broadcast	Specify the OSPF NBMA network								
point-to-multipoint	Specify an OSPF P2MP network								
point-to-point	Specify the OSPF P2P network								

Default	-
Mode	Interface Configuration Mode.
Usage Guide	This command configures the network type of the OSPFv3 network.
Example	<pre>Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ipv6 ospf network ? broadcast Specify OSPF broadcast multi-access network non-broadcast Specify OSPF NBMA network point-to-multipoint Specify OSPF point-to-multipoint network point-to-point Specify OSPF point-to-point network Switch(config-if-vlan1)#ipv6 ospf network broadcast Switch(config-if-vlan1)#</pre>

ipv6 ospf priority

Command	ipv6 ospf priority <priority> [instance-id <id>] no ipv6 ospf priority[instance-id <id>]
Parameter	Configure the priority when electing “Defined layer 3 switch” at the interface. The “no ipv6 ospf [<ip-address>] priority” command restores the default value. <id> is the interface instance ID ranging between 0~255 and defaulted at 0 <priority> is the priority of which the valid value ranges between 0 ~ 255.
Default	The default priority when electing DR is 1.
Mode	Interface Configuration Mode.
Usage Guide	When two layer 3 switches connected to the same segments both want to be the “Defined layer 3 switch”, the priority will decide which one should be chosen. Normally the one with higher priority will be elected, or the one with larger router-id number if the priorities are the same. A layer 3 switch with a priority equal to 0 will not be elected as “Defined layer 3 switch” or “Backup Defined layer 3 switch”. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.
Example	Configure the priority of DR electing. Configure the interface vlan 1 to no election right, namely set the priority to 0. <pre>Switch#config terminal Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ipv6 ospf priority 0</pre>

ipv6 ospf retransmit-interval

Command	ipv6 ospf retransmit-interval <time> [instance-id <id>] no ipv6 ospf retransmit-interval [instance-id <id>]
Parameter	Specify the retransmit interval of link state announcements between the interface and adjacent layer 3 switches. The “no ipv6 ospf retransmit-interval [instance-id <id>]” command restores the default value. <id> is the interface instance ID ranging between 0~255 and defaulted at 0 <time> is the retransmit interval of link state announcements between the interface and adjacent layer 3 switches, shown in seconds and ranging between 1 ~ 65535.
Default	Default retransmit interval is 5 seconds.
Mode	Interface Configuration Mode.
Usage Guide	When a layer 3 switch transmits LSA to its neighbor, it will maintain the link state announcements till confirm from the object side is received. If the confirm packet is not received within the interval, the LSA will be retransmitted. The retransmit interval must be larger than the time it takes to make a round between two layer 3 switches. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.
Example	Configure the LSA retransmit interval of interface vlan 1 to 10 seconds. <pre>Switch#config terminal Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ipv6 ospf retransmit-interval 10</pre>

ipv6 ospf transmit-delay

Command	ipv6 ospf transmit-delay <time> [instance-id <id>] no ipv6 ospf transmit-delay [instance-id <id>]
Parameter	Configure the LSA sending delay time on the interface. The “no ipv6 ospf transmit-delay [instance-id <id>]” command restores to the default. <id> is the interface instance ID ranging between 0~255 and defaulted at 0 <time> is the delay time of sending LSA on the interface, which is shown in seconds and ranged between 1 ~ 65535.
Default	The default delay time of send LSA on the interface is 1 second by default.
Mode	Interface Configuration Mode.

Usage Guide

The LSA ages by time in the layer 3 switches but not in the transmission process. So by increasing the transmit-delay before sending LSA so that it will be sent out. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example

Set the interface vlan 1 LSA sending delay to 3 seconds.

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 ospf transmit-delay 3

ipv6 router ospf

Command

[no] ipv6 router ospf {area <area-id> [instance-id <instance-id>|tag <WORD> [instance-id <instance-id>]] tag <WORD> aea <area-id> [instance-id <instance-id>]}

Enable ospf route on the interface; the “**no ipv6 router ospf {area <area-id> [instance-id <instance-id>]] tag <WORD> [instance-id <instance-id>]] tag <WORD> area <area-id> [instance-id <instance-id>]}**” command cancels this configuration.

Parameter

<area-id> is an area ID which could be shown in digits ranging between 0 ~ 4294967295, or an IPv4 address
<instance-id> is the interface instance ID ranging between 0~255 and defaulted at 0
<WORD> ospfv3 process identifier

Default

Not configured

Mode

Interface Configuration Mode.

Usage Guide

To enable this command on the interface, the area id must be configured. The instance ID and instance tag are optional. The ospfv3 process allows one routing instance for each instance ID. The route can be enabled on a interface with a instance ID. If the instance IDs are different, several OSPF process can be run on one interface. However different OSPF process should not use the same instance ID The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure 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

max-concurrent-dd

Command	max-concurrent-dd <value> no max-concurrent-dd
Parameter	Configure with this command the current dd max concurrent number in the OSPF processing. The “ no max-concurrent-dd ” command restores the default. <value> ranges between <1-65535>, the capacity of concurrent dd data packet processing.
Default	No default configuration. No dd concurrent limit.
Mode	OSPFv3 Configuration Mode.
Usage Guide	Specify the current dd max concurrent number in the OSPF processing.
Example	Set the max concurrent dd to 20. Switch#config terminal Switch(config)#router ipv6 ospf Switch(config-router)#max-concurrent-dd 20

passive-interface

Command	[no] passive-interface {<ifname> vlan <vlan-id> default}
Parameter	Configure that the hello group not sent on specific interfaces. The “ no passive-interface {<ifname> vlan <vlan-id> default } ” command cancels this function. <ifname> is the specific name of interface.
Default	Not configured
Mode	OSPFv3 Configuration Mode.
Usage Guide	-

Example	<pre>Switch#config terminal Switch(config)#router ipv6 ospf Switch(config-router)#passive-interface vlan1</pre>
redistribute	
Command	[no]redistribute {kernel connected static rip isis bgp} [metric<value>] [metric-type {1 2}][route-map<word>]
Parameter	Introduce route learnt from other routing protocols into OSPFv3. kernel Introduce from kernel route connected Introduce from direct route static Introduce from static route rip Introduce from the RIP route isis Introduce from ISIS route bgp Introduce from BGP route metric <value> is the introduced metric value, ranging between 0-16777214 metric-type {1 2} is the metric value type of the introduced external route, which can be 1 or 2, and it is 2 by default route-map <word> targets to the probe of the route map for introducing route
Default	-
Mode	OSPFv3 Configuration Mode.
Usage Guide	Learn and introduce other routing protocol into OSPFv3 area to generate AS-external_LSAs.
Example	<pre>Switch#config terminal Switch(config)#router ipv6 ospf Switch(config-router)#redistribute bgp metric 12 metric-type 1</pre>

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>] To redistribute routing information form process-tag to this command. The no form of command cancels the redistribution of process-tag routing to this process. When input the optional parameters of metric, metric type and routemap, then restores default

configuration.

Parameter

process-tag is the process ID of IPv6 OSPF process, NULL by default.
metric <value> is the metric for redistributed routing, range between 0 to 16777214.
metric-type {1|2} is the metric type for redistributed routing, only can be 1 or 2, and 2 by default.
route-map <word> is the pointer to the introduced routing map.

Default

Not redistributed any OSPFv3 routing by default.

Mode

Router IPv6 OSPF Configuration Mode.

Usage Guide

When process-id is not input, that means OSPFv3 routing will be redistributed by default (Process-tag is NULL). The no form of command input the optional parameters of metric, metric-type and routemap, then restores default configuration. When not input any optional parameters that mean to delete the router of redistributed process.

Example

```
Switch(config)#router ipv6 ospf
Switch(config-router)#redistribute ospf
```

router-id

Command

router-id<router-id>
no router-id

Parameter

Configure router ID for ospfv3 process. The “**no router-id**” restores ID to 0.0.0.0.
<router-id> is the router ID shown in IPv4 format.

Default

0.0.0.0 by default.

Mode

OSPFv3 Configuration Mode.

Usage Guide

If the router-id is 0.0.0.0, the ospfv3 process can not be normally enabled. It is required to configure a router-id for ospfv3.

Example

```
Switch(config)#router ipv6 ospf
Switch(config-router)#router-id 1.1.1.1
```

router ipv6 ospf

Command

[no] router ipv6 ospf [<WORD>]

This command initializes the ospfv3 routing process and enters ospfv3 mode for configuring the ospfv3 routing process. The “**no router ipv6 ospf [<WORD>]**” command stops relevant process.

Parameter	<WORD> ospfv3 is the process mark which could be random strings made up of characters and digits
Default	-
Mode	Global Mode
Usage Guide	To let the ospfv3 routing process work properly, this command must be configured and ospfv3 must at least be enabled on one interface. When the tag configured by the ipv6 router ospf area command under interface mode matches with the tag of ospf process, the ospfv3 process is enabled on this interface.
Example	Switch#config terminal Switch(config)#router ipv6 ospf IPI

show ipv6 ospf

Command	show ipv6 ospf [<WORD>]
Parameter	Display OSPF global and area messages. <WORD> is the process tag which is a character string.
Default	Not displayed.
Mode	All modes
Usage Guide	-
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 Unknown 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 Unknown LSA 0

show ipv6 ospf database

Command	<pre>show ipv6 ospf [<WORD>] 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>]] show ipv6 ospf [<WORD>] database [area <value> <ip-address>] [adv-router <ip- address> <self-originated>] [detail] [vrf <vrf name> <all> <default>]</pre>																																																												
Parameter	Display the OSPF link state data base message. <WORD>is the process tag which is a character string. <advertiser_router>is the ID of Advertising router, shown in IPv4 address format area <value> <0-4294967295> OspfV3 area ID as a decimal value adv-router <ip-address> Advertising Router (as an IP address) <self-originated> Self-originated link states Detail Database information in detail <vrf name> VRF name <all> Display information for all VRFs <default> Default VRF																																																												
Default	Not displayed																																																												
Mode	All modes																																																												
Usage Guide	According to the output messages of this command, we can view the OSPF link state database messages.																																																												
Example	Use show ipv6 ospf database command will be able to show LSA messages of the OSPF routing protocol For Example, the displayed messages are: OSPFv3 Router with ID (192.168.2.2) (Process *null*) Link-LSA (Interface Vlan1) <table><tr><td>Link State ID</td><td>ADV Router</td><td>Age</td><td>Seq#</td><td>CkSum</td><td>Prefix</td></tr><tr><td>0.0.7.211</td><td>192.168.2.2</td><td>1409</td><td>0x80000001</td><td>0x6dda</td><td>1</td></tr><tr><td>0.0.7.212</td><td>192.168.2.3</td><td>1357</td><td>0x80000001</td><td>0x248e</td><td>1</td></tr></table> Link-LSA (Interface Vlan2) <table><tr><td>Link State ID</td><td>ADV Router</td><td>Age</td><td>Seq#</td><td>CkSum</td><td>Prefix</td></tr><tr><td>0.0.7.211</td><td>192.168.2.1</td><td>1450</td><td>0x80000001</td><td>0xa565</td><td>1</td></tr><tr><td>0.0.7.212</td><td>192.168.2.2</td><td>1399</td><td>0x80000001</td><td>0x4305</td><td>1</td></tr></table> Router-LSA (Area 0.0.0.0) <table><tr><td>Link State ID</td><td>ADV Router</td><td>Age</td><td>Seq#</td><td>CkSum</td><td>Link</td></tr><tr><td>0.0.0.0</td><td>192.168.2.1</td><td>1390</td><td>0x80000006</td><td>0x9fe2</td><td>1</td></tr><tr><td>0.0.0.0</td><td>192.168.2.2</td><td>1354</td><td>0x80000007</td><td>0x4af5</td><td>2</td></tr><tr><td>0.0.0.0</td><td>192.168.2.3</td><td>1308</td><td>0x80000004</td><td>0xbbc4</td><td>1</td></tr></table> Network-LSA (Area 0.0.0.0)	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 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	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
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 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																																																								
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																																																								

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

Displayed information's	Explanations
Link-LSA (Interface Vlan1)	Link LSA messages of interface Vlan1
Router-LSA (Area 0.0.0.0)	Router LSA messages in Area 0
Network-LSA (Area 0.0.0.0)	Network LSA in Area 0
Intra-Area-Prefix-LSA (Area 0.0.0.0)	Intra-domain Prefix LSA in Area 0

show ipv6 ospf interface

Command `show ipv6 ospf interface <ifname>|vlan <vlan-id>`

Display the OSPF interface messages.

Parameter `< ifname >` is the name of the interface.

Default Not displayed

Mode All modes

Usage Guide -

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

```

Displayed information	Explanations
Vlan1 is up, line protocol is up	Let the interface up both logically and physically
IPv6 Prefixes fe80::203:fff:fe01:257c/64 (Link-Local Address) 2001:1:1::1/64	IPv6 address of the interface and the length of the prefix
OSPFv3 Process (*null*) Area 0.0.0.1 Instance ID 0	Ospf3 process the interface belongs Area the interface belongs Instance ID is 0
Router ID 192.168.2.2, Network Type BROADCAST, Cost: 10	Process ID; Router ID; Network Type; Cost
Transmit Delay is 1 sec, State DR, Priority 1	LAS transmission delay on the interface; state; electing the priority of the layer 3 switch.
Designated Router (ID) 192.168.2.2	Specifying layer 3 switch
Interface Address fe80::203:fff:fe01:257c	
Backup Designated Router (ID) 192.168.2.3	Back up designated layer 3 switch
Interface Address fe80::203:fff:fe01:d28	
Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due in 00:00:10	OSPF protocol timer; including hello packet, poll interval packets, router dead, router retransmission.
Neighbor Count is 1, Adjacent neighbor count is 1	Numbers of the adjacent layer 3 switch; number of the layer 3 switches established with neighbor relation

show ipv6 ospf neighbor

Command	show ipv6 ospf [<WORD>] neighbor [<neighbor_id> <ifname> detail detail]						
Parameter	Show OSPF adjacent point messages.						
	<WORD>is process tag, which is a character string						
	<neighbor_id> is the neighbor ID shown in IPv4 address format						
	detail: Show neighbor details						
	<ifname> name of the interface						
Default	Not displayed						
Mode	All modes						
Usage Guide	OSPF neighbor state can be checked by viewing the output of this command.						
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
	Displayed information			Explanations			
	Neighbor ID			Neighbor ID			
	Instance ID			Instance ID			
	Address			IP address of neighboring layer 3 switch			
	Interface			Interface the neighbor belongs			
state			Neighbor relationship state				
pri			Priority				

show ipv6 ospf route

Command	show ipv6 ospf [<WORD>] route
Parameter	Show the OSPF route table messages. <WORD> is the processes tag, which is a character string.

Default	Not displayed
Mode	All modes
Usage Guide	-
Example	<pre>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</pre>

show ipv6 ospf redistribute

Command	show ipv6 ospf [<process-tag>] redistribute
Parameter	To display the routing message redistributed from external process of OSPF. IPv6 OSPF is the tag ID, to display all routing messages redistributed from external process of IPv6 OSPF if there is no parameter.
Default	None.
Mode	Admin Mode and Configuration Mode.
Usage Guide	None.
Example	<pre>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:</pre>

ospf process def
bgp

show ipv6 ospf topology

Command	show ipv6 ospf [<WORD>] topology [area <area-id>]																
Parameter	Show messages of OSPF topology. <WORD> is the processes tag, which is a character string. <area-id> is an area ID which could be shown in digits ranging between 0 ~ 4294967295, or an IPv4 address.																
Default	Not displayed																
Mode	All modes																
Usage Guide	None.																
Example	Switch#show ipv6 ospf topology OSPFv3 Process (*null*) OSPFv3 paths to Area (0.0.0.0) routers <table><tr><th>Router ID</th><th>Bits Metric</th><th>Next-Hop</th><th>Interface</th></tr><tr><td>192.168.2.1</td><td>10</td><td>192.168.2.1</td><td>Vlan2</td></tr><tr><td>192.168.2.2</td><td>--</td><td></td><td></td></tr><tr><td>192.168.2.3</td><td>10</td><td>192.168.2.3</td><td>Vlan1</td></tr></table>	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
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														

show ipv6 ospf virtual-links

Command	show ipv6 ospf [<WORD>] virtual-links
Parameter	Show OSPF virtual link messages. <WORD> is the processes tag, which is a character string.
Default	Not displayed
Mode	All modes

Usage Guide	None.
Example	<pre>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</pre>

show ipv6 route process-detail

Command	show ipv6 route [database] process-detail
Parameter	Display the IP routing table with specific process ID or Tag. The parameter of database means displaying all the routers, no parameter means only displaying effective routers.
Default	-
Mode	Admin mode
Usage Guide	None.
Example	<pre>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</pre>

timers spf

Command	timers spf <spf-delay> <spf-holdtime> no timers spf
	Adjust route calculation timer value. The “no timers spf” restores the relevant value to

Parameter	default.
	<spf-delay> 5 seconds by default <spf-holdtime> 10 seconds by default
Default	-
Mode	OSPFv3 Configuration Mode.
Usage Guide	In this command the delay time between receiving topology change and SPF calculation, and further configured the hold time between two discontinuous SPF calculations.
Example	Switch#config terminal Switch(config)#router ipv6 ospf Switch(config-router)#timers spf 5 10

6 Commands for MBGP4+

debug ipv6 bgp redistribute message send

Command	debug ipv6 bgp redistribute message send no debug ipv6 bgp redistribute message send
	To enable debugging switch of sending messages for redistribution of routing information from external process such as OSPFv3 and others to MBGP4+. The no command will disable the debugging switch.
Parameter	-
Default	Closed.
Mode	Admin mode
Usage Guide	-
Example	Switch#debug ipv6 bgp redistribute message send

debug ipv6 bgp redistribute route receive

Command	debug ipv6 bgp redistribute route receive no debug ipv6 bgp redistribute route receive

To enable debugging switch of received messages from NSM for MBGP4+. The no form of this command will disable debugging switch of received messages from NSM for MBGP4+.

Parameter	-
Default	Closed.
Mode	Admin mode
Usage Guide	-
Example	Switch#debug ipv6 bgp redistribute route receive Switch#no debug ipv6 bgp redistribute route receive

redistribute ospf (MBGP4+)

Command	redistribute ospf [<process-tag>] [route-map<word>] no redistribute ospf [<process-tag>]
Parameter	To redistribute routing information form OSPFv3 to MBGP4+. The no form of this command will remove the configuration. process-tag is the process character string of the OSPFv3, the length is less than 15. If no process id is specified, the default process will be used. route-map <word> is the pointer to the introduced routing map.
Default	Not redistributed by default.
Mode	BGP IPv6 Configuration Mode.
Usage Guide	-
Example	To redistribute routing information from OSPFv3 process with the tag as ABC to MBGP4+ (as number as 1). Switch(config)#router bgp 1 Switch(config-router)#address-family ipv6 unicast Switch (config-router-af)#redistribute ospf abc

show ipv6 bgp redistribute

Command	show ipv6 bgp redistribute

Show the configuration information of redistribution other out routing to MBGP4+.

Parameter	-
Default	Not shown by default.
Mode	Admin mode
Usage Guide	-
Example	Switch#show ipv6 bgp redistribute

7 Commands for ISIS

router isis

Command	router isis <WORD> no router isis < WORD>	
Parameter	Configure this command to enable the ISIS process. < WORD > Indicates the area tag for the ISIS process to be created. The range of values should be specified, which is a string with a length not exceeding 60 characters.	
Default	The ISIS process is not enabled by default.	
Mode	Config mode	
Usage Guide	-	
Example	Switch#config terminal Switch(config)#router isis test Switch(config-router)#	

net

Command	net NET no net NET

Parameter	Configure this command to set the network entity label for the ISIS process.
	NET specifies the tag for the network entity to be created, in the format of XX.XXXX. XXXX.XX, where X represents a digit.
Default	Default: Not configured
Mode	ISIS router mode
Usage Guide	-
Example	Switch#config terminal Switch(config)#router isis test Switch(config-router)#net 10.0000.0000.0000.01

is-type

Command	is-type [level-1 level-1-2 level-2-only] no is-type
Parameter	Configure this command to specify the type of the ISIS process that will be issued.
	level-1 Only as a site router
	level-1-2 Both as a site router and as a regional router
	level-2-only Only as a regional router
Default	The default setting is level-1-2. If there is an existing ISIS process in the level-1-2 mode, the default will be level-1 (there can only be one ISIS process in the level-1-2 mode).
Mode	ISIS router mode
Usage Guide	-
Example	Switch#config terminal Switch(config)#router isis test Switch(config-router)#net 10.0000.0000.0000.01 Switch(config-router)#is-type level-2-only

area-password

Command	area-password WORD no area-password
Parameter	Issue this command to configure the authentication key for the ISIS process area.
	WORD The authentication key for the ISIS area, which is a string with a length not exceeding 254 characters.

Default	Default: Not configured
Mode	ISIS router mode
Usage Guide	The regional authentication key for level-1 IS-IS neighbors affects the authentication process. If the keys of the two devices are different, routing exchange cannot be performed.
Example	Switch#config terminal Switch(config)#router isis test Switch(config-router)#area-password test

domain-password

Command	domain -password WORD no domain -password
Issue this command to configure the authentication key for the routing domain of the ISIS process.	
Parameter	WORD The authentication key for the ISIS routing domain is a string with a length not exceeding 254 characters.
Default	Default: Not configured
Mode	ISIS router mode
Usage Guide	The authentication key of the routing domain affects the authentication of the level-2 IS-IS neighbors. If the keys of the two devices are different, routing exchange cannot be performed.
Example	Switch#config terminal Switch(config)#router isis test Switch(config-router)#domain-password test

ignore-lsp-error

Command	ignore-lsp-errors no ignore-lsp-errors
Issue this command to configure the ISIS process to ignore LSPs with error checks.	
Parameter	

Default	Default: Not configured
Mode	ISIS router mode
Usage Guide	-
Example	Switch#config terminal Switch(config)#router isis test Switch(config-router)# ignore-lsp-errors

lsp-gen-interval

Command	lsp-gen-interval [level-1 level-2] <1-120> no lsp-gen-interval
	Issue this command to configure the ISIS process and re-generate the minimum interval between identical LSPs.
Parameter	<1-120> The minimum interval time, measured in seconds
Default	The default setting is 30 seconds.
Mode	ISIS router mode
Usage Guide	-
Example	Switch#config terminal Switch(config)#router isis test Switch(config-router)# lsp-gen-interval 15

lsp-refresh-interval

Command	lsp-refresh-interval <1-65535> no lsp- refresh -interval
	Issue this command to configure the ISIS process and re-generate the minimum interval between identical LSPs.
Parameter	<1-65535> The minimum interval time, measured in seconds
Default	The default setting is 900 seconds
Mode	ISIS router mode

Usage Guide	-
Example	<pre>Switch#config terminal Switch(config)#router isis test Switch(config-router)# lsp-refresh-interval 500</pre>

max-area-addresses

Command	max-area-addresses <3-254> no max-area-addresses
	This command is used to configure the number of manually configurable area addresses allowed for the ISIS process.
Parameter	<3-254> The maximum number of manually configured area addresses
Default	Default is 3
Mode	ISIS router mode
Usage Guide	-
Example	<pre>Switch#config terminal Switch(config)#router isis test Switch(config-router)# max-area-addresses 5</pre>

max-lsp-lifetime

Command	max-lsp-lifetime <1-65535> no max-lsp-lifetime
	Issue this command to configure the maximum LSP lifetime for the ISIS process.
Parameter	<1-65535> LSP maximum survival time
Default	The default duration is 1200 seconds.
Mode	ISIS router mode
Usage Guide	-
Example	<pre>Switch#config terminal Switch(config)#router isis test Switch(config-router)# max-lsp-lifetime 900</pre>

spf-interval

Command	spf-interval [level-1 level-2] <1-120> no spf-interval
	Issue this command to configure the interval for route calculation between ISIS processes.
Parameter	<1-120> The intervals between routing calculations
Default	The default duration is 10 seconds.
Mode	ISIS router mode
Usage Guide	-
Example	Switch#config terminal Switch(config)#router isis test Switch(config-router)# spf-interval level-1 60

dynamic-hostname

Command	dynamic-hostname [area-tag] no dynamic-hostname
	Issue this command to activate the dynamic host names for the ISIS process.
Parameter	area-tag When the command carries the "area-tag", use the "area-tag" of the ISIS route as the hostname.
Default	Default setting is not enabled.
Mode	ISIS router mode
Usage Guide	
Example	Switch#config terminal Switch(config)#router isis test Switch(config-router)# dynamic-hostname

adjacency-check

Command	adjacency-check no adjacency-check
	Issue this command to configure the ISIS process to enable the ISIS neighbor protocol support.
Parameter	
Default	Default setting is not enabled.
Mode	ISIS router mode
Usage Guide	-
Example	Switch#config terminal Switch(config)#router isis test Switch(config-router)# adjacency-check

summary-address

Command	summary-address A.B.C.D/M [level-1 level-1-2 level-2] no summary-address A.B.C.D/M
	Issue this command to configure the ISIS process for IP address summarization.
Parameter	A.B.C.D/M IPv4 address, with M representing the number of mask bits level-1 Summarize in the level-1 area level-1-2 Summarize at the regional and sub-regional levels level-2 Summarized into the level-2 subdomain
Default	Default setting is not enabled.
Mode	ISIS router mode
Usage Guide	-
Example	Switch#config terminal Switch(config)#router isis test Switch(config-router)# summary-address 192.168.3.111/24

set-overload-bit suppress

Command	set-overload-bit [suppress [external interlevel] on-startup <5-86400>] no set-overload-bit

Issue this command to configure the overload bit for the ISIS process.	
Parameter	suppress If the overload bit is set, suppress the following types of IP prefixes. external Do not notify the IP prefixes learned from other protocols. interlevel Do not acquire the IP prefix by learning from another level of ISIS. on-startup Only temporarily set the overload position after a reboot. <5-86400> Notify the system that it is in an overloaded state after rebooting.
Default	Default setting is not enabled.
Mode	ISIS router mode
Usage Guide	-
Example	Switch#config terminal Switch(config)#router isis test Switch(config-router)# set-overload-bit external

metric-style

Command	metric-style [narrow wide transition] [level-1 level-1-2 level-2] no metric-style [narrow wide transition] [level-1 level-1-2 level-2]
Issue this command to configure the ISIS measurement style.	
Parameter	narrow Using the old version of TLV, with narrow measurement wide Using the new version of TLV, with width measurement included transition Send and receive both styles of TLV simultaneously during the transition period. level-1 Limited to level-1 level-1-2 Limited to level-1-2 level-2 Limited to level-2
Default	Default setting is not enabled.
Mode	ISIS router mode
Usage Guide	-
Example	Switch#config terminal Switch(config)#router isis test Switch(config-router)# metric-style wide transition

mpls traffic-eng

Command	mpls traffic-eng [level-1 level-2 router-id A.B.C.D] no mpls traffic-eng [level-1 level-2 router-id A.B.C.D]
	Issue this command to configure the ISIS process and MPLS routing parameters protocol.
Parameter	level-1 Only on the ISIS level-1 is MPLS TE permitted level-2 Only on the ISIS level-2 is MPLS TE permitted. router-id System's stable traffic, IP address A.B.C.D ISIS router ID in IP address format
Default	Default setting is not enabled.
Mode	ISIS router mode
Usage Guide	-
Example	Switch#config terminal Switch(config)#router isis test Switch(config-router)# mpls traffic-eng level-1

capability cspf

Command	capability cspf no capability cspf
	Issue this command to enable the restricted shortest path first (CSPF) feature for the ISIS process.
Parameter	
Default	Default setting is not enabled.
Mode	ISIS router mode
Usage Guide	-
Example	Switch#config terminal Switch(config)#router isis test Switch(config-router)# capability cspf

debug isis all

Command	debug isis all no debug isis all
	Turn on the debugging switch that displays various event information of ISIS; the "no" operation of this command is to turn off this debugging switch.
Parameter	-
Default	The debugging switch has been turned off.
Mode	Admin mode
Usage Guide	-
Example	Switch#debug isis all

debug isis ifsm

Command	debug isis ifsm no debug isis ifsm
	Enable the OSPF interface status machine debugging switch; the no operation of this command is to disable this debugging switch.
Parameter	-
Default	The debugging switch has been turned off.
Mode	Admin mode
Usage Guide	-
Example	Switch#debug isis ifsm

debug isis nfsm

Command	debug isis nfsm no debug isis nfsm
	Turn on the debugging switch that displays the status of ISIS neighbors; the "no" operation of this command is to turn off this debugging switch.
Parameter	-
Default	The debugging switch has been turned off.

Mode	Admin mode
Usage Guide	-
Example	Switch#debug isis nfsm

debug isis pdu

Command	debug isis pdu no debug isis pdu
	Turn on the debugging switch for displaying ISIS protocol data units; the "no" operation of this command is to disable this debugging switch.
Parameter	-
Default	The debugging switch has been turned off.
Mode	Admin mode
Usage Guide	-
Example	Switch# debug isis pdu

debug isis lsp

Command	debug isis lsp no debug isis lsp
	Turn on the ISIS link state data unit debugging switch; the "no" operation of this command is to turn off this debugging switch.
Parameter	-
Default	The debugging switch has been turned off.
Mode	Admin mode
Usage Guide	-
Example	Switch# debug isis lsp

debug isis spf

Command	debug isis spf no debug isis spf
	Turn on the ISIS routing calculation debugging switch; the "no" operation of this command is to turn off this debugging switch.
Parameter	-
Default	The debugging switch has been turned off.
Mode	Admin mode
Usage Guide	-
Example	Switch# debug isis spf

debug isis events

Command	debug isis events no debug isis events
	Turn on the debug switch for displaying ISIS events; the "no" operation of this command is to turn off this debug switch.
Parameter	-
Default	The debugging switch has been turned off.
Mode	Admin mode
Usage Guide	-
Example	Switch# debug isis events

debug isis nsm

Command	debug isis nsm no debug isis nsm

Turn on the debug switch that displays ISIS nsm information; the no operation of this command will disable this debug switch.

Parameter	-
Default	The debugging switch has been turned off.
Mode	Admin mode
Usage Guide	-
Example	Switch# debug isis nsm

show debugging isis

Command	show debugging isis
Parameter	Display the status of the debug switch for the ISIS protocol. -
Default	-
Mode	All modes
Usage Guide	-
Example	Switch#show debugging isis IS-IS debugging status: IS-IS Interface FSM debugging is on IS-IS Neighbor FSM debugging is on IS-IS events debugging is on IS-IS PDU debugging is on IS-IS lsp debugging is on IS-IS spf debugging is on IS-IS NSM debugging is on

debug ospf redistribute route receive

Command	debug ospf redistribute route receive no debug ospf redistribute route receive
Parameter	Enable/disable the debugging switch for receiving routing information sent by NSM when opening/closing the OSPF process. -

Default	The debugging switch has been turned off.
Mode	Admin mode
Usage Guide	-
Example	Enable the debugging switch for receiving routing information sent by NSM in the OSPF process. Switch# debug ospf redistribute route receive

redistribute

Command	redistribute {kernel connected static rip ospf <1-65535> bgp} [metric <value>] [metric-type {external internal}] [route-map <word>] [level-1 level-1-2 level-2] no redistribute {connected rip ospf <1-65535> bgp static kernel}																					
	Use this command to bind the specified routing policy for redistribution. The "no" operation of this command cancels this. Configuration																					
Parameter	<table><tr><td>kernel</td><td>Introduced from the core routing;</td></tr><tr><td>connected</td><td>Introduced from the direct connection routing;</td></tr><tr><td>static</td><td>Introduce from static routes;</td></tr><tr><td>rip</td><td>Introduced from the RIP routing;</td></tr><tr><td>ospf <1-65535></td><td>Introduced from OSPF routes;</td></tr><tr><td>bgp</td><td>Introduced from BGP routes;</td></tr><tr><td>metric <value></td><td>It is the metric assigned to the introduced route, with a value range of 0 to 4261412864;</td></tr><tr><td>metric-type {external internal}</td><td>It is the metric type of the introduced external route, and the default value is "external".</td></tr><tr><td>route-map <word></td><td>Pointer to the routing map used to introduce the routing;</td></tr><tr><td>level-1 level-1-2 level-2</td><td>Specify the ISIS area where the route is introduced.</td></tr></table>		kernel	Introduced from the core routing;	connected	Introduced from the direct connection routing;	static	Introduce from static routes;	rip	Introduced from the RIP routing;	ospf <1-65535>	Introduced from OSPF routes;	bgp	Introduced from BGP routes;	metric <value>	It is the metric assigned to the introduced route, with a value range of 0 to 4261412864;	metric-type {external internal}	It is the metric type of the introduced external route, and the default value is "external".	route-map <word>	Pointer to the routing map used to introduce the routing;	level-1 level-1-2 level-2	Specify the ISIS area where the route is introduced.
kernel	Introduced from the core routing;																					
connected	Introduced from the direct connection routing;																					
static	Introduce from static routes;																					
rip	Introduced from the RIP routing;																					
ospf <1-65535>	Introduced from OSPF routes;																					
bgp	Introduced from BGP routes;																					
metric <value>	It is the metric assigned to the introduced route, with a value range of 0 to 4261412864;																					
metric-type {external internal}	It is the metric type of the introduced external route, and the default value is "external".																					
route-map <word>	Pointer to the routing map used to introduce the routing;																					
level-1 level-1-2 level-2	Specify the ISIS area where the route is introduced.																					
Default	-																					
Mode	config-router mode																					
Usage Guide	-																					
Example	Switch#config terminal Switch(config)#router isis Switch(config-router)#redistribute connected metric 12 route-map x																					

redistribute isis

Command	redistribute isis {level-1 level-2} into {level-2 level-1} [route-map <word>] no redistribute isis {level-1 level-2} into {level-2 level-1} [route-map<word> distribute-list <WORD>]	
	Use this command to bind the specified routing policy for routing leakage. The "no" operation of this command cancels this configuration.	
Parameter	level-1 level-2	The area designated for routing;
	level-2 level-1	The area to which the designated route is leaked;
	route-map <word>	Pointer to the routing map used for routing leaks;
	<WORD>	Access-list name
Default	-	
Mode	config-router mode	
Usage Guide	Leaks routes from one IS-IS level to another. The command redistributes IS-IS routes from level-1 into level-2, or from level-2 into level-1, optionally applying a route-map for filtering. The no form removes the redistribution configuration.	
Example	Switch#config terminal Switch(config)#router isis Switch(config-router)#redistribute isis level-1 into level-2 route-map x	

default-information

Command	default-information originate [route-map <word>] no default-information originate [route-map <word>]	
	Use this command to bind the specified routing policy for routing leakage. The "no" operation of this command cancels this configuration.	
Parameter	route-map <word>	Pointer to the routing map used to declare the default route;
Default	-	
Mode	config-router mode	
Usage Guide	-	
Example	Switch#config terminal Switch(config)#router isis Switch(config-router)# default-information originate route-map x	

is-name

Command	is-name WORD no is-name
	Use this command to specify the dynamic ISIS name. The "no" operation of this command cancels this configuration.
Parameter	WORD Specify the name, with a length less than 64.
Default	-
Mode	ISIS router mode
Usage Guide	-
Example	Switch#config terminal Switch(config)#router isis Switch(config-router)# is-name test

ip router isis

Command	ip router isis [WORD] no ip router isis [WORD]
	Use this command to add the interface to the corresponding ISIS process. The "no" operation of this command cancels this configuration.
Parameter	WORD Specify the ISIS process Routing process tag, which should be a string with a length not exceeding 60 characters.
Default	-
Mode	Interface Configuration Mode.
Usage Guide	-
Example	Switch#config terminal Switch(config)#interface vlan 21 Switch(config-if-vlan21)ip router isis test

isis circuit-type

Command	isis circuit-type [level-1 level-1-2 level-2-only] no isis circuit-type

Use this command to configure the line type of the interface.
The "no" operation of this command cancels this configuration.

Parameter	level-1	Level-1 only adjacencies are formed
	level-1-2	Level-1-2 adjacencies are formed
	level-2-only	Level-2 only adjacencies are formed
Default	-	
Mode	Interface Configuration Mode.	
Usage Guide	-	
Example	Switch#config terminal Switch(config)#interface vlan 21 Switch(config-if-vlan21) isis circuit-type level-1	

isis csnp-interval

Command	isis csnp-interval <0-65535> [level-1 level-2] no isis circuit-interval [level-1 level-2]	
	Use this command to configure the CSNP interval for the interface. The "no" operation of this command cancels this configuration.	
Parameter	<0-65535>	Message interval, measured in seconds;
	level-1	Specify the interval time for level-1 CSNP;
	level-2	Specify the interval time for level-2 CSNP.
Default	The default duration is 10 seconds.	
Mode	Interface Configuration Mode	
Usage Guide	-	
Example	Switch#config terminal Switch(config)#interface vlan 21 Switch(config-if-vlan21) isis csnp-interval 50	

isis hello-interval

Command	isis hello-interval <0-65535> [level-1 level-2] no isis hello-interval [level-1 level-2]	
	Use this command to configure the HELLO interval of the interface.	

Parameter	The "no" operation of this command cancels this configuration.	
	<1-65535>	Message interval, measured in seconds;
	level-1	Specify hello-interval for level-1 IIHs
	level-2	Specify hello-interval for level-2 IIHs
Default	The default duration is 10 seconds.	
Mode	Interface Configuration Mode	
Usage Guide	-	
Example	Switch#config terminal Switch(config)#interface vlan 21 Switch(config-if-vlan21) isis hello-interval 5	

isis hello-interval minimal

Command	isis hello-interval minimal [level-1 level-2] no isis hello-interval [level-1 level-2]	
Parameter	Use this command to configure the HELLO interval of the interface. The "no" operation of this command cancels this configuration.	
	minimal	Keep the duration for 1 second, and the interval time depends on the multiplier.
	level-1	Specify the Hello interval time for level-1 IIH.
	level-2	Specify the Hello interval time for level-2 IIH.
Default	The default duration is 10 seconds.	
Mode	Interface Configuration Mode	
Usage Guide	-	
Example	Switch#config terminal Switch(config)#interface vlan 21 Switch(config-if-vlan21) isis hello-interval minimal	

isis hello-multiplier

Command	isis hello-multiplier <3-1000> [level-1 level-2] no isis hello-multiplier [level-1 level-2]	
	Use this command to set the multiplier for the retention time of the "hello" message.	

Parameter	The "no" operation of this command cancels this configuration.	
	<3-1000>	Set the multiplier for the Hello retention time;
	level-1	Specify hello multiplier for level-1 IIHs
	level-2	Specify hello multiplier for level-2 IIHs
Default	The default value is 3.	
Mode	Interface Configuration Mode	
Usage Guide	-	
Example	Switch#config terminal Switch(config)#interface vlan 21 Switch(config-if-vlan21) isis hello- multiplier 10	

isis hello padding

Command	isis hello padding no isis hello padding	
	Use this command to add padding to the ISIS hello packets. The "no" operation of this command cancels this configuration.	
Parameter		
Default	It is not enabled by default.	
Mode	Interface Configuration Mode	
Usage Guide	-	
Example	Switch#config terminal Switch(config)#interface vlan 21 Switch(config-if-vlan21) isis hello padding	

isis lsp-interval

Command	isis lsp-interval <1-4294967295> no isis lsp-interval	
	Use this command to set the LSP transmission interval. The "no" operation of this command will cancel this configuration.	
Parameter	<1-4294967295>	Transmission interval, measured in milliseconds;
Default	The default value is 33 milliseconds.	

Mode	Interface Configuration Mode
Usage Guide	-
Example	Switch#config terminal Switch(config)#interface vlan 21 Switch(config-if-vlan21) lsp-interval 100

isis metric

Command	isis metric <1-63> [level-1 level-2] no isis metric [level-1 level-2]
	Use this command to set the default metric value for the interface. The “no” operation of this command will cancel this configuration.
Parameter	<1-63> Default measurement value; level-1 Apply metric to level-1 links level-2 Apply metric to level-2 links
Default	The default value is 10.
Mode	Interface Configuration Mode
Usage Guide	-
Example	Switch#config terminal Switch(config)#interface vlan 21 Switch(config-if-vlan21) isis metric 15

isis wide-metric

Command	isis wide-metric <1-16777214> [level-1 level-2] no isis wide-metric [level-1 level-2]
	Use this command to set the width measurement value of the interface. The “no” operation of this command cancels this configuration.
Parameter	<1-16777214> Wide metric level-1 Apply metric to level-1 links level-2 Apply metric to level-2 links
Default	The default value is 10.
Mode	Interface Configuration Mode

Usage Guide	-
Example	<pre>Switch#config terminal Switch(config)#interface vlan 21 Switch(config-if-vlan21) isis wide-metric 15</pre>
isis password	
Command	isis password WORD [level-1 level-2] no isis password [level-1 level-2]
	Use this command to set the width measurement value of the interface. The "no" operation of this command cancels this configuration.
Parameter	WORD Set the authentication password for the interface, with a length not exceeding 254. level-1 Specify password for level-1 PDUs level-2 Specify password for level-2 PDUs
Default	Default: Not configured
Mode	Interface Configuration Mode
Usage Guide	-
Example	<pre>Switch#config terminal Switch(config)#interface vlan 21 Switch(config-if-vlan21) isis password test</pre>

isis priority

Command	isis priority <0-127> [level-1 level-2] no isis priority [level-1 level-2]
	Use this command to set the priority for the election of the specified router. The "no" operation of this command will cancel this configuration.
Parameter	<0-127> Priority value; level-1 Specify priority for level-1 routing level-2 Specify priority for level-2 routing
Default	The default value is 64.
Mode	Interface Configuration Mode
Usage Guide	-

Example	Switch#config terminal Switch(config)#interface vlan 21 Switch(config-if-vlan21) isis priority 40

isis retransmit-interval

Command	isis retransmit-interval <0-65535> no isis retransmit-interval
	Use this command to set the retransmission interval for each LSP. The "no" operation of this command will cancel this configuration.
Parameter	<0-65535> Interval between retransmissions of the same LSP (seconds)
Default	The default value is 5.
Mode	Interface Configuration Mode
Usage Guide	-
Example	Switch#config terminal Switch(config)#interface vlan 21 Switch(config-if-vlan21) isis retransmit-interval 10

isis mesh-group

Command	isis mesh-group <1-4294967295> no isis mesh-group
	Use this command to set up the ISIS grid group. The "no" operation of this command will cancel this configuration.
Parameter	<0-4294967295> Mesh group number
Default	Default configuration is not set.
Mode	Interface Configuration Mode
Usage Guide	Assigns the interface to an IS-IS mesh group to reduce LSP flooding in fully meshed networks. The no form removes the interface from the mesh group.
Example	Switch#config terminal Switch(config)#interface vlan 21 Switch(config-if-vlan21) isis mesh-group 5

isis mesh-group blocked

Command	isis mesh-group blocked no isis mesh-group
	Use this command to set up the ISIS grid group. The "no" operation of this command will cancel this configuration.
Parameter	blocked Block LSPs on this interface
Default	Default configuration is not set.
Mode	Interface Configuration Mode
Usage Guide	-
Example	Switch#config terminal Switch(config)#interface vlan 21 Switch(config-if-vlan21) isis mesh-group blocked

restart-timer

Command	restart-timer <5-65535> [level-1 level-1-2 level-2] no restart-timer
	Use this command to set the ISIS restart timer. The "no" operation of this command will cancel this configuration.
Parameter	<5-65535> The unit is seconds. level-1 Only level-1; level-1-2 level-1-2; level-2 Only level-2;
Default	The default duration is 60 seconds.
Mode	ISIS router mode
Usage Guide	Sets the IS-IS restart timer duration in seconds. The level parameter restricts the configuration to a specific IS-IS level. The no form restores the default value of 60 seconds.
Example	Switch#config terminal Switch(config)#router isis Switch(config-router) restart-timer 10

show isis database

Command	show isis database [detail verbose] <LSP-ID> [level-1 level-2]	
	Used to display the routing information of ISIS.	
Parameter	detail	Detailed link state database information
	verbose	Verbose database information
	<LSP-ID>	LSPID in the form of xxxx.xxxx.xxxx.xx-xx
	level-1	IS-IS Level-1 routing link state database
	level-2	IS-IS Level-2 routing link state database
Default	-	
Mode	All modes	
Usage Guide	ISIS routing information can be displayed based on different parameters (such as LSP-ID or ISIS LEVEL address).	
Example	Switch# show isis database detail	

show isis topology

Command	show isis topology [level-1 level-2]	
	Used to display the information of the ISIS path to the intermediate system.	
Parameter	level-1	Path to all level-1 routers in the area
	level-2	Path to all level-2 routers in the domain
Default	-	
Mode	All modes	
Usage Guide	Displays IS-IS topology information, showing the path to intermediate systems. The level-1 option displays paths to level-1 routers in the area, and level-2 displays paths to level-2 routers in the domain.	
Example	Switch# show isis topology	

show ip isis route

Command	show ip isis [<area-tag>] route

Used to display the ISIS routing table of the IPv4 protocol.

Parameter	<area-tag> Routing area identifier of the ISIS process																																																															
Default	-																																																															
Mode	All modes																																																															
Usage Guide	-																																																															
Example	Switch# show ip isis route Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, D - discard, e - external metric Area 1: <table><tr><td></td><td>Destination</td><td>Metric</td><td>Next-Hop</td><td>Interface</td></tr><tr><td>L2</td><td>1.0.0.0/16</td><td>30</td><td>111.1.1.1</td><td>Vlan111</td></tr><tr><td>L2</td><td>1.1.0.0/16</td><td>30</td><td>111.1.1.1</td><td>Vlan111</td></tr><tr><td>L2</td><td>1.2.0.0/16</td><td>30</td><td>111.1.1.1</td><td>Vlan111</td></tr><tr><td>L2</td><td>1.3.0.0/16</td><td>30</td><td>111.1.1.1</td><td>Vlan111</td></tr><tr><td>L2</td><td>1.4.0.0/16</td><td>30</td><td>111.1.1.1</td><td>Vlan111</td></tr><tr><td>L2</td><td>1.5.0.0/16</td><td>30</td><td>111.1.1.1</td><td>Vlan111</td></tr><tr><td>L2</td><td>1.6.0.0/16</td><td>30</td><td>111.1.1.1</td><td>Vlan111</td></tr><tr><td>L2</td><td>1.7.0.0/16</td><td>30</td><td>111.1.1.1</td><td>Vlan111</td></tr><tr><td>L2</td><td>1.8.0.0/16</td><td>30</td><td>111.1.1.1</td><td>Vlan111</td></tr><tr><td>L2</td><td>1.9.0.0/16</td><td>30</td><td>111.1.1.1</td><td>Vlan111</td></tr><tr><td>L2</td><td>1.10.0.0/16</td><td>30</td><td>111.1.1.1</td><td>Vlan111</td></tr></table>					Destination	Metric	Next-Hop	Interface	L2	1.0.0.0/16	30	111.1.1.1	Vlan111	L2	1.1.0.0/16	30	111.1.1.1	Vlan111	L2	1.2.0.0/16	30	111.1.1.1	Vlan111	L2	1.3.0.0/16	30	111.1.1.1	Vlan111	L2	1.4.0.0/16	30	111.1.1.1	Vlan111	L2	1.5.0.0/16	30	111.1.1.1	Vlan111	L2	1.6.0.0/16	30	111.1.1.1	Vlan111	L2	1.7.0.0/16	30	111.1.1.1	Vlan111	L2	1.8.0.0/16	30	111.1.1.1	Vlan111	L2	1.9.0.0/16	30	111.1.1.1	Vlan111	L2	1.10.0.0/16	30	111.1.1.1	Vlan111
	Destination	Metric	Next-Hop	Interface																																																												
L2	1.0.0.0/16	30	111.1.1.1	Vlan111																																																												
L2	1.1.0.0/16	30	111.1.1.1	Vlan111																																																												
L2	1.2.0.0/16	30	111.1.1.1	Vlan111																																																												
L2	1.3.0.0/16	30	111.1.1.1	Vlan111																																																												
L2	1.4.0.0/16	30	111.1.1.1	Vlan111																																																												
L2	1.5.0.0/16	30	111.1.1.1	Vlan111																																																												
L2	1.6.0.0/16	30	111.1.1.1	Vlan111																																																												
L2	1.7.0.0/16	30	111.1.1.1	Vlan111																																																												
L2	1.8.0.0/16	30	111.1.1.1	Vlan111																																																												
L2	1.9.0.0/16	30	111.1.1.1	Vlan111																																																												
L2	1.10.0.0/16	30	111.1.1.1	Vlan111																																																												

show clns neighbors

Command	show clns <area-tag> neighbors [vlan <1-4094> IFNAME] [detail]
	Used to display the neighbor adjacency relationship of CLNS.
Parameter	<area-tag> Routing area identifier of the ISIS process vlan <1-4094> VLAN port number IFNAME Interface Name detail Show detailed information
Default	-
Mode	All modes
Usage Guide	-
Example	Switch#show clns neighbors vlan 111

```

Area 1:
System Id      Interface  SNPA                State  Holdtime  Type Protocol
0000.0201.0102 Vlan111    0000.0201.0102     Init   27        L2    IS-IS
Switch#

```

show clns is-neighbors

Command	show clns <area-tag> is-neighbors [vlan <1-4094> IFNAME] [detail]
Parameter	Used to display the neighbor adjacency relationship of ISIS. <area-tag> Routing area identifier of the ISIS process vlan <1-4094> VLAN port number IFNAME Interface Name detail Show detailed information
Default	-
Mode	All modes
Usage Guide	-
Example	Switch#show clns is-neighbors vlan 111 <pre> Area 1: System Id Interface State Type Priority Circuit Id 0000.0201.0102 Vlan111 Init L2 0 0000.0201.0102.01 Switch# </pre>

show isis interface

Command	show isis interface [vlan <1-4094> IFNAME]
Parameter	Used to display the status and configuration of the ISIS interface. vlan <1-4094> VLAN port number IFNAME Interface Name
Default	-
Mode	All modes
Usage Guide	-

Example	<pre> Switch#show isis interface vlan 111 Vlan111 is up, line protocol is up Routing Protocol: IS-IS (1) Circuit Type: level-1-2 Local circuit ID: 0x01 Local SNPA: 84e5.d8e1.79c9 IP interface address: 111.1.1.230/24 IPv6 interface address: 2111::230/64 fe80::86e5:d8ff:fee1:79c9/64 Level-1 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0230.01 Number of active level-1 adjacencies: 0 Level-2 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0230.01 Number of active level-2 adjacencies: 0 Next IS-IS LAN Level-1 Hello in 4 seconds Next IS-IS LAN Level-2 Hello in 6 seconds </pre>

show isis counter

Command	show isis counter
Parameter	Used to display the ISIS system counter management information database.
Default	-
Mode	All modes
Usage Guide	-

Example	<pre> Switch#show isis counter Area 1: IS-IS Level-1 isisSystemCounterEntry: isisSysStatCorrLSPs: 0 isisSysStatAuthTypeFails: 0 isisSysStatAuthFails: 0 isisSysStatLSPDbaseOloads: 0 isisSysStatManAddrDropFromAreas: 0 isisSysStatAttmptToExMaxSeqNums: 0 isisSysStatSeqNumSkips: 0 isisSysStatOwnLSPPurges: 0 isisSysStatIDFieldLenMismatches: 0 isisSysStatMaxAreaAddrMismatches: 0 isisSysStatPartChanges: 0 </pre>

isisSysStatSPFRuns: 4

IS-IS Level-2 isisSystemCounterEntry:
isisSysStatCorrLSPs: 0
isisSysStatAuthTypeFails: 0
isisSysStatAuthFails: 0
isisSysStatLSPDbaseOloads: 0
isisSysStatManAddrDropFromAreas: 0
isisSysStatAttmptToExMaxSeqNums: 0
isisSysStatSeqNumSkips: 0
isisSysStatOwnLSPPurges: 0
isisSysStatIDFieldLenMismatches: 0
isisSysStatMaxAreaAddrMismatches: 0
isisSysStatPartChanges: 0
isisSysStatSPFRuns: 6
Switch#

show isis interface counter

Command	show isis interface counter
Parameter	The count information used to display the status and configuration of the ISIS interface. -
Default	-
Mode	All modes
Usage Guide	-
Example	Switch#show isis interface counter Vlan111: IS-IS LAN Level-1 isisCircuitCounterEntry: isisCircAdjChanges: 0 isisCircNumAdj: 0 isisCircInitFails: 0 isisCircRejAdjs: 0 isisCircIDFieldLenMismatches: 0 isisCircMaxAreaAddrMismatches: 0 isisCircAuthTypeFails: 0 isisCircAuthFails: 0 isisCircLanDesISChanges: 0 IS-IS LAN Level-2 isisCircuitCounterEntry: isisCircAdjChanges: 4 isisCircNumAdj: 2

```

isisCircInitFails: 201
isisCircRejAdjs: 0
isisCircIDFieldLenMismatches: 0
isisCircMaxAreaAddrMismatches: 0
isisCircAuthTypeFails: 0
isisCircAuthFails: 0
isisCircLanDesISChanges: 2
IS-IS Level-1 isisPacketCounterEntry:
  isisPacketCountIIHello in/out: 0/128
  isisPacketCountLSP in/out: 0/0
  isisPacketCountCSNP in/out: 0/0
  isisPacketCountPSNP in/out: 0/0
  isisPacketCountUnknown in/out: 0/0
IS-IS Level-2 isisPacketCounterEntry:
  isisPacketCountIIHello in/out: 143/209
  isisPacketCountLSP in/out: 70/6
  isisPacketCountCSNP in/out: 0/32
  isisPacketCountPSNP in/out: 1/0
  isisPacketCountUnknown in/out: 0/0

```

show cspf lsp

Command	show cspf lsp
Parameter	Used to display the information of CSPF LSP. -
Default	-
Mode	All modes
Usage Guide	-
Example	Switch# show cspf lsp

clear ip isis

Command	clear ip isis [all <area-tag>]
Parameter	Used to display the restart of the ISIS process. All All ISIS processes <area-tag> Specify the area tag for the ISIS process

Default	-
Mode	Admin mode
Usage Guide	
Example	Switch# clear ip isis all

8 Commands for IPV6 ISIS

address-family ipv6

Command	address-family ipv6 [unicast] no address-family ipv6 [unicast]
	Use this command to enter the IPv6 address series command mode. The "no" operation of this command cancels this configuration.
Parameter	unicast Address family modifier
Default	There is no default configuration.
Mode	ISIS router mode
Usage Guide	-
Example	Switch#config terminal Switch(config)#router isis Switch(config-router)# address-family ipv6 unicast Switch(config-router-af)#

summary-prefix

Command	summary-prefix X:X::X:X/M [level-1 level-1-2 level-2] no summary-prefix X:X::X:X/M
	Use this command to summarize the IPv6 routes. The "no" operation of this command will cancel this configuration.
Parameter	X:X::X:X/M IPv6 prefix, for example: fe80::1/64; level-1 Summarize into level-1 area level-1-2 Summarize into both area and sub-domain level-2 Summarize into level-2 sub-domain
Default	There is no default configuration.

Mode	ISIS routing IPv6 address group mode
Usage Guide	-
Example	<pre>Switch#config terminal Switch(config)#router isis Switch(config-router)# address-family ipv6 unicast Switch(config-router-af)# summary-prefix fe80::1/64 level-1</pre>

multi-topology

Command	multi-topology [transition] no multi-topology [transition]
	Use this command to enable the multi-topology mode. The "no" operation of this command will cancel this configuration.
Parameter	Transition Accept and generate both IS-IS IPv6 and Multi-topology IPv6 TLVs
Default	There is no default configuration.
Mode	ISIS routing IPv6 address group mode
Usage Guide	-
Example	<pre>Switch#config terminal Switch(config)#router isis Switch(config-router)# address-family ipv6 unicast Switch(config-router-af)# multi-topology transition</pre>

redistribute

Command	<pre>redistribute {kernel connected bgp rip static } <level-1 level-1-2 level-2> [metric<value>] [metric-type (< external> < internal>)] [metric<value> route- map<WORD>]</pre> <pre>redistribute isis <WORD1> <level-1 into level-2 level-2 into level-1> [distribute- list<WORD2> route-map<WORD>]</pre> <pre>redistribute ospf <level-1 level-1-2 level-2> [metric<value>] [metric-type (< external> < internal>)] [metric<value> route-map<WORD>]</pre> <pre>no redistribute {kernel connected bgp rip static } <level-1 level-1-2 level- 2> [metric<value>] [metric-type (< external> < internal>)] [metric<value> </pre>

route-map<WORD>]

no redistribute isis <WORD1> <level-1 into level-2 | level-2 into level-1> [distribute-list<WORD2> | route-map<WORD>]

no redistribute ospf <level-1 | level-1-2 | level-2> [metric<value>] [metric-type (< external> | < internal>)] [metric<value> | route-map<WORD>]

Parameter

kernel introduce from kernel route.

connected introduce from direct route.

static introduce from static route.

rip introduce from the RIP route.

bgp introduce from BGP route.

isis introduce from ISIS route.

<WORD> Route-map name

is-type level of IS-IS

level-1 IS-IS level-1 routes only

level-1-2 IS-IS level-1 and level-2 routes

level-2 IS-IS level-2 routes only

metric <value> is the introduced metric value, ranging between 0- 4261412864.

metric-type (< external> | < internal> set IS-IS External or Internal metric type

<WORD1> ISO routing area tag

<WORD2> Access-list name

Default

-

Mode

ISIS routing IPv6 address group mode

Usage Guide

Redistributes routes from other routing protocols into IS-IS. Supported source protocols include kernel, connected, static, rip, bgp, and isis. The command allows configuration of the IS-IS level, metric value, metric type (external/internal), and optional route-map or distribute-list for filtering. The no form removes the redistribution configuration.

Example

Switch#config terminal

Switch(config)#router isis

Switch(config-router)#address-family ipv6 unicast

Switch(config-router-af)# redistribute bgp level-1 metric 1 metric-type external route-map 1

default-information

Command

default-information originate route-map <WORD>

no default-information originate route-map <WORD>

Parameter

<WORD>

Pointer to route-map entries

Default	There is no default configuration.
Mode	ISIS routing IPv6 address group mode
Usage Guide	Generates a default route into IS-IS when the condition specified in the route-map is met. The no form removes this configuration.
Example	<pre>Switch#config terminal Switch(config)#router isis Switch(config-router)# address-family ipv6 unicast Switch(config-router-af)# default-information originate route-map 1</pre>

adjacency-check

Command	adjacency-check
	no adjacency-check
Parameter	NONE
Default	There is no default configuration.
Mode	ISIS routing IPv6 address group mode
Usage Guide	Enables adjacency check for IS-IS IPv6 unicast address family. The no form disables this function.
Example	<pre>Switch#config terminal Switch(config)#router isis Switch(config-router)# address-family ipv6 unicast Switch(config-router-af)# adjacency-check</pre>

ipv6 router isis

Command	ipv6 router isis [WORD] no ipv6 router isis [WORD]
	Use this command to add the interface to the corresponding ISIS process. The "no" operation of this command will cancel this configuration.
Parameter	WORD Specify the ISIS process Routing process tag, which should be a string with a length not exceeding 60 characters;
Default	There is no default configuration.

Mode	Interface Configuration Mode
Usage Guide	-
Example	Switch#config terminal Switch(config)#interface vlan 21 Switch(config-if-vlan21)ip router isis test

show ipv6 isis topology

Command	show ipv6 isis <area-tag> topology [level-1 level-2]	
	Used to display the information of the ISIS path to the intermediate system.	
Parameter	level-1	Path to all level-1 routers in the area
	level-2	Path to all level-2 routers in the domain
Default	-	
Mode	All modes	
Usage Guide	-	
Example	Switch# show ipv6 isis topology level-1	

show ipv6 isis route

Command	show ipv6 isis [<area-tag>] route	
	Used to display the ISIS routing table of the IPv6 protocol.	
Parameter	<area-tag>	Routing area identifier of the ISIS process
Default	-	
Mode	All modes	
Usage Guide	-	
Example	Switch# show ipv6 isis route Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, D - discard, e - external metric	

9.Commands for BFD

bfd authentication key

Command	bfd authentication key <1-255> no bfd authentication key
	Enable BFD authentication function for the interface and configure the used key. The "no" operation of this command will disable the BFD authentication function.
Parameter	<1-255 > Key number
Default	The interface has not enabled the BFD authentication function.
Mode	Interface configuration mode
Usage Guide	Configure the key number used by the BFD interface. Different interfaces can use different encryption authentication methods. Output: BFD specifies the interface to use encrypted authentication.
Example	Enable BFD authentication function on the interface, and use key number 1. Switch (config-if-vlan50) # bfd authentication key 1

bfd authentication key md5

Command	bfd authentication key <1-255> md5 <WORD> no bfd authentication key <1-255>
	Configure the key used by BFD and the authentication string encrypted by md5. The "no" command deletes the configured key.
Parameter	<1-255 > key number <WORD> MD5 Authentication key (at most 16 characters)
Default	No authentication key and authentication string are configured by default.
Mode	Global configuration mode
Usage Guide	Configure the md5 mode and authentication key string used by BFD authentication. After configuring this command, BFD will use the optional field in the packet for authentication. BFD will only establish a neighbor relationship when the key configurations on both ends of BFD are consistent.

Example	Use MD5 encryption, key number is 1, and authentication string is 123456. Switch (config)#bfd authentication key 1 md5 123456
bfd authentication key text	
Command	bfd authentication key <1-255> text <WORD> no bfd authentication key <1-255>
Parameter	Configure the key used by BFD authentication and the authentication string encrypted by text. The "no" command deletes the configured key. <1-255 > Key number <WORD> Text Authentication key (at most 16 characters)
Default	No authentication key and authentication string are configured by default.
Mode	Global configuration mode
Usage Guide	Configure the authentication mode and authentication string used by BFD. After configuring this command, BFD will use the optional field in the packet for authentication. BFD will only establish a neighbor relationship when the authentication passwords on both ends of BFD are consistent.
Example	Use text encryption, key number is 1, and authentication string is 123456. Switch (config)#bfd authentication key 1 text 123456

bfd echo

Command	bfd echo no bfd echo
Parameter	Enable bfd echo function. The "no" command disables the bfd echo function. -
Default	The echo function is not enabled on the interface by default.
Mode	Interface configuration mode
Usage Guide	Enable the echo function. The session in UP status sends echo packets, thereby reducing the frequency of control packets.

Example	Enable the echo function on the interface. <pre>Switch (config)#in vlan 50 Switch (config-if-vlan50)#bfd echo</pre>
bfd echo-source-ip	
Command	bfd echo-source-ip <ipv4-address> no bfd echo-source-ip
Parameter	Configure the source address of Echo packets for link fault detection. The "no" command deletes the configured source address of Echo packets. <ipv4-address> It is an IPv4 address. The legitimacy of the configured parameter is guaranteed by the user, and no legitimacy check of the address is performed.
Default	No source address of Echo packets is configured by default.
Mode	Global configuration mode
Usage Guide	When IPv4 link BFD uses the echo function for link fault detection, the source address of Echo packets needs to be configured. The configuration of the source address is flexible, as long as it avoids the generation of ICMP redirect packets. The destination address of the packet is a local interface address to ensure that the packet can return along the original path. There are no special requirements for the UDP data content of the packet.
Example	Configure the source address of bfd echo packets to 192.168.1.1. <pre>Switch (config)#bfd echo-source-ip 192.168.1.1</pre>

bfd echo-source-ipv6

Command	bfd echo-source-ipv6 <ipv6-address> no bfd echo-source-ipv6
Parameter	Configure the source address of Echo packets for link fault detection. The "no" command deletes the configured source address of Echo packets. <ipv6-address> It is an IPv6 address. The legitimacy of the configured parameter is guaranteed by the user, and no legitimacy check of the address is performed.
Default	No source address of Echo packets is configured by default.

Mode	Global configuration mode
Usage Guide	When IPv6 link BFD uses the echo function for link fault detection, the source address of Echo packets needs to be configured. The configuration of the source address is flexible, as long as it avoids the generation of ICMPv6 redirect packets. The destination address of the packet is a local interface address to ensure that the packet can return along the original path. There are no special requirements for the UDP data content of the packet.
Example	Configure the source address of bfd echo packets to 2000::1 Switch (config)#bfd echo-source-ipv6 2000::1

bfd enable

Command	bfd enable no bfd enable
	Enable bfd echo function. The "no" command disables the bfd echo function.
Parameter	-
Default	The default function is not enabled.
Mode	VRRP(v3) group configuration mode
Usage Guide	After enabling the BFD detection function on this group, if the group receives a hello packet when it is in the backup state, it will notify BFD to establish the corresponding session. The local IP and remote IP are the actual IPs of the two ends' interfaces.
Example	Enable BFD function on VRRP group 1. Switch (config)#router vrrp 1 Switch (config-router)#virtual-ip 50.1.1.10 Switch (config-router)#interface vlan 50 Switch (config-router)#bfd enable Switch (config-router)#enable Enable BFD function on VRRPv3 group 1. Switch (config)#router ipv6 vrrp 1 Switch (config-router)#virtual-ipv6 fe80::1 interface vlan 50 Switch (config-router)#bfd enable Switch (config-router)#enable

bfd interval

Command	bfd interval <value1> min_rx <value2> multiplier <value3> no bfd interval
	Configure the minimum sending time interval and session detection multiplier of BFD control packets. The “no” operation of this command restores the detection multiplier to the default value.
Parameter	<value1> Minimum sending time interval, unit: ms, range: 200-1000. The minimum sending time interval may vary for different models. <value2> Minimum receiving time interval, unit: ms, range: 200-1000. The minimum receiving time interval may vary for different models. <value3> Session detection multiplier, range: 3-50.
Default	The default minimum sending interval is 400ms, the minimum receiving interval is 400ms, and the detection multiplier is 5.
Mode	Interface configuration mode
Usage Guide	Configure the minimum sending time interval and session detection multiplier of BFD control packets. The default minimum sending time interval is 400ms, and the session detection multiplier is 5.
Example	Modify the BFD minimum sending interval and minimum receiving interval of the interface to 800ms, and the detection multiplier to 50. Switch (config)#in vlan 50 Switch (config-if-vlan50)#bfd interval 800 min-rx 800 multiplier 50 Switch (config-if-vlan50)#

bfd min-echo-recv-interval

Command	bfd min-echo-recv-interval <value> no bfd min-echo-recv-interval
	Configure the minimum receiving time interval of BFD control packets. The “no” command operation restores the minimum receiving interval of echo packets to the default value.
Parameter	<value> Minimum receiving time interval, unit: ms, range: 200-1000. The minimum receiving time interval may vary for different models.

Default	The default minimum echo receiving interval is 400ms.
Mode	Interface configuration mode
Usage Guide	<value> is the minimum receiving time interval, unit: ms, range: 200-1000. The minimum receiving time interval may vary for different models. The default minimum receiving time interval is 400ms.
Example	Configure the minimum receiving interval of BFD echo packets to 800ms. Switch (config)#in vlan 50 Switch (config-if-vlan50)#bfd min-echo-recv-interval 800

bfd mode

Command	bfd mode {active passive} no bfd mode
	Configure the working mode before BFD session establishment. The default mode is active. The “no” operation of this command restores the active mode.
Parameter	active active mode passive passive mode
Default	The default working mode is active.
Mode	Global configuration mode
Usage Guide	Configure the working mode before BFD session establishment. By default, it is active mode. Regardless of whether BFD control packets from the peer are received, BFD control packets will be sent actively.
Example	Set the global BFD working mode to passive. Switch (config)#bfd mode passive

debug bfd

Command	debug bfd {packet events all fsm error timer notify}
	Enable the corresponding debug switch for BFD functions.
Parameter	all Turn on all debugging packet BFD packets events BFD events fsm BFD fsm error BFD error

timer	BFD timer
notify	BFD notify
Default	-
Mode	Admin mode
Usage Guide	Enable the corresponding debug switch for BFD functions.
Example	Enable the debug switch for BFD functions. Switch #debug bfd all

ip ospf bfd enable

Command	ip ospf bfd enable no ip ospf bfd enable
	Configure the OSPF protocol to be linked with BFD on the specified interface. The "no" command operation is used to disable the function of linking the configured OSPF protocol with BFD.
Parameter	-
Default	By default, the linkage function between OSPF and BFD is not enabled.
Mode	Interface configuration mode
Usage Guide	-
Example	Switch (config-if-vlan50)#ip ospf bfd enable

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 [<1-255> <WORD>]
	Configure static routes to be linked with BFD. The "no" command operation cancels the configuration of static routes and BFD linkage.
Parameter	<name> VRF name <ipv4-address> route destination address mask subnet mask of the route nexthop destination address of the route

<1-255>	Distance value for this route
<WORD>	Tag
Default	The default configuration does not link static routes with BFD.
Mode	Config mode
Usage Guide	Configure BFD to be linked with this route and specify the detection mode. When specifying the outgoing interface, BFD binding is not supported for now.
Example	Configure BFD and link it with this configuration of static routing and BFD. Switch (config)#ip route 10.1.1.0/24 20.1.1.2 bfd 2

ipv6 ospf bfd enable

Command	ipv6 ospf bfd enable [instance-id <value>] no ipv6 ospf bfd enable [instance-id <value>]
Parameter	Configure the OSPFv3 protocol to be linked with BFD on the specified interface. The "no" command is used to disable the configured linkage function. <value> <0-255> Interface instance ID
Default	By default, the linkage function between OSPF and BFD is not enabled.
Mode	Interface configuration mode
Usage Guide	By default, the linkage function is not configured on the specified interface that has started the OSPFv3 protocol. When BFD detects a link failure, it will notify the OSPFv3 protocol, enabling it to handle the failure quickly.
Example	Enable the linkage function of OSPFv3 and BFD on the interface. Switch (config)#in vlan 50 Switch (config-if-vlan50)# ipv6 ospf bfd enable

ipv6 ospf bfd enable instance-id

Command	ipv6 ospf bfd enable instance-id <0-255> no ipv6 ospf bfd enable
Parameter	Configure the specified OSPFv3 instance to be linked with BFD on the designated interface. The "no" command is used to disable the configured linkage function. -

Default	Default setting is not enabled.
Mode	Interface configuration mode
Usage Guide	On the designated interface where the OSPFv3 protocol has been activated, the linkage function of the specified instance is configured. When BFD detects a link failure, it will notify the OSPFv3 protocol, enabling it to quickly handle the fault.
Example	Enable the linkage function of OSPFv3 and BFD on the interface. Switch (config)#in vlan 50 Switch (config-if-vlan50)# ipv6 ospf bfd enable instance-id 254

ipv6 rip bfd enable

Command	ipv6 rip bfd enable no ipv6 rip bfd enable
	On the interface, configure the RIPng protocol to be linked with BFD on the specified interface. The "no" command is used to disable the configured linkage function.
Parameter	-
Default	Default setting is not enabled.
Mode	Interface configuration mode
Usage Guide	RIPng will notify BFD to establish a session with the source IP address of the RIPng packet as the remote IP address, and BFD will detect the session status and promptly notify RIPng of the status.
Example	Enable the linkage function between RIPng and BFD on the interface. Switch (config)#in vlan 50 Switch (config-if-vlan50)# ipv6 rip bfd enable

ipv6 route bfd

Command	ipv6 route <ipv6-address> <nexthop> bfd <1-225> no ipv6 route <ipv6-address> <nexthop> bfd <1-225>

Configure the IPv6 static route to be linked with BFD.
The "no" command is used to cancel this linkage configuration.

Parameter	<ipv6-address>	Routing destination address
	nexthop	The next-hop address of the route
	<1-225>	Distance value for this prefix

Default The default configuration does not link IPv6 static routes with BFD.

Mode Config configuration mode

Usage Guide Configure BFD to be linked with this route and specify the detection mode. When specifying the outgoing interface, BFD binding is not supported for now.

Example Configure IPv6 static routes in conjunction with BFD functionality
Switch (config)#ipv6 route 3000::/64 2010::1 bfd 1

neighbor

Command **neighbor [<ipv6-address> | <ipv4-address> | <WORD>] fall-over bfd [<multi-hop> | <single-hop>]**
no neighbor [<ipv6-address> | <ipv4-address> | <WORD>] fall-over bfd [<multi-hop> | <single-hop>]

Configure the BFD link detection function on the BGP (4+) peer neighbors.
The "no" command is used to cancel this configuration.

Parameter	<ipv4-address>	IPv4 address
	<ipv6-address>	IPv6 address
	<WORD>	Neighbor tag
	<multi-hop>	Specify multi-hop bfd session
	<single-hop>	Specify single-hop bfd session

Default Default setting is not enabled.

Mode Routing configuration mode

Usage Guide Enable BFD link detection on the configured BGP (4+) peer neighbors. When BFD detects a failure in the neighbor link, it will notify the BGP (4+) protocol.

Example Enable the BFD link detection function for the BGP peer neighbors.
Switch (config)#router bgp 1
Switch (config-router)#neighbor 1.1.1.1 fall-over bfd single-hop

rip bfd enable

Command	rip bfd enable no rip bfd enable
	Configure the RIP protocol to be linked with BFD on the specified interface. The "no" command is used to cancel this configuration.
Parameter	-
Default	Default setting is not enabled.
Mode	Interface configuration mode
Usage Guide	RIP will notify BFD to establish a BFD session using the source IP address of the received RIP packet as the remote endpoint. BFD then monitors the session state and promptly reports any changes back to RIP for fast convergence.
Example	Enable the linkage function between RIP and BFD on the interface. Switch (config-if-vlan50)#rip bfd enable

show bfd neighbor

Command	show bfd neighbor [[<ipv6-address> <ipv4-address>][details]]
	Display the information of BFD neighbors in the switch
Parameter	<ipv6-address> The neighbor information displayed for the specified IPv6 address. <ipv4-address> The neighbor information displayed for the specified IPv4 address. Here, the IP address refers to the remote IP address. Details Display detailed information about neighbor.
Default	-
Mode	All modes
Usage Guide	Display the information of BFD neighbors in the switch
Example	View the relevant information of the BFD neighbor. Switch #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. Pol 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						
Pol 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)						

show bfd interface

Command	show bfd interface
	Display the information of BFD interfaces in the switch
Parameter	None
Default	-
Mode	All modes
Usage Guide	Display the information of BFD interfaces in the switch
Example	View the relevant information of the BFD interface. Switch #show bfd interface

16-Commands for Stacking

1 Commands for Vsf Configuration

switch convert mode

Command	switch convert mode <stand-alone> <vsf>	
Parameter	<stand-alone>	Stand alone mode
	<vsf>	Virtual Switch Framework
Default	At startup, based on the VSF configuration file "vsf.cfg", the system determines the mode in which the device should operate.	
Mode	Global Mode	
Usage Guide	The equipment supports two operation modes: independent operation mode and VSF mode. The device in the independent operation mode can only operate independently, while the device in the VSF mode can form a VSF with other devices. The two modes can be switched through the command line.	
Example	When the equipment is in independent operation mode, configure the equipment to enter VSF mode. Switch(config)#switch convert mode vsf	

vsf port-group

Command	vsf port-group <port-number> no vsf port-group <port-number>	
Parameter	port-number	Logical VSF port number, with values ranging from 1 to 2
Default	Not configured	
Mode	Global Mode	
Usage Guide	Configure VSF ports. The same device can only have two VSF port-groups configured, namely VSF port-group 1 and VSF port-group 2.	
Example	Configure the logical VSF port. Switch(config)#vsf port group 1	

vsf port-group interface ethernet

Command	vsf port-group interface [<IFNAME> ethernet <IFNAME>] no vsf port-group interface [<IFNAME> ethernet <IFNAME>]		
Parameter	<table><tr><td><IFNAME></td><td>Interface Name or number</td></tr></table>	<IFNAME>	Interface Name or number
<IFNAME>	Interface Name or number		
Default	Default: Unbound physical port		
Mode	VSF port mode		
Usage Guide	A vsf port-group can bind up to 8 physical ports. When a port joins the vsfport-group mode, it is set to "on". If more than 8 ports are bound, it will prompt the user that binding is not possible. Cross-board binding of physical ports is supported. Currently, only 10-Gigabit ports and logical VSF ports can be bound.		
Example	Create the logical VSF interface and enter the configuration mode of the VSF interface. Bind the physical port 1/0/1 to the logical VSF interface. Switch(config)#vsf port-group 1 Switch(config)#vsf port-group interface ethernet 1/0/1		

vsf domain

Command	vsf domain <domain-id> no vsf domain		
Parameter	<table><tr><td>domain-id</td><td>Domain number, with the range of values from 1 to 32</td></tr></table>	domain-id	Domain number, with the range of values from 1 to 32
domain-id	Domain number, with the range of values from 1 to 32		
Default	The equipment is in domain 1		
Mode	Global Mode		
Usage Guide	A domain is a logical concept. When devices are connected together through the VSF link, they form a VSF. The collection of these member devices constitutes a VSF domain. To accommodate various networking applications, multiple VSFs can be deployed within the same network. VSFs use domain numbers to distinguish each other. Devices within the same domain can form a VSF, while devices or VSFs from different domains cannot form a VSF. Before forming a VSF, a conflict check for domain numbers needs to be conducted. The default value of the domain number is 1.		
Example	In the standalone mode, set the vsf domain number to 2. Switch(config)#vsf domain 2		

vsf member

Command	vsf member < <i>member-id</i> > no vsf member < <i>member-id</i> >	
Parameter	member-id	Member ID, the valid range of values is <1 - 8>
Default	The equipment does not have a member number	
Mode	Global Mode	
Usage Guide	The member number identifies each device. In the VSF group, each device has a unique member number. This number must be configured in order to enter the VSF mode. Configuring this command multiple times, the last one takes effect. Initial state, there is no member number. After the device enters the VSF mode, the port format is modified according to the member number. Conflicts in member numbers cannot form VSF.	
Example	In the standalone mode, the configuration member number is 2. Switch(config)#vsf member 2	

vsf priority

Command	vsf priority < <i>priority</i> > no vsf priority	
Parameter	priority	The priority value of VSF members, with the range of values being 1 to 32.
Default	The default priority of the equipment is 1.	
Mode	Global Mode	
Usage Guide	In the standalone operation mode, member priorities are configured. Member priorities are used for role elections. The higher the member priority value, the higher the priority. Devices with higher priorities have a greater chance of becoming the Master when competing. By configuring different priorities for different devices, a certain device can be designated as the Master of the VSF.	

Example

In the standalone mode, set the priority of the configuration members to 30.
Switch(config)#vsf priority 30

vsf auto-merge enable

Command

vsf auto-merge enable
no vsf auto-merge enable

Parameter

-

Default

The equipment does not have a member number.

Mode

Global Mode

Usage Guide

When the two VSF groups have achieved the correct physical connection for some reason, and the connection method is to use their respective VSF ports for connection, and there are no conflicts in vsf domain or vsf member id, during the connection process, operations such as port up, establishment of VSF ports, and binding will trigger the automatic merging of the two VSF groups. During the merging process, based on the comparison of priority and member id, the VSF group that fails the election will be restarted, and after the restart, it will join the VSF group that has won the election.

Example

In the standalone mode, enable the automatic merging function.
Switch(config)#vsf auto-merge enable

vsf member description

Command

vsf member <member-id> description <text>
no vsf member <member-id> description

Parameter

member-id	Member number
text	User-defined description

Default

The equipment does not have a member number.

Mode

Global Mode

Usage Guide

In the VSF mode, add the description information of the device. This is convenient for managing the device. For example, if there are multiple VSFs in a network, or if the physical locations of the members of a VSF are relatively scattered, then the role of each device in the network topology and other user-defined information can be clarified by adding the description method.

Example

Add member 1 information as "Master"
Switch(config)#vsf member 1 description Master

vsf link delay

Command

vsf link delay <interval>
no vsf link delay

Parameter

interval	The delay reporting time value for VSF link down is 0 by default, meaning it is reported immediately. The range is from 200 to 2000 milliseconds.

Default

The default delay reporting time value has not been configured. The value is 0.

Mode

Global Mode

Usage Guide

After configuring the vsf link delay, if the VSF link status changes from up to down, the port will not immediately report the link status change to the system. After the configured time interval, if the VSF link is still in the down state, the port will then report the link status change to the system, and the system will make corresponding processing. If the VSF link status changes from down to up, the link layer will immediately report to the system. This command takes effect immediately after being configured.

Example

In the VSF operation mode, the configuration delay reporting is set to 1500 milliseconds.
Switch(config)#vsf link delay 1500

2 Commands for Mad Configuration

vsf mad lacp enable

Command	vsf mad lacp enable no vsf mad lacp enable
Parameter	-
Default	LACP MAD detection function is turned off
Mode	Port-channel configuration mode
Usage Guide	Only devices in VSF mode can configure this command. Configure the specified port-channel as an LACP MAD conflict detection group. Members of the group send TLV messages with MAD.
Example	Enable the LACP MAD detection function on the port-channel1 interface. Switch(config)#interface port-channel 1 Switch(config-if-port-channel1)#vsf mad lacp enable

vsf mad bfd enable

Command	vsf mad bfd enable vsf mad bfd disable
Parameter	-
Default	BFD MAD detection function has been turned off.
Mode	Interface Configuration Mode
Usage Guide	Only devices in VSF mode can configure this command. Configure the specified interface to support BFD MAD detection function.
Example	Enable the BFD MAD detection function in interface VLAN 2. Switch(config)#interface vlan 2 Switch(config-if-vlan2)#vsf mad bfd enable

vsf mad ip address

Command	vsf mad ip address <i><ip-address></i> <i><ip-mask></i> member <i><member-number></i> no vsf mad ip address <i><ip-address></i> <i><ip-mask></i> member <i><member-number></i>	
Parameter	ip-address	IP address
	ip-mask	Subnet mask
	member-number	Member device number, within the range of: 1 - 8
Default	The interface has not been configured with the MAD address.	
Mode	Interface Configuration Mode	
Usage Guide	Only devices in VSF mode can configure this command. When configuring this command, a session with the configuration address as the remote address will be created.	
Example	Create BFD sessions corresponding to the member devices in 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	

vsf mad exclude

Command	vsf mad exclude no vsf mad exclude	
Parameter	-	
Default	The equipment is not configured with the MAD retention port.	
Mode	Port Mode	
Usage Guide	After the VSF link is disconnected, there will be two devices with exactly the same global configuration in the network. When these devices connect to the network, it may cause network failures. To prevent this from happening, the system will perform multiple Active detection and finally retain only one Active device. The other devices will enter the Recovery state and all business interfaces on the Recovery state devices will be closed. Using this command allows the specified port not to be closed. Which interfaces need to be retained is determined by the user.	

Example	Configure the MAD retention port at port 2/1/4. Switch(config)#inte e 2/1/4 Switch (config-if-ethernet2/1/4)#vsf mad exclude

vsf mad restore

Command	vsf mad restore
Parameter	-
Default	VSF is not configured with restore.
Mode	Global Mode
Usage Guide	The VSF link breakage causes multiple Active conflicts. The original VSF splits into two VSFs in the active state. To prevent configuration conflicts in the network, the VSF system will use the multi-Active detection mechanism to keep the state of one VSF as Active (allowing it to continue working normally), and change the state of the other VSF to Recovery (VSFs in this state cannot process business messages). If a VSF in the Active state fails and cannot work, this command can be used to restore the VSF in the Recovery state to a normal working state.
Example	Restore the VSF that is in the Recovery state to its normal working condition. Switch(config)#vsf mad restore

show mad config

Command	show mad config
Parameter	-
Default	-
Mode	All modes
Usage Guide	This command is only available in VSF mode. It displays whether LACP and BFD are enabled, and also retrieves which ports have enabled these functions.
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	
display information	explain
Current lacp MAD status	Display the current status of lacp MAD
Current bfd MAD status	Display the current status of BFD MAD
Reserved ports	The reserved interface configured by the user
Reserved ports(defaults)	The interfaces that are automatically retained by the system (do not require user configuration and are retained automatically)
MAD lacp enabled aggregation port	Enable the aggregated port with LACP MAD functionality
MAD BFD enabled interface	The interface that enables BFD MAD

3 Commands for Vsf Debug

show vsf

Command	show vsf
Parameter	-
Default	-
Mode	All modes
Usage Guide	This command is only available in VSF mode. It obtains the role election information through the VSF protocol, and acquires the VSF configuration information by reading the VSF configuration file vsf.cfg of each device. It also retrieves and displays information such as bridge MAC, CPU-MAC, etc.

Example	Switch# show vsf

show vsf config

Command	show vsf config
Parameter	-
Default	-
Mode	All modes
Usage Guide	When the VSF group consists of a single device, the configuration of this device is collected; if the VSF group contains multiple devices, a configuration collection request is sent to other devices to collect the configuration information of the entire VSF group.

Example	Switch# show vsf config

show vsf cpu-database all-member brief-information

Command	show vsf cpu-database all-member brief-information
Parameter	-
Default	-
Mode	All modes
Usage Guide	Display the brief information of all VSF 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

show vsf cpu-database member basic-information

Command	show vsf cpu-database [member <1-8>] basic information	
Parameter	<1-8>	Member ID of VSF
Default	-	
Mode	All modes	
Usage Guide	This command can display the basic information of all or the specified VSF members in the CPU database.	
Example	<pre>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 Priority: 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</pre>	

show vsf cpu-database member running-information

Command	show vsf cpu-database [member <1-8>] running-information

Parameter	<1-8> Member ID of VSF
Default	None
Mode	All modes
Usage Guide	Display the operation information of all or the specified VSF members in the CPU database.
Example	<pre>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</pre>

show vsf cpu-database member port-information

Command	show vsf cpu-database [member <1-8>] port-information	
Parameter	<1-8>	VSF member ID
Default	-	
Mode	All modes	
Usage Guide	Display the basic information of the VSF ports of all or the specified VSF members in the CPU database.	
Example	<pre>Switch# show vsf cpu-database member 2 port-information Vsf cpu database member 2 port information: Vsf port index 1:</pre>	

Unit: 0
port: 1
Weight: 0
Bflag: 1

show vsf cpu-database member port-link-information

Command	show vsf cpu-database [member <1-8>] port-link-information		
Parameter	<table><tr><td><1-8></td><td>VSF member ID</td></tr></table>	<1-8>	VSF member ID
<1-8>	VSF member ID		
Default	-		
Mode	All modes		
Usage Guide	Display the operational information of the VSF interface links of all or the specified VSF members in the CPU database.		
Example	<pre>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</pre>		

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>	
Parameter	alive	Keep-alive message
	all	Open all VSF protocol messages
	config	Configuration information message. This parameter refers to the message exchange between VSF members during the configuration stage. This stage mainly involves the exchange of messages among VSF members to obtain the necessary information for master election and to conduct the election of master and standby master
	member-infor	Member Information Message
	probe	The VSF member detection message, whose function is to detect all the information of the VSF interfaces
	routing	The message for disseminating VSF member information, which includes: local VSF port information, required modid information, number of chips information, Master election priority, status information of CPUDB, as well as the destination chip number and port number information of the CPU reaching this CPU
	topo	Topology analysis message. The task of the topology analysis stage is that the Master calculates an acyclic network based on the collected topology information, and the Master assigns Module IDs to all members, calculates the corresponding relationship between each member's VSF port and the destination Module ID, and then distributes these results to each member.
	Default	-
Mode	Admin mode	
Usage Guide	During the formation process of the VSF group, it will go through stages such as discovery and topology analysis. At different stages, the devices will be in different states. For example, in the discovery stage, the devices will go through three sub-stages: probe, routing, and config. Through this debug switch, you can selectively view the detailed information of the corresponding protocol packets at different stages.	
Example	Turn on the switch for viewing the VSF keep-alive message log Switch# debug vsf packet detail alive	

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>	
Parameter	receive	Turn on the switch for debugging received VSF messages
	send	Turn on the debugging switch for sending VSF messages
	all	Turn on the receiving and sending functions simultaneously
	vsf-port-number	VSF port number
Default	-	
Mode	Admin mode	
Usage Guide	After enabling the switch for debugging information of VSF messages, you can observe the sending and receiving of VSF protocol messages.	
Example	Turn on the switch for sending VSF message logs Switch# debug vsf packet send	

debug vsf event

Command	debug vsf event no debug vsf event	
Parameter	-	
Default	-	
Mode	Admin mode	
Usage Guide	After enabling the VSF event debugging information switch, when the defined event occurs during each stage of VSF operation, corresponding outputs can be provided to the user.	
Example	Enable VSF event debugging information. Switch# debug vsf event	

debug vsf error

Command	debug vsf error no debug vsf error
Parameter	-
Default	-
Mode	Admin mode
Usage Guide	After enabling this debug, various error messages during each stage of the VSF operation can be displayed.
Example	Enable VSF error debugging information. Switch# debug vsf error

debug vsf atp

Command	debug vsf atp no debug vsf atp
Parameter	-
Default	-
Mode	Admin mode
Usage Guide	Enables debugging for VSF ATP (Auto Test Procedure) events. The no form disables this debugging.
Example	Enable VSF event debugging information. Switch# debug vsf atp

debug vsf detail

Command	debug vsf detail <alive> <all> <disc> <topo> no debug vsf detail <alive> <all> <disc> <topo>

Parameter	-
Default	-
Mode	Admin mode
Usage Guide	Enables detailed VSF debugging information for specific modules. The alive option debugs keepalive messages, disc debugs discovery processes, topo debugs topology events, and all enables all detailed debugging.
Example	Enable VSF event debugging information. Switch# debug vsf detail all

debug vsf fsm

Command	debug vsf fsm no debug vsf fsm
Parameter	-
Default	-
Mode	Admin mode
Usage Guide	Enables debugging for VSF Finite State Machine (FSM) state transitions.
Example	Enable VSF event debugging information. Switch# debug vsf fsm

debug vsf restart

Command	debug vsf restart no debug vsf restart
Parameter	-
Default	-
Mode	Admin mode
Usage Guide	Enables debugging for VSF restart events.

Example	Enable VSF event debugging information. Switch# debug vsf restart

debug vsf timer

Command	debug vsf timer no debug vsf timer
Parameter	-
Default	-
Mode	Admin mode
Usage Guide	Enables debugging for VSF timer events.

Example	Enable VSF event debugging information. Switch# debug vsf timer

debug vsf warn

Command	debug vsf warn no debug vsf warn
Parameter	-
Default	-
Mode	Admin mode
Usage Guide	Enables debugging for VSF warning messages.

Example	Enable VSF event debugging information. Switch# debug vsf warn

4 Commands for devsm configuration

debug devsm

Command	debug devsm {send receive state} no debug devsm {send receive state}	
Parameter	send	Display the sent device management messages
	receive	Display the received device management messages
	stat	Display the information on the status changes of the board cards
Default	-	
Mode	Admin mode	
Usage Guide	This command shows the status of message transmission and reception as well as the state transitions of the board. The "no" form of this command turns off the DEBUG display.	
Example	Open devsm and send the message information. Switch# debug devsm send	

force runcfg-sync

Command	force runcfg-sync	
Parameter	-	
Default	-	
Mode	Admin mode	
Usage Guide	When running-config is different from startup-config, this command can be used to synchronize the running-config from the active master to the standby master. In this way, when the master-slave switch occurs, the new running-config will be used as the configuration recovery information.	
Example	Force the synchronization of the "running-config" from the "active master" to the "standby master". Switch# force runcfg-sync	

force switchover

Command	force switchover
Parameter	-
Default	-
Mode	Admin mode
Usage Guide	When a standby master exists, executing this command on the active master will trigger a master-slave switch. The original standby master will then become the new active master.
Example	Forcefully require the active master to switch to the standby master. Switch# force switchover

reset slot

Command	reset member <NUM> slot <WORD>	
Parameter	<NUM>	<1-8> Member ID
	<WORD>	Slot number, such as 1,2,3...M1,M2
Default	-	
Mode	Admin mode	
Usage Guide	Resets the specified slot on a designated member switch in a VSF stack. The member parameter specifies the member ID, and the slot parameter specifies the slot number to reset.	
Example	Reset the designated board card. Switch# reset member 1 slot 3	

runcfg-sync

Command	runcfg-sync [<interval>]	
Parameter	interval	For the synchronization interval, the unit is minutes, and the range of values is 5 to 1440 or 0; 0 indicates that the automatic synchronization function is turned off; if no parameters are added, it means that the running-config synchronization function is enabled. When the configuration file changes, the default synchronization interval is 5 minutes.
Default	-	
Mode	Global Mode	
Usage Guide	This command configures the time interval at which the active master synchronizes the running-config with the standby master. If the synchronization time is set too short, it will impose unnecessary burden on the switch. If the configuration does not change frequently or is saved by the write command after being changed, it is recommended to disable the automatic synchronization function.	
Example	Set the synchronization interval for the running-config to 1440 minutes. Switch(config)#runcfg-sync 1440	

show slot

Command	show slot [<slotno>]	
Parameter	slotno	For the slot number where the board card is located, the value range for 4-slot equipment is 1 to 4, and for 8-slot equipment, it is 1 to 8
Default	If the "slotno" is not specified, the default setting is to list all the board card information.	
Mode	vsc mode	
Usage Guide	Display the basic information of each board card.	
Example	Switch#show slot 3 -----Slot : 3----- Inserted: YES Module type: MS700-4XS16GX8GB Work mode: SLAVE 956	

Work state:	RUNNING
Local software version:	5.5.34.0
Hardware version:	1.0
Bootrom version:	2.1.3
Serial number:	n063500215
Manufacture date:	2006/08/23
Temperature:	43C/109F

17-Evpn vxlan+Mlag+Esi

1 Commands for Basic Configuration

address-family l2vpn evpn

Command	address-family l2vpn evpn no address-family l2vpn evpn
Paramrter	none none
Default	–
Mode	config-router mode
Usage Guide	This command is used to enable the L2VPN EVPN address family in BGP, thereby realizing the routing exchange function of the VXLAN control plane. This command needs to be entered in the "router bgp <AS number>" view and then the address family configuration mode. Within the address family sub-view, activate the routing exchange capability of the EVPN neighbor by using the command "neighbor <IP> activate". Before configuration, a BGP neighbor relationship must be established by using the command "neighbor <IP> remote-as <AS number>". The command "no address-family l2vpn evpn" is used to delete the entire EVPN address family configuration.
Example	Switch #configure terminal Switch (config)# router bgp 200 Switch (config-router)# address-family l2vpn evpn

arp-cache disable

Command	arp-cache disable no arp-cache disable
Paramrter	none none
Default	–
Mode	config-nvo-acc-if mode
Usage Guide	This command is used to disable the ARP cache function of the specified interface.

	After execution, the interface stops dynamically learning and storing the IP-MAC mapping. The "no arp-cache disable" command can be used to re-enable the ARP cache.
Example	Switch #configure terminal Switch (config)#nvo vxlan access-if port-vlan e1/0/10 2 Switch (config-nvo-acc-if)#arp-cache disable Switch (config-nvo-acc-if)#exit

arp-nd flood-suppress

Command	arp-nd flood-suppress no arp-nd flood-suppress
Paramrter	none none
Default	–
Mode	config-nvo-acc-if mode
Usage Guide	Flood suppresses ARP and ND packets. After enabling, the device will act as a proxy to respond to ARP/ND requests, reducing broadcast flooding. The "no" command can disable this function.
Example	Switch #configure terminal Switch (config)#nvo vxlan access-if port-vlan e1/0/10 2 Switch (config-nvo-acc-if)#arp-nd flood-suppress Switch (config-nvo-acc-if)#exit

arp proxy-send enable

Command	arp proxy-send enable no arp proxy-send
Paramrter	none none
Default	–

Mode	config-irb-if mode
Usage Guide	This command is used to enable ARP request proxy sending on the VXLAN interface.
Example	Switch #configure terminal Switch (config)#interface irb 1001 Switch (config-irb-if)# arp proxy-send enable

clear nvo vxlan mac-table dynamic

Command	clear nvo vxlan mac-table dynamic	
Paramrter	none	none
	vnid <1-16777215>	vnid number
	vnid<1-16777215> mac MAC_ADDR	vnid number and mac address
Default	-	
Mode	Exec mode	
Usage Guide	This command is used to clear the dynamic MAC address entries in the VXLAN table. clear nvo vxlan mac-table dynamic : Clear all dynamic table entries. clear nvo vxlan mac-table dynamic vnid<1-16777215>: Clear all dynamic MAC entries for the specified VNID. clear nvo vxlan mac-table dynamic vnid<1-16777215> mac <MAC_ADDR>: After clearing the specified VNID and MAC, the system will enable the VXLAN access function on this interface, allowing connection to the terminal hosts.	
Example	Switch # clear nvo vxlan mac-table dynamic Switch # clear nvo vxlan mac-table dynamic vnid 5000 Switch # clear nvo vxlan mac-table dynamic vnid 8000 mac 00:1A:2B:3C:4D:5E	

evpn irb-forwarding anycast-gateway-mac

Command	evpn irb-forwarding anycast-gateway-mac XXXX.XXXX.XXXX no evpn irb-forwarding anycast-gateway-mac

Paramrter	XX-XX-XX-XX-XX-XX	Source MAC Address (Option One)
	XX:XX:XX:XX:XX:XX	Source MAC Address (Option Two)
	XXXX.XXXX.XXXX	Source MAC Address (Option Three)
Default	-	
Mode	Config mode	
Usage Guide	This command is used to configure the multicast gateway MAC address for global IRB forwarding. The parameter MAC_ADDR specifies the MAC address of the multicast gateway (format: 00:11:22:33:44:55). This command needs to be executed in the global configuration mode. After the configuration, the system will use the specified multicast MAC address to handle the forwarding traffic of all IRB interfaces. The MAC address must conform to the standard format and be globally unique.	
Example	<pre>Switch #configure terminal Switch (config)#evpn irb-forwarding anycast-gateway-mac 0000.0000.1313 Or Switch (config)#evpn irb-forwarding anycast-gateway-mac 00:00:00:00:13:13 Or Switch (config)#evpn irb-forwarding anycast-gateway-mac 00-00-00-00-13-13 Switch (config)# no evpn irb-forwarding anycast-gateway-mac</pre>	

evpn NAME

Command	evpn NAME no evpn NAME	
Paramrter	NAME	The name of the IRB interface to be associated
Default	-	
Mode	config-nvo mode	
Usage Guide	This command is used to create an Ethernet Virtual Private Network (EVPN) instance and associate it with the specified IRB (Integrated Routing Bridge) interface. The parameter NAME specifies the name of the IRB interface to be associated (such as irb100). This command needs to be executed in the EVPN configuration view. Before execution, the corresponding IRB interface must be pre-created through the command "interface irb<ID>".	

	If the specified IRB interface does not exist, the command will fail to execute and return an error message.
Example	Switch #configure terminal Switch (config)# nvo vxlan id 36 ingress-replication Switch (config-nvo)# evpn irb100

evpn-vlan-service

Command	evpn-vlan-service vlan-based
Paramrter	vlan-based Base mode
Default	-
Mode	config-vrf mode
Usage Guide	This command is used to enable the vlan-base mode.
Example	Switch (config)#mac vrf vrf1 Switch (config-vrf)# evpn-vlan-service vlan-based Switch (config-vrf)# no evpn-vlan-service vlan-based

interface irb

Command	interface irb<1-4094> no interface irb<1-4094>
Paramrter	<1-4094> IRB interface number
Default	-
Mode	Config mode
Usage Guide	This command is used to create or enter the configuration mode of the IRB (Integrated Routing and Bridging) interface. Parameter <1-4094> specifies the number of the IRB interface (range 1-4094).

	After executing the command, the system will automatically create the corresponding IRB interface (if it does not exist) and enter the interface configuration view. In the IRB interface view, you can configure EVPN-related functions (such as broadcast gateway, ARP proxy, etc.).
Example	<pre>Switch #configure terminal Switch (config)#interface irb1 Switch (config)#no interface irb1</pre>

Local-proxy-arp enable

Command	local-proxy-arp enable
Paramrter	none none
Default	-
Mode	config-irb-if mode
Usage Guide	Enable the local agent under the IRB interface view.
Example	<pre>Switch #configure terminal Switch (config)# interface irb1 Switch (config-irb-if)# local-proxy-arp enable</pre>

l3vni

Command	l3vni <L3 VNID> no l3vni <L3 VNID>
Paramrter	<1-16777215> L3 VNID cannot be the same as L2 VNID
Default	-
Mode	config-vrf mode
Usage Guide	This command is used to configure the L3 virtual network identifier (VNI) to achieve the

	three-layer routing function of VXLAN. Parameter <1-16777215> specifies the L3 VNI value. It is necessary to ensure that it is different from the already configured L2 VNI. This command needs to be executed in the VRF configuration view (the VRF must be created beforehand). If the specified VRF does not exist, or the VNI value conflicts with the existing L2 VNI, the command will fail to execute and return an error message.

Example	<pre>Switch #configure terminal Switch (config)#ip vrf l3vrf Switch (config-vrf)#l3vni 1002 Switch (config-vrf)#no l3vni 1002</pre>

mac

Command	mac MAC_ADDR mac MAC_ADDR ip A.B.C.D no mac MAC_ADDR no mac MAC_ADDR ip A.B.C.D				
Paramrter	<table> <tr> <td>MAC_ADDR</td><td>MAC address: xxxx.xxxx.xxxx</td></tr> <tr> <td>A.B.C.D</td><td>IP address</td></tr> </table>	MAC_ADDR	MAC address: xxxx.xxxx.xxxx	A.B.C.D	IP address
MAC_ADDR	MAC address: xxxx.xxxx.xxxx				
A.B.C.D	IP address				
Default	-				
Mode	config-nvo-acc-if mode				
Usage Guide	Support two configuration modes: For adding static MAC address table entries Adding static MAC address entries and binding IP addresses The "no" command deletes the added MAC addresses				
Example	<pre>Switch #configure terminal Switch (config)# nvo vxlan access-if port-vlan e1/0/10 10 Switch (config-nvo-acc-if)#mac 2222.2222.2222 Switch (config-nvo-acc-if)#mac 2222.2222.3333 ip 1.1.1.1 Switch (config-nvo-acc-if)# no mac 2222.2222.2222 Switch (config-nvo-acc-if)# no mac 2222.2222.3333 ip 1.1.1.1</pre>				

mac vrf

Command	mac vrf WORD no mac vrf WORD	
Paramrter	WORD	VRF instance name
Default	-	
Mode	Config mode	
Usage Guide	Commands used to create or delete MAC VRF (Virtual Routing and Forwarding Instance) on network devices that support EVPN.	
Example	Switch #configure terminal Switch (config)#mac vrf vrf1 Switch (config)#no mac vrf vrf1	

map vnid

Command	map vnid <1-16777215> map vnid <1-16777215> track WORD no map vnid <1-16777215>	
Paramrter	<1-16777215>	VNID number
	WORD	Tracking item identifier
Default	-	
Mode	config-nvo-acc-if mode	
Usage Guide	This command is used to map the access port attributes to the specified VXLAN network identifier (VNI). After execution, the traffic of the current sub-interface will be associated with the specified VNI. The no command can be used to remove this mapping relationship. For map vnid <1-16777215> track WORD, the AC interface is associated with the NVO service and also with the track instance.	
Example	Switch #configure terminal Switch (config)#nvo vxlan access-if port-vlan e1/0/10 2	

	Switch (config-nvo-acc-if)# map vnid 100
	Switch (config-nvo-acc-if)# map vnid 20 track 2
	Switch (config-nvo-acc-if)# no map vnid 100
	Switch (config-nvo-acc-if)# no map vnid 20
	Switch (config-nvo-acc-if)#exit

nvo vxlan access-if

Command	nvo vxlan access-if (port IFNAME (port-vlan IFNAME <1-4094>)) no nvo vxlan access-if (port IFNAME (port-vlan IFNAME <1-4094>))	
Paramrter	port IFNAME Specify the interface name port-vlanI FNAME<1-4094> Specify the VLAN mapping for the designated interface	
Default	-	
Mode	Config mode	
Usage Guide	Configure the access interface type and associated parameters for VXLAN to define the mapping relationship between the underlying physical interface and the VXLAN tunnel. Configure the ac interface. The "no" command is used to cancel the configuration related to the ac interface.	
Example	Switch #configure terminal Switch (config)#nvo vxlan access-if port-vlan e1/0/10 5 Switch (config)#no nvo vxlan access-if port-vlan e1/0/10 5	

nvo vxlan disable

Command	nvo vxlan disable	
Paramrter	none	none
Default	-	
Mode	Config mode	
Usage Guide	This command disables the VXLAN module.	

Example	Switch #configure terminal Switch (config)#nvo vxlan disable

nvo vxlan enable

Command	nvo vxlan enable
Paramrter	none none
Default	-
Mode	Config mode
Usage Guide	This command is used to enable VXLAN and activate the VXLAN module.
Example	Switch #configure terminal Switch (config)#nvo vxlan enable

nvo vxlan id

Command	nvo vxlan id <1-16777215> (ingress-replication) no nvo vxlan id <1-16777215>
Paramrter	<1-16777215> VNID ingress-replication Enable the Head-End Replication mode
Default	-
Mode	Config mode
Usage Guide	Used to set the VXLAN ID and enable the head-end replication mode. The "no" command cancels the VNID configuration.
Example	Switch #configure terminal Switch (config)#nvo vxlan id 300 ingress-replication Switch (config-nvo)#exit Switch (config)#nvo vxlan id 200

	Switch (config-nvo)#exit
	Switch (config)#no nvo vxlan id 200

nvo vxlan irb

Command	nvo vxlan irb no nvo vxlan irb
Paramrter	none none
Default	-
Mode	Config mode
Usage Guide	Enable IRB Gateway The "no" command disables IRB
Example	Switch #configure terminal Switch (config)#nvo vxlan irb Switch (config)#no nvo vxlan irb

nvo vxlan vtep-ip-global

Command	nvo vxlan vtep-ip-global A.B.C.D no nvo vxlan vtep-ip-global
Paramrter	A.B.C.D IP address
Default	-
Mode	Config mode
Usage Guide	Use this command to set the global configuration of the source VTEP IP address. The "no" command cancels the global configuration of the VTEP IP.
Example	Switch (config)#nvo vxlan vtep-ip-global 10.10.11.1

track WORD evpn peer A.B.C.D

Command	track WORD evpn peer A.B.C.D no track WORD evpn peer	
Parameter	WORD	Tracking item identifier
	A.B.C.D	Source IP address
Default	-	
Mode	Config mode	
Usage Guide	Create a track instance to trigger the creation of BFD painting detection for EVPN peers Real-time monitor the route reachability to the BGP neighbor A.B.C.D	
Example	Switch (config)# track 2 evpn peer 20,1,1.1	

vxlan host-reachability-protocol evpn-bgp NAME

Command	vxlan host-reachability-protocol evpn-bgp NAME	
Parameter	NAME	VRF instance name
Default	-	
Mode	config-nvo mode	
Usage Guide	This command is used to configure the host reachability protocol of VXLAN as EVPN-BGP and specify the VRF that carries the VMID routes. The parameter NAME is the name of the VRF instance (which needs to be created beforehand). This command must be executed in the VXLAN tenant view where dynamic tunnels have been configured. If the tenant has configured static tunnels , the command will fail (protocol conflict).	
Example	Switch (config)#nvo vxlan id 3 Switch (config-nvo)#vxlan host-reachability-protocol evpn-bgp l2vrf	

vxlan static-entry host-mac

Command	vxlan static-entry host-mac <MAC_ADDR> remote-vtep-ip <A.B.C.D> no vxlan static-entry host-mac <MAC_ADDR> remote-vtep-ip <A.B.C.D>	
Paramrter	<MAC_ADDR>	MAC address
	<A.B.C.D>	IP address
Default	-	
Mode	config-nvo mode	
Usage Guide	This command is used to configure the static FDB entry of VXLAN, specifying the remote VTEP IP of the target MAC address. Command format: vxlan static-entry host-mac <MAC_ADDR> remote-vtep-ip <A.B.C.D> <MAC_ADDR>: The MAC address of the target host (format: 00:11:22:33:44:55) <A.B.C.D>: The unicast IP address of the target VTEP This command must be executed in the tenant view that is configured as VXLAN mode. If the tenant mode is not VXLAN, the command will fail to execute and return an error message.	
Example	<pre>Switch #configure terminal Switch (config)# nvo vxlan id 37 ingress-replication Switch(config-nvo)#vxlan static-entry host-mac 00:1A:2B:3C:4D:5E remote-vtep-ip 10.100.200.1</pre>	

2.Commands for Show

show evpn l3vni-map

Command	show evpn l3vni-map
Paramrter	none none
Default	-
Mode	All mode
Usage Guide	Display the mapping relationship between L3 VNI (used for cross-subnet routing) and L2 VNI (used for Layer 2 forwarding) in the EVPN network
Example	Display the connections related to l3vni, l2vni and irb. Switch (config)#show evpn l3vni-map

show evpn track

Command	show evpn track show evpn track WORD
Paramrter	none none WORD Tracking item identifier
Default	-
Mode	All mode
Usage Guide	Check the status of the EVPN track instance
Example	Switch (config)# show evpn track Switch (config)# show evpn track 2

show interface irb

Command	show interface irb <1-4094>
Paramrter	<1-4094> IRB parameter interface number

Default	-
Mode	All mode
Usage Guide	The command used to display the configuration information of the IRB (Integrated Routing and Bridging) interface
Example	<pre>Switch #show interface irb1</pre>

show nvo vxlan

Command	<pre>show nvo vxlan show nvo vxlan vni-name WORD show nvo vxlan vnid <1-16777215></pre>				
Paramrter	<table> <tr> <td>vni-name WORD</td><td>VNI Name</td></tr> <tr> <td>vnid <1-16777215></td><td>vnid</td></tr> </table>	vni-name WORD	VNI Name	vnid <1-16777215>	vnid
vni-name WORD	VNI Name				
vnid <1-16777215>	vnid				
Default	-				
Mode	All mode				
Usage Guide	Display the configuration and status information of the VXLAN network, supporting filtering queries by VNI number (vnid) or VNI name, and used for verifying the configuration validity of the VXLAN overlay network.				
Example	Query the configuration and status of the VXLAN network. <pre>Switch (config)# show nvo vxlan Switch (config)# show nvo vxlan vnid 37</pre>				

show nvo vxlan access-if brief

Command	<pre>show nvo vxlan access-if brief show nvo vxlan access-if brief (vnid <1-16777215>)</pre>		
Paramrter	<table> <tr> <td>(vnid <1-16777215>)</td><td>Specify the VNI interface entrance</td></tr> </table>	(vnid <1-16777215>)	Specify the VNI interface entrance
(vnid <1-16777215>)	Specify the VNI interface entrance		

Default	-
Mode	All mode
Usage Guide	This command is used to display the status and configuration summary of the VXLAN access interface.
Example	Display all configuration information. Display configuration information related to vnid 37. Switch (config)# show nvo vxlan access-if brief Switch (config)# show nvo vxlan access-if brief vnid 37

show nvo vxlan access-if-config

Command	show nvo vxlan access-if-config ((LINE) (vnid <1-16777215>))	
Paramrter	LINE	Optional parameter starting marker
	vnid <1-16777215>	Optional VNID filtering parameters
Default	-	
Mode	All mode	
Usage Guide	Display detailed configuration information of the VXLAN access interface, including MAC/IP mapping relationship and VNID (VXLAN Network Identifier) binding status. Support filtering by VNID.	
Example	Display the configuration information related to the physical interface. Display the configuration information related to Vnid 37. Switch (config)# show nvo vxlan access-if-config e1/0/40 Switch (config-nvo)#show nvo vxlan access-if-config vnid 37	

show nvo vxlan arp-cache

Command	show nvo vxlan arp-cache show nvo vxlan arp-cache summary

	show nvo vxlan arp-cache vnid <1-16777215>	
Paramrter	summary	Display statistical count
	vnid <1-16777215>	Optional VNID filtering parameters
Default	-	
Mode	All mode	
Usage Guide	Display the ARP cache table entries in the VXLAN network, supporting filtering by VNID (VXLAN Network Identifier) and outputting in statistical mode.	
Example	Display VXLAN-related ARP cache table entries. Display statistics of the number of VXLAN-related ARP cache table entries. Display ARP cache table entries related to VNID 37. Switch (config)# show nvo vxlan arp-cache Switch (config)# show nvo vxlan arp-cache summary Switch (config)# show nvo vxlan arp-cache vnid 37	

show nvo vxlan dynamic-tunnel

Command	show nvo vxlan dynamic-tunnel show nvo vxlan dynamic-tunnel summary	
Paramrter	summary	Statistical figures
Default	-	
Mode	All mode	
Usage Guide	Display the number information of dynamic tunnel status.	
Example	The switch displays dynamic tunnel-related information. Switch (config)# show nvo vxlan dynamic-tunnel	

show nvo vxlan fdb-entry

Command	show nvo vxlan fdb-entry	
Paramrter	none	none
Default	-	
Mode	All mode	
Usage Guide	Used to display the FDB table entries of the VXLAN network, including MAC addresses, VTEP mappings, etc.	
Example	Display VXLAN-related information. Switch (config)# show nvo vxlan fdb-entry	

show nvo vxlan mac-table

Command	show nvo vxlan mac-table show nvo vxlan mac-table summary show nvo vxlan mac-table vnid <1-16777215> show nvo vxlan mac-table hardware summary show nvo vxlan mac-table hardware vnid <1-16777215>	
Paramrter	summary	Display statistical count
	vnid	Filter display by VNID
	hardware summary	Hardware statistical count
	hardware vnid	Hardware-related VNID
Default	-	
Mode	All mode	
Usage Guide	Display the MAC address table of the VXLAN network, supporting three modes: hardware table item query, VNID filtering and statistical summary.	
Example	Display the MAC address table entries of the VXLAN network. Switch (config)# show nvo vxlan mac-table Switch (config)# show nvo vxlan mac-table hardware	

show nvo vxlan static host

Command	show nvo vxlan static host state	
Paramrter	none	none
Default	-	
Mode	All mode	
Usage Guide	Display the status information of the static host.	
Example	Switch (config)# show nvo vxlan static host state	

show nvo vxlan vlan-vnid

Command	show nvo vxlan vlan-vnid show nvo vxlan vlan-vnid summary show nvo vxlan vlan-vnid vnid <1-16777215> how nvo vxlan vlan-vnid bridge-vlan <2-2094>	
Paramrter	summary	Display the statistical quantity
	vnid <1-16777215>	Filter the mapping vnid of the specified VXLAN network
	bridge-vlan<2-2094>	Range supported for Bridge-VLAN
Default	-	
Mode	All mode	
Usage Guide	Display the mapping relationship between VLAN and VXLAN network identifiers (VNI), and support filtering or displaying statistical summaries based on VNI.	
Example	Switch (config)# show nvo vxlan vlan-vnid Switch (config)# show nvo vxlan vlan-vnid summary Switch (config)# show nvo vxlan vlan-vnid vnid 37	

Switch (config)# show nvo vxlan vlan-vnid bridge-vlan 2

show running-config interface irb

Command	show running-config interface irb	
Paramrter	<1-4094>	IRB interface number
Default	-	
Mode	All mode	
Usage Guide	This command is used to query the configuration information of IRB.	
Example	Switch # show running-config interface irb1001	

show running-config nvo vxlan

Command	show running-config nvo vxlan	
Paramrter	none	none
Default	-	
Mode	All mode	
Usage Guide	Display the relevant configuration information of nvo vxlan on the switch.	
Example	Switch (config)# show running-config nvo vxlan	

show running-config track

Command	show running-config track

Paramrter	none none
Default	-
Mode	All mode
Usage Guide	Check the track configuration
Example	Switch (config)# show running-config track

3.Commands for Mclag

Authentication

command	authentication type hmac-sha256 key WORD no authentication
parameter	WORD Configured authentication key, character length range [1-32]
Default	Not configured by default
mode	DOMAIN_MODE
Usage Guide	This command is used to configure the neighbor connection hmac-sha256 authentication function of the MELAG of the switch. The no authentication command is used to disable the authentication function.
Example	Enable the MLAG authentication function using the HMAC-SHA256 encryption algorithm on the switch Switch(config)domain 1 Switch(domain-if-1)#authentication type hmac-sha256 key 123456

connection timer

command	connection-timeout timer <10-300> no connection-timeout timer
parameter	<10-300> Mlag connection timeout duration (10-300).
Default	The default value is 30
mode	DOMAIN_MODE
Usage Guide	This command is used to specify the timeout timer duration for mlag peer-link connect to peer after the mlag binding is finished. The no connection-timeout timer command is used to restore the connection timeout timer, and the duration value is set to the default value of 30.
Example	Configure the duration of the mlag connection timeout timer on the switch Switch(config)#domain 1 Switch(domain-if-1)# connection-timeout timer 60

dad ip vrf

command	dad ip vrf WORD no dad ip vrf
parameter	WORD The IP VRF name that DAD wants to bind
Default	It is not bound by default
mode	DOMAIN_MODE
Usage Guide	This command is used to configure the DAD link IP VRF of the mlag domain of the switch. The no dad ip vrf command is used to delete the DAD link IP VRF of the mlag domain of the switch.
Example	The switch configure the DAD link IP VRF of the mlag domain Switch(domain-if-1)#dad ip vrf mgmt Switch(domain-if-1)#no dad ip vrf

dad keepalive-interval timer

Command	dad keepalive-interval timer ms <100-1000>	
Paramrter	<100-1000>	The value of the timer
Default	-	
Mode	domain-if mode	
Usage Guide	Adjust the sending interval of the keepalive message for MLAG dual-master detection (DAD), and optimize the sensitivity of detecting abnormality of the opposite device. The shorter the interval, the faster the fault detection, but it will consume more bandwidth.	
Example	Switch (config)# domain 1 Switch (domain-if-1)# dad keepalive-interval timer ms 100	

dad link

Command	dad link (udp tcp ...) no dad link	
Paramrter	udp	UDP protocal
	tcp	TCP protocal
	none	UDP protocal
Default	-	
Mode	domain-if mode	
Usage Guide	Enable dual-master detection with mclag and enable link-layer (Link-local) address conflict detection. The "No" command cancels the detection.	
Example	Switch (config)#domain 1 Switch (domain-if-1)# dad link udp Switch (domain-if-1)#no dad link	

dad local

Command	dad local A.B.C.D peer A.B.C.D no dad local A.B.C.D peer A.B.C.D
Paramrter	A.B.C.D ip address
Default	–
Mode	domain-if mode
Usage Guide	Specify the local IP and the remote IP for DAD detection to prevent IP conflicts. The "No" command cancels the configuration detection between the two ends.
Example	Switch (config)#domain 1 Switch (domain-if-1)# dad link Switch (domain-if-1)# dad local 192.168.13.11 peer 192.168.13.12 Switch (domain-if-1)#no dad local 192.168.13.11 peer 192.168.13.12

dad session-timeout timer ms

Command	dad session-timeout timer ms <3000-60000>
Paramrter	<3000-60000> Time value
Default	-
Mode	domain-if mode
Usage Guide	Set the timeout duration for dual-master detection sessions (the maximum waiting time for keeping alive). Long-latency links need to extend the timeout to prevent accidental disconnection. Harsh environments require rapid fault switching (set a low value).
Example	Switch (config)# domain 1 Switch (domain-if-1)# dad session-timeout timer ms 3000

delay-restore timer

Command	delay-restore timer <0-300> no delay-restore timer
Paramrter	<0-300> Timer time range: <0 - 300>
Default	Default: 0 seconds
Mode	domain-if mode
Usage Guide	Disable link recovery delay (default is 0 seconds). Enable the port immediately after the fault is repaired to avoid frequent switching due to jitter. The "no" command is used to cancel the configuration.
Example	Switch (config)#domain 1 Switch (domain-if-1)#delay-restore timer 0 Switch (domain-if-1)#no delay-restore timer

domain

Command	domain <1-24> no domain <1-24>
Paramrter	<1-24> Threshold value, range < 1 - 24 >
Default	-
Mode	Config mode
Usage Guide	Define a redundant domain (with Domain ID 1) for logical isolation of the redundant group. The "no" command cancels the redundant domain.
Example	Switch (config)# domain 1 Switch (config)# no domain 1

ip vrf

command	ip vrf WORD no ip vrf
parameter	WORD The IP VRF name that MCLAG wants to bind
Default	It is not bound by default
mode	DOMAIN_MODE
Usage Guide	This command is used to configure the peer link IP VRF of the mclag domain of the switch. The no ip vrf command is used to delete the peer link IP VRF of the mclag domain of the switch.
Example	The switch configure the peer link IP VRF of the mclag domain Switch(domain-if-1)#ip vrf mgmt Switch(domain-if-1)#no ip vrf

Keepalive

command	keepalive-interval timer <1-2>
parameter	<1-2> The value of the timer (1-2)
Default	The default value is 1
mode	DOMAIN_MODE
Usage Guide	This command is used to configure the time interval at which keepalive packets are sent peer_link link.
Example	Interval of keepalive packets on the switch Switch(config)#domain 1 Switch(domain 1)#keepalive-interval timer 2

nvo vxlan mlag-vip-global

Command	nvo vxlan mlag-vip-global A.B.C.D no nvo vxlan mlag-vip-global
Parameter	A.B.C.D Source IP address
Default	-
Mode	Config mode
Usage Guide	Global configuration for the MLAG IP address. The "no" command cancels the global configuration of the MLAG address.
Example	Switch (config)# nvo vxlan mlag-vip-global 10.10.11.1 Switch (config)# no nvo vxlan mlag-vip-global

orphan-port ethernet-port

command	orphan-port ethernet-port<1-56> no orphan-port ethernet-port<1-56>
parameter	<1-56> Physical port id value range (1-56)
Default	The MLAG orphan physical port is not configured by default
mode	DOMAIN_MODE
Usage Guide	This command is used to configure the orphan physical port of the MCLAG domain. The no orphan-port ethernet <1-56> command is used to delete the orphan physical port of the mclag domain. Currently, multiple orphan physical port can be configured.
Example	Add orphan physical port of the MCLAG domain to the switch Switch(domain-if-1)# orphan-port ethernet-port 10 Delete orphan physical port of the MCLAG domain from the switch Switch(domain-if-1)# no orphan-port ethernet-port 10

orphan-port port-channel

command	orphan-port port-channel <1-127> no orphan-port port-channel <1-127>
parameter	<1-127> Agg-group port id value range (1-127)
Default	The MLAG orphan agg-group port is not configured by default
mode	DOMAIN_MODE
Usage Guide	This command is used to configure the orphan agg-group port of the MCLAG domain. The no orphan-port port-channel <1-127> command is used to delete the orphan agg-group port of the mclag domain. Currently, multiple orphan agg-group port can be configured.
Example	Add orphan agg-group port of the MCLAG domain to the switch Switch(domain-if-1)# orphan-port port-channel 10 Delete orphan agg-group port of the MCLAG domain from the switch Switch(domain-if-1)# no orphan-port port-channel 10

port-channel

Command	port-channel IFNAME no port-channel IFNAME
Paramrter	IFNAME <1-16> Member Interface
Default	-
Mode	domain-if mode
Usage Guide	Add member interfaces from the mclag domain. The "no" command cancels the added member interfaces.
Example	Switch (config)#port-group 2 Switch (config)#domain 1 Switch (domain-if-1)# port-channel 2 Switch (domain-if-1)#no port-channel 2

priority

Command	priority <0-65535> no priority	
Paramrter	<0-65535>	Priority value
Default	-	
Mode	domain-if mode	
Usage Guide	Set the priority of the devices (the higher the number, the higher the priority to become the main device)	
Example	Switch (config)# domain 1 Switch (domain-if-1)#priority 1	

role swap

Command	role swap	
Paramrter	none	none
Default	-	
Mode	domain-if mode	
Usage Guide	To force the primary and backup roles to switch, it is necessary to perform the operation in the domain configuration mode of the Primary device. There will be a brief interruption of traffic (at the millisecond level), and the data plane will be seamlessly migrated.	
Example	Switch (config)# domain 1 Switch (domain-if-1)# role swap	

session timeout

command	session-timeout timer <3-60>
parameter	<3-60> Timeout Indicator (3-60)
Default	The default value is 6
mode	DOMAIN_MODE
Usage Guide	This command is used to specify the timeout period for sending keepalive packets peer_link link.
Example	The switch configures the timeout period Switch(config)#domain 1 Switch(domain 1)#session-timeout timer 15

show mclag-arp domain

Command	show mclag-arp domain <1-24>
Paramrter	<1-24> Threshold value, range < 1 - 24 >
Default	-
Mode	All mode
Usage Guide	Query the ARP table information of the specified MCLAG domain (Domain).
Example	Switch (config)# show mclag-arp domain 1

show mclag configuration

Command	show mclag configuration
Paramrter	none none
Default	-

Mode	All mode
Usage Guide	Display MCLAG related configuration information.
Example	Switch (config)# show mclag configuration

show mclag-mac domain

Command	show mclag-mac domain <1-24>
Paramrter	<1-24> Threshold value, range < 1 - 24 >
Default	-
Mode	All mode
Usage Guide	Query the MAC table information of the specified MCLAG domain (Domain).
Example	Switch (config)# show mclag-mac domain 1

show mclag-state domain

Command	show mclag-state domain <1-24>
Paramrter	<1-24> Domain ID value
Default	-
Mode	All mode
Usage Guide	Diagnose the health status of the MCLAG domain (control plane synchronization/fault detection).
Example	Switch (config)# show mclag-state domain 1

source A.B.C.D peer A.B.C.D interface port-channel WORD

Command	source A.B.C.D peer A.B.C.D interface port-channel WORD	
Paramrter	A.B.C.D	Manually set the IP address of the backup device
	WORD	Interface name
Default	-	
Mode	domain-if mode	
Usage Guide	Configure the source IP, peer IP, aggregated interface for communication between MLAG peers. The Peer IP must not be the gateway address. It should be directly connected or reachable via routing.	
Example	Switch (config)# domain 1 Switch (domain-if-1)# source 192.168.10.12 peer 192.168.10.11 interface port-channel 1	

vxlan mlag-virtual-mac

Command	vxlan mlag-virtual-mac XXXX.XXXX.XXXX no vxlan mlag-virtual-mac	
Paramrter	XXXX.XXXX.XXXX	Source MAC address
Default	-	
Mode	Config mode	
Usage Guide	Set the same static MAC address on both ends of the MLAG devices, and associate this virtual MAC address with the corresponding MLAG domain configuration.	
Example	Switch (config)# vxlan mlag-virtual-mac 1010.1011.1011.1000	

4.Commands for ESI

evpn esi hold-time

Command	evpn esi hold-time <10-300> no evpn esi hold-time	
Paramrter	<10-300>	Time threshold, measured in seconds
Default	-	
Mode	Config mode	
Usage Guide	This command is used to set the time setting that ESI can reserve before enabling EVPN. The "No" command cancels the configuration.	
Example	Switch (config)# evpn esi hold-time 10 Switch (config)# no evpn esi hold-time	

evpn multi-homed esi

Command	evpn multi-homed esi XX:XX:XX:XX:XX:XX:XX:XX no evpn multi-homed esi	
Paramrter	XX:XX:XX:XX:XX:XX:XX:XX	ESI value
Default	-	
Mode	config-if-ethernet mode	
Usage Guide	Set the ESI value for the AC port.	
Example	Switch (config)# interface ethernet 1/0/1 Switch (config-if-ethernet1/0/1)#evpn multi-homed esi 01:01:01:01:01:01:01:01 Switch (config-if-ethernet1/0/1)#no evpn multi-homed esi	

evpn vxlan multihoming enable

Command	evpn vxlan multihoming enable no evpn vxlan multihoming enable	
Paramrter	none	none
Default	-	
Mode	Config mode	
Usage Guide	Global enablement of EVPN VXLAN multi-homing.	
Example	Switch (config)# evpn vxlan multihoming enable Switch (config)# no evpn vxlan multihoming enable	

show bgp l2vpn evpn esi-vni-hash

Command	show bgp l2vpn evpn esi-vni-hash	
Paramrter	none	none
Default	-	
Mode	All mode	
Usage Guide	Show the hash calculation process and results used for DF election within the BGP process.	
Example	Switch (config)# show bgp l2vpn evpn esi-vni-hash	

show bgp l2vpn evpn route-type es-route

Command	show bgp l2vpn evpn route-type es-route show bgp l2vpn evpn route-type es-route vrf WORD show bgp l2vpn evpn route-type es-route rd WORD	

Paramrter	vrf WORD Routing forwarding instance name rd WORD The value of the routing discriminator, in the format of ASN:nn or IP:nn
Default	-
Mode	All mode
Usage Guide	Display detailed information about Type 4 routes related to multi-homing Ethernet segments (Ethernet Segment, ES) in the BGP EVPN (Ethernet VPN) network. This command is used to check and diagnose the control plane status of the EVPN multi-homing environment.
Example	Switch (config)# show bgp l2vpn evpn route-type es-route Switch (config)# show bgp l2vpn evpn route-type es-route vrf l3vrf Switch (config)# show bgp l2vpn evpn route-type es-route rd 10: 11

show bgp l2vpn evpn route-type ethernet-ad-per-es

Command	show bgp l2vpn evpn route-type ethernet-ad-per-es rd WORD show bgp l2vpn evpn route-type ethernet-ad-per-es vrf WORD
Paramrter	rd WORD The value of the routing discriminator is in the format of ASN:nn or IP:nn vrf WORD Routing forwarding instance name
Default	-
Mode	All mode
Usage Guide	Display detailed information for Ethernet AD per ES routes (type: 1). RD: By RD classification, display all Ethernet A-D per-ES routes generated and sent by this device, as well as those learned from other BGP EVPN peers. VRF: Display the status of Ethernet A-D per-ES routes associated with ES within each VRF instance, especially the DF election results.
Example	Switch (config)# show bgp l2vpn evpn route-type ethernet-ad-per-es rd 20:20 Switch (config)# show bgp l2vpn evpn route-type ethernet-ad-per-es vrf lvrif

show bgp l2vpn evpn route-type ethernet-ad-per-evi

Command	show bgp l2vpn evpn route-type ethernet-ad-per-evi rd WORD show bgp l2vpn evpn route-type ethernet-ad-per-evi vrf WORD	
Paramrter	rd WORD	The value of the routing discriminator is in the format of ASN:nn or IP:nn.
	vrf WORD	Routing Forwarding Instance Name
Default	-	
Mode	All mode	
Usage Guide	Display detailed information for Ethernet AD per EVI routing (Type: 1). rd: View the detailed sending and receiving status of each EVI Ethernet automatic discovery routing through the routing discriminator, which is used to troubleshoot routing propagation issues; vrf: Focus on the virtual routing forwarding instance, quickly verify whether the redundancy mode of all Ethernet segments within the specified tenant is fully active or single-active, to ensure that the business configuration conforms to the design expectation.	
Example	Switch (config)# show bgp l2vpn evpn route-type ethernet-ad-per-evi rd 20:20 Switch (config)# show bgp l2vpn evpn route-type ethernet-ad-per-evi vrf lvr	

show evpn multi-homing

Command	show evpn multi-homing show evpn multi-homing all show evpn multi-homing esi	
Paramrter	all	Display all information
	esi	Display ESI/PE/MAC-VRF/Tenant information
Default	-	
Mode	All mode	
Usage Guide	This command is used to display detailed information about multiple links.	
Example	Switch (config)# show evpn multi-homing	

```
Switch (config)# show evpn multi-homing all
Switch (config)# show evpn multi-homing esi
```

5.Commands for Evpn Show

show bgp l2vpn evpn

Command	<pre>show bgp l2vpn evpn show bgp l2vpn evpn vrf WORD show bgp l2vpn evpn rd WORD show bgp l2vpn evpn prefix WORD</pre>	
Paramrter	vrf WORD	Routing Forwarding Instance Name
	rd WORD	The value of the routing discriminator is in the format of ASN:nn or IP:nn.
	prefix WORD	Prefix name
Default	-	
Mode	All mode	
Usage Guide	This command is used to display detailed information of BGP EVPN routes, and it supports filtering and customized display through various methods such as VRF name, route discriminator (RD), prefix filtering, etc.	
Example	<pre>Switch (config)# show bgp l2vpn evpn Switch (config)# show bgp l2vpn evpn vrf B Switch (config)# show bgp l2vpn evpn rd 1: 10 Switch (config)# show bgp l2vpn evpn prefix 10.1.1.0</pre>	

show bgp l2vpn evpn detail

Command	<pre>show bgp l2vpn evpn detail</pre>

Paramrter	none none
Default	-
Mode	All mode
Usage Guide	This command is used to display detailed information for each BGP EVPN route.
Example	Switch (config)# show bgp l2vpn evpn detail

show bgp l2vpn evpn irb-vni-hash vrf

Command	show bgp l2vpn evpn irb-vni-hash vrf WORD
Paramrter	WORD Routing Forwarding Instance Name
Default	-
Mode	All mode
Usage Guide	Show how the BGP process calculates hash values for known unicast traffic within the specified VRF (tenant) to determine the selection among multiple equivalent paths.
Example	Switch (config)# show bgp l2vpn evpn irb-vni-hash vrf abc

show bgp l2vpn evpn peer-group

Command	show bgp l2vpn evpn peer-group WORD
Paramrter	WORD Neighborhood Group Name
Default	-
Mode	All mode

Usage Guide	Display the summary information and detailed status of all peer groups under the BGP EVPN address family.
Example	Switch (config)# show bgp l2vpn evpn peer-group abc

show bgp l2vpn evpn route-type mac-ip

Command	show bgp l2vpn evpn route-type mac-ip rd WORD show bgp l2vpn evpn route-type mac-ip vrf WORD	
Paramrter	rd WORD The value of the routing discriminator is in the format of ASN:nn or IP:nn vrf WORD Routing Forwarding Instance Name	
Default	-	
Mode	All mode	
Usage Guide	Display detailed information of MAC-IP routes (Type: 2) rd: Display detailed information of all MAC/IP published routes under the specified route discriminator (RD). vrf: Display summary information of all MAC/IP published routes under the specified virtual routing forwarding instance (VRF).	
Example	Switch (config)# show bgp l2vpn evpn route-type mac-ip rd WORD Switch (config)# show bgp l2vpn evpn route-type mac-ip vrf WORD	

show bgp l2vpn evpn route-type mcast

Command	show bgp l2vpn evpn route-type mcast	
Paramrter	none	none
Default	-	
Mode	All mode	

Usage Guide	Display detailed information of the Inclusive MULTICAST routing (Type: 3). Display information of all multicast type routes learned in the BGP EVPN control plane.
Example	Switch (config)# show bgp l2vpn evpn route-type mcast

show bgp l2vpn evpn route-type prefix-route

Command	show bgp l2vpn evpn route-type prefix-route rd WORD show bgp l2vpn evpn route-type prefix-route vrf WORD	
Paramrter	rd WORD	The value of the routing discriminator is in the format of ASN:nn or IP:nn.
	vrf WORD	Routing Forwarding Instance Name
Default	-	
Mode	All mode	
Usage Guide	Display detailed information of Prefix-Route (type: 5). rd: Displays detailed information of all IP prefix routes under the specified routing identifier (RD), which is used for diagnosing the announcement and learning of Layer 3 subnets or external introduced routes propagated through Type 5 routes in the EVPN network. vrf: Displays summary information of all IP prefix routes under the specified virtual routing and forwarding instance (VRF), which is used to verify the Layer 3 subnet reachability and routing penetration status across VXLAN within this tenant.	
Example	Switch (config)# show bgp l2vpn evpn route-type prefix-route rd 20:20 Switch (config)# show bgp l2vpn evpn route-type prefix-route vrf abc	

show bgp l2vpn evpn summary

Command	show bgp l2vpn evpn time	
Paramrter	none	none
Default	-	

Mode	All mode
Usage Guide	This command is used to display the summary of BGP EVPN neighbor status.
Example	<pre>Switch (config)# show bgp l2vpn evpn summary</pre>

show bgp l2vpn evpn time

Command	show bgp l2vpn evpn time	
Paramrter	none	none
Default	-	
Mode	All mode	
Usage Guide	This command is used to display the learning time for each BGP EVPN route.	
Example	<pre>Switch (config)# show bgp l2vpn evpn time</pre>	

show bgp l2vpn evpn vni-ipvrf-hash

Command	show bgp l2vpn evpn vni-ipvrf-hash	
Paramrter	none	none
Default	-	
Mode	All mode	
Usage Guide	This command is used to display the BGP EVPN vni-ipvrf-hash table.	
Example	<pre>Switch (config)# show bgp l2vpn evpn vni-ipvrf-hash</pre>	

show bgp l2vpn evpn vni-mac-table

Command	show bgp l2vpn evpn vni-mac-table vrf WORD	
Paramrter	vrf WORD	VPN routing/forwarding instance name
Default	-	
Mode	All mode	
Usage Guide	This command is used to display the BGP EVPN vni-mac-table table.	
Example	Switch (config)# show bgp l2vpn evpn vni-mac-table vrf B	

show bgp l2vpn evpn vni-vrf-hash

Command	show bgp l2vpn evpn vni-vrf-hash	
Paramrter	none	none
Default	-	
Mode	All mode	
Usage Guide	This command is used to display the BGP EVPN vni-vrf-hash table.	
Example	Switch (config)# show bgp l2vpn evpn vni-vrf-hash	

6.Commands for Static Vxlan

tunnel mode vxlan

Command	tunnel mode (vxlan ...) no tunnel mode
Parameter	vxlan Static vxlan tunnel.
Default	-
Mode	Tunnel mode
Usage Guide	You need to first enter the tunnel configuration mode before making any configuration. In this mode, the VXLAN tunnels created are static VXLAN tunnels.
Example	Below is the demonstration of setting the tunnel mode to VXLAN mode. <pre> Switch#config Switch(config)#interface tunnel 1 Switch(config-if-tunnel1)# tunnel mode vxlan Switch(config-if-tunnel1)#show running-config current-mode ! interface Tunnel1 tunnel mode vxlan !</pre>

tunnel map vnid

Command	tunnel map vnid <1-16777215> no tunnel map vnid
Parameter	<1-16777215> VNI ID
Default	-
Mode	Tunnel mode
Usage Guide	Before configuration, nvo vxlan must be enabled first, and a vxlan id needs to be created (when multiple tunnels with the same destination IP but different VNIDs need to be created, VNID creation requires enabling ingress-replication). Also, the tunnel mode needs to be set to vxlan first. After all the src-ip, dst-ip and vnid of the tunnel are configured, the tunnel can be established. Before establishing the tunnel, it is necessary to ensure that the loopback interface with the IP as the src-ip has been created. In this mode, the vxlan tunnel created is a static vxlan tunnel. Multiple VNIDs can be bound to the same tunnel. After the tunnel is established successfully, if you want to modify the tunnel attributes or delete

	the tunnel, you need to first release the binding between the tunnel and the VNID (no tunnel map VNID).
Example	Below is the demonstration of setting the tunnel binding vnid. <pre> Switch#config Switch(config)#nvo vxlan enable Switch(config)#nvo vxlan id 1 Switch(config-nvo)# quit Switch(config)#interface loopback 1 Switch(config)#ip address 1.1.1.1/32 Switch(config-loopback)# quit Switch(config)#interface tunnel 1 Switch(config-if-tunnel1)#tunnel mode vxlan Switch(config-if-tunnel1)#tunnel source 1.1.1.1 Switch(config-if-tunnel1)#tunnel destination 2.2.2.2 Switch(config-if-tunnel1)#tunnel map vnid 1 Switch(config-if-tunnel1)#show running-config current-mode ! interface Tunnel1 tunnel source 1.1.1.1 tunnel destination 2.2.2.2 tunnel mode vxlan tunnel map vnid 1 ! </pre>

show nvo vxlan static-tunnel

Command	show nvo vxlan static-tunnel (<1-200> summary)	
Paramrter	<1-200>	Tunnel interface number (indicating the specific tunnel status)
	summary	Display the overall summary of the tunnel status
	<cr>	Display the status of each tunnel
Default	-	
Mode	Config mode	
Usage Guide	Before use, nvo vxlan needs to be enabled first.	
Example	Below is the demonstration of setting the tunnel binding vnid. <pre> Switch#config Switch(config)#nvo vxlan enable </pre>	

```
Switch(config)# show nvo vxlan static-tunnel 1
Switch(config)# show nvo vxlan static-tunnel summary
Switch(config)# show nvo vxlan static-tunnel
```

18-Commands for MPLS

1 MPLS Configuration

mpls enable

Command	Mpls enable no mpls enable
Parameter	None
Default	By default, the MPLS protocol is enabled
Mode	Global Mode
Usage Guide	This command enables the MPLS protocol
Example	Enable the MPLS protocol function globally. Switch(config)# mpls enable

mpls forward soft

Command	mpls forward soft no mpls forward soft
Parameter	None
Default	By default, it is MPLS hard conversion
Mode	Global Mode
Usage Guide	Configures MPLS forwarding to use software forwarding mode. By default, MPLS uses hardware forwarding mode. The soft mode enables forwarding through software processing. The no form restores the default hardware forwarding mode.
Example	Enable the MPLS protocol function globally. Switch(config)# mpls forward soft

mpls ingress-ttl

Command	Mpls ingress-ttl<0-255> No Mpls ingress-ttl
Parameter	<0-255> TTL value
Default	By default, there is no configuration
Mode	Global Mode
Usage Guide	If Ingress-TTL can be configured in ingress LSR, the ttl value of the top label of the MPLS message stack entering the LSP through the LSP entry router should be set to Ingress-TTL.
Example	Set the value of Ingress TTLd to 45. Switch(config)# mpls ingress-ttl 45

mpls local-packet-handling

Command	mpls local-packet-handling no mpls local-packet-handling
Parameter	None
Default	It is not configured by default.
Mode	Global Mode
Usage Guide	After enabling this Command, all TCP packets will be labeled with MPLS tags.
Example	enabled mpls local-packet-handling Switch(config)#mpls local-packet-handling

show mpls

Command	Show mpls

Parameter	None
Default	Default no configuration
Mode	All Modes
Usage Guide	This Command displays all tag data
Example	Switch(config)#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: 23 Custom egress TTL configured: 33 Log message detail: Debug messages being logged by MPLS Forwarder Debug messages being log by MPLS Hard Drv Admin group detail: none
display content	explain
Minimum label configured	The minimum label value set
Maximum label configured	The maximum label value set
Per label-space information	Information of each tag space
Custom ingress TTL configured	The entry TTL value set by the user
Custom egress TTL configured	The exit TTL value set by the user
Log message detail	Debug information
Label-space 0 is using minimum label xx and maximum label	The minimum and maximum values used in label space 0

show mpls forwarding-table

Command	Show mpls forwarding-table
Parameter	None
Default	None
Mode	All Modes
Usage Guide	Use this command to display all LSP information generated by the left and right ingress switches of the switch, and also to display the FTN with the selected representation.

Example	

show mpls ftn-table brief

Command	Show mpls ftn-table brief														
Parameter	None														
Default	There is no default.														
Mode	All Modes														
Usage Guide	You can use this command to display the summary information of the FTN routes established by MPLS on this switch.														
Example	Switch#show mpls ftn-table brief FTN Entry Brief Information ----- <table><tr><td>FEC</td><td>Out-Label</td><td>Out-intf</td><td>Next hop</td><td>Oper-code</td><td>Op-State</td><td>Vrf</td></tr><tr><td>100.1.1.0/24</td><td>3</td><td>Vlan10</td><td>0.0.0.0</td><td>Push</td><td>Up</td><td>0</td></tr></table>	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
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									

show mpls ftn-tabledetail

Command	show mpls ftn-tabledetail
Parameter	None
Default	There is no default.
Mode	All Modes
Usage Guide	Displays the details of the public FTN routes established by MPLS under this 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

Display content	Explained
FTN ID	FEC ID
VrfIndex	Vrf Index
Fec	Fec Address
Nexthop addr	Next Hop Address
Owner	Cross-Link Table Creation Protocol
Primary	Whether Precedence
Row Status	Active State
Exp-bits	Experimental Bit
Incoming DSCP	Differentiated Services CodePoint.
Tunnel ID	Tunnel ID
Protected LSP id	Protected LSP ID
QoS Resource id	QoS Resource ID
in label	In Tag
In-Interface	In-Interface
Out-Label	Out-Tag
Out-Interface	Out-of-Interface
Admin Status	Management Status
Oper Status	Available Status
Oper Code	Tag Opcode

show mpls ilm-table

Command	show mpls ilm-table
Parameter	[<1-15>] User permission level

Default	There is no default.					
Mode	User Mode/adminMode					
Usage Guide	Use this command to display the ILM routing information established 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
Display content				Explained		
In-Label				Incoming label		
Out-Label				Outgoing label		
In-Intf				Incoming interface		
Out-Intf				Outgoing interface		
Nexthop				next hop address		
FEC				FEC address		

show mpls vrf-table

Command	show mpls vrf-table[vrf-name]
Parameter	None
Default	None
Mode	All Modes
Usage Guide	This command can be used to display the details of all VRF entries that have been configured. If the Parameter indicates the name of the VRF, the details of the VRF entry are displayed.
Example	Switch#show mpls vrf-table Output for VRF table with id: 1 <pre> ----- 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 </pre>

	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
Display content	Explained		
FTN ID	FEC ID		
VrfIndex	Vrf Index		
Fec	Fec Address		
Nexthop addr	Next Hop Address		
Owner	Cross-Link Table Creation Protocol		
Primary	Whether Precedence		
Row Status	Active State		
Exp-bits	Experimental Bit		
Incoming DSCP	Differentiated Services CodePoint.		
Tunnel ID	Tunnel ID		
Protected LSP id	Protected LSP ID		
QoS Resource id	QoS Resource ID		
in label	In Tag		
In-Interface	In-Interface		
Out-Label	Out-Tag		
Out-Interface	Out-of-Interface		
Admin Status	Management Status		
Oper Status	Available Status		
Oper Code	Tag Opcode		

2 Commands for LDP

advertisement-mode

Command	advertisement-mode (downstream-on-demand downstream-unsolicited) no advertisement-mode (downstream-on-demand downstream-unsolicited)	
Parameter	downstream-on-demand	Downstream on-demand mode
	downstream-unsolicited	Downstream active mode
Default	By default, it is downstream active mode.	
Mode	LDP protocol configuration mode	
Usage Guide	LDP Label Distribution Mode is the LDP protocol for label distribution, which provides two modes, one is downstream on demand mode, that is, only the upstream makes a label request, the switch distributes tags for the upstream, otherwise it will not be distributed, and the other is downstream unsolicited, that is, all upstream labels are assigned regardless of whether the upstream needs them or not. It is recommended to use this mode with the label retention mode and LSP control mode, the downstream active corresponds to the free mode in the reserved mode and the independent mode in the control mode, while the downstream corresponds to the conservative mode and the ordered mode on demand. It is not recommended to configure other attributes separately. If the label distribution mode is configured under the interface, the command is invalid. no form is deconfigured.	
Example	Configure the label distribution mode to the downstream active mode. Switch (config)#router ldp Switch (config-router)#advertisement mode downstream on demand	

clear ldp adjacency

Command	clear ldp adjacency (A.B.C.D *)	
Parameter	A.B.C.D	LDP neighbors
	*	All LDP neighbors
Default	None	
Mode	admin Mode	

Usage Guide	Use this command to clear the neighbor's negotiation with the switch if the configuration remains unchanged.
Example	Clear the adjacency to the neighbor 10.10.10.1. Switch#clear ldp adjacency 10.10.10.1

clear ldp session

Command	clear ldp session (A.B.C.D *)				
Parameter	<table> <tr> <td>A.B.C.D</td><td>The peer address of the LDP session</td></tr> <tr> <td>*</td><td>All LDP sessions</td></tr> </table>	A.B.C.D	The peer address of the LDP session	*	All LDP sessions
A.B.C.D	The peer address of the LDP session				
*	All LDP sessions				
Default	None				
Mode	admin Mode				
Usage Guide	Use this Command to clear the session process, and the switch restarts the session process with the configuration unchanged. Note the relationship between session and adjacency, multiple adjacency can be established in one session.				
Example	Clear all LDP sessions. Switch#clear ldp session *				

clear ldp statistics

Command	clear ldp statistics
Parameter	none
Default	None.
Mode	admin Mode
Usage Guide	This command clears all stats.

Example	Clear LDP statistics. Switch#clear ldp statistics

control-mode

Command	control-mode (ordered independent) no control-mode (ordered independent)				
Parameter	<table> <tr> <td>ordered</td><td>Orderly Control Mode</td></tr> <tr> <td>independent</td><td>Independent control mode</td></tr> </table>	ordered	Orderly Control Mode	independent	Independent control mode
ordered	Orderly Control Mode				
independent	Independent control mode				
Default	independent.				
Mode	LDP protocol configuration mode				
Usage Guide	LSP has two different control methods: independent mode and ordered mode. Independent label control means that an LSR does not need to ensure that it has obtained a downstream label map for a specific FEC before publishing it upstream. In an ordered control mode, an LSR must ensure that it has obtained a downstream label map for this FEC before distributing a label map related to a particular FEC upstream (unless the LSR itself is an egress router for this FEC). For hop-by-hop routing applications, an independent LSP control method is generally used, and DU (downstream active) mode is generally selected for label distribution. Ordered Mode must be used in conjunction with DoD (Downstream On-Demand) mode. Its no form is deconfigured.				
Example	Configure the LSP control mode to order mode. Switch(config)#router ldp Switch(config-router)#control-mode ordered				

ldp enable/disable

Command	ldp enable ldp disable
Parameter	none

Default	LDP is not launched.
Mode	Interface mode
Usage Guide	LDP protocol is a label exchange protocol used for label exchange on the public network, and it is commonly used in BGP VPN environments. Use <code>router ldp</code> to start the LDP protocol globally, but for interfaces that actually run the LDP protocol, you need to use <code>ldp enable</code> and start label-switching in the interface configuration mode for the protocol to run normally.
Example	Enable LDP on the VLAN interface. <pre>Switch(config)# int vlan 9 Switch(config-if-vlan9)# ldp enable</pre>

global-merge-capability

Command	global-merge-capability (merge-capable non-merge-capable) no global-merge-capability				
Parameter	<table> <tr> <td>merge-capable</td><td>All interfaces perform label aggregation</td></tr> <tr> <td>non-merge-capable</td><td>All interfaces do not perform label aggregation</td></tr> </table>	merge-capable	All interfaces perform label aggregation	non-merge-capable	All interfaces do not perform label aggregation
merge-capable	All interfaces perform label aggregation				
non-merge-capable	All interfaces do not perform label aggregation				
Default	Global enables tag merging capabilities.				
Mode	LDP protocol configuration mode				
Usage Guide	LSR maps multiple input tags to the same FEC, and the outbound and outbound interfaces corresponding to these input tags will be the same. This way, when packets with different tags reach LSR, the output packets will carry the same tags, a situation known as label merging. Sessions with a change in label merging capability on the interface will be restarted. Its no form reverts to its default value.				
Example	The configuration does not enable tag merging capabilities. <pre>Switch(config)#router ldp Switch(config-router)#global-merge-capability non-merge-capable</pre>				

hello-interval

Command	hello-interval <1-65535> no hello-interval
Parameter	<1-65535> Time interval value (in seconds)
Default	By default, it is 5s.
Mode	LDP protocol configuration mode
Usage Guide	LDP discovers neighbors and keeps connected by sending a multicast Hello, the command can configure the time interval at which Hello is sent, and its relationship with hold time should be noted, usually not more than 1/3 of the hold time. When the interface configures the Hello sending interval, the globally configured command is invalid on the interface. Its no form reverts to its default value.
Example	Configure hello interval to 10. Switch(config)#router ldp Switch(config-router)#hello-interval 10

hold-time

Command	hold-time <3-65535> no hold-time
Parameter	<3-65535> Hold time value (in seconds)
Default	The default is 15s.
Mode	LDP protocol configuration mode
Usage Guide	LDP discovers neighbors and keeps connected by sending a multicast Hello, the command can configure the hold time of the neighbor generated by the multicast, and its relationship with the hello interval should be noted in relation to the hello interval, which should usually be greater than or equal to 3 times the hello interval. When an interface is configured with a multicast neighbor hold time, the globally configured command is invalid on that interface. Its no form reverts to the default value.
Example	Configure the global hold time value to 50.

```
Switch(config)#router ldp
Switch(config-router)#hold time 50
```

import-bgp-routes

Command	import bgp routes no import-bgp-routes
Parameter	none
Default	LDP does not introduce BGP routes.
Mode	LDP protocol configuration mode
Usage Guide	Normally, LDP reads routes from the system routing table. Exceptions are not introduced for default routes and routes from BGP. Introducing default routes can be confusing and therefore cannot be introduced at any time. However, if the user confirms that this is not a problem, BGP routes can be introduced and labeled by setting the command. Its no form is configured to restore Default.
Example	Ingest BGP routes and set ingest route tags. Switch(config)#router ldp Switch(config-router)#import-bgp-routes

keepalive-interval

Command	keepalive interval <1-65535> no keepalive-interval
Parameter	<1-65535> Time interval value (in seconds)
Default	The default is 10s.
Mode	LDP protocol configuration mode
Usage Guide	After establishing a TCP session, LDP sends keepalives to each other to maintain a connection

	when there is no data, and this instruction is used to set the interval at which keepalives are sent. You should avoid setting the value too small and causing too many keepalive messages. When the interface configuration connection maintains the send interval, the globally configured command is invalid on that interface. Its no form reverts to its default value.
Example	The configuration global keepalive interval value is 50s. <pre>Switch(config)#router ldp Switch(config-router)# keepalive-interval 50</pre>

keepalive-timeout

Command	keepalive-timeout <30-65535> no keepalive-timeout
Parameter	<30-65535> Hold time value (in seconds)
Default	The default is 30s.
Mode	LDP protocol configuration mode
Usage Guide	After establishing a TCP session, LDP will send keepalive to each other to maintain the connection when there is no data, and if no data is received or keepalive is received within the time set by this command, the connection is considered to be disconnected. Normally, you should set a keepalive send interval with this value greater than or equal to 3 times. When the connection is configured for a hold time, the globally configured command is invalid on that interface. Its no form reverts to its default value.
Example	Configure the global keepalive timeout value. <pre>Switch(config)#router ldp Switch(config-router)#keepalive-timeout 50</pre>

label-retention-mode

Command	label-retention-mode (conservative liberal) no label-retention-mode (conservative liberal)
Parameter	conservative Conservative mode

	liberal liberal Mode
Default	liberal Mode
Mode	LDP protocol configuration mode
Usage Guide	The protocol provides two modes, one is conservative mode, that is, only the label information that is useful to the switch is retained, otherwise it will not be processed, and the other is free mode (liberal), that is, all label information is retained. This mode should be used in conjunction with the tag distribution mode, which corresponds to the downstream active mode in the distribution mode, and the conservative mode corresponds to the downstream on-demand. In particular, there is a difference between the effects of manually configuring Free Mode and the default Free Mode effects. If the free mode is manually configured, the reserved mode on the interface will be adjusted to the same mode as the global without configuration. In the default free mode, the retention mode on the interface is adjusted according to the label distribution mode on the interface. In general, it is not recommended to configure this attribute because its attribute corresponds to the distribution mode, and changing the distribution mode will automatically change the label retention mode. If the label retention mode has changed, but the interface is not configured on the session of the interface that does not have the label retention mode, reconnect the session. noCommand reverts to Default.
Example	Configure the global label to keep the mode as free mode. <pre>Switch(config)#router ldp Switch(config-router)#label-retention-mode liberal</pre>

label-switching

Command	label switching no label-switching
Parameter	none
Default	The interface does not turn on the label exchange function.
Mode	Interface Mode
Usage Guide	This command is used to turn on the label switching function on the interface, otherwise the LDP protocol will not work properly. No operation is to turn off the label exchange function of the interface.
Example	Enables the label swap function of interface VLAN1.

```
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#label-switching
```

ldp advertisement-mode

Command	ldp advertisement-mode (downstream-on-demand downstream-unsolicited) no ldp advertisement-mode (downstream-on-demand downstream-unsolicited)	
Parameter	downstream-on-demand	Downstream On-Demand Mode
	downstream-unsolicited	Downstream active mode
Default	Use global configuration.	
Mode	Interface Mode	
Usage Guide	This command is used to configure the interface label distribution mode, which can be selected as downstream unsolicited or downstream on demand. For port configuration, you can use a different parameter than the global one. By default, the global default parameter or the globally configured distribution mode is used, and when the interface is configured with this parameter, the interface configuration is adopted. If the label distribution mode is set to the other two modes, the label distribution mode will be changed at the same time. If the configured parameter is downstream active, set the interface label retention mode to Libral mode and the LSP control mode to independent mode. If the downstream is on-demand, set the interface label retention mode to Consevation Mode and the LSP control mode to Ordered Mode. This command can be configured for the interface and can use a different parameter than the global one. no, and use the global setting.	
Example	Under Interface mode, set the label distribution mode to downstream active <pre>Switch (config)#int vlan 9 Switch (config-if-vlan9)#ldp advertisement-mode downstream-unsolicited</pre>	

ldp hello-interval

Command	ldp hello-interval <1-65535> no ldp hello-interval	
Parameter	<1-65535>	Time interval value (in seconds)

Default	Use global configuration.
Mode	Interface Mode
Usage Guide	This command is used to configure the time interval at which the interface sends multicast Hello packets. This command is configured for the interface and can use a different parameter than the global one. no operation to cancel the setting and use the global setting.
Example	Set the Hello sending interval to 25s. Switch (config)#int vlan 9 Switch (config-if-vlan9)#ldp hello-interval 25

ldp hold-time

Command	ldp hold-time <3-65535> no ldp hold-time
Parameter	<3-65535> Holding time (in seconds)
Default	Use global configuration.
Mode	Interface Mode
Usage Guide	LDP discovers neighbors and keeps connected by sending a multicast Hello, this Command can configure the hold time of the neighbors generated by the multicast, and its relationship with the hello interval should be noted in relation to the hello interval, which should usually be greater than or equal to 3 times the hello interval. The command is configured for the port and can use a different parameter than the global. no operation to cancel the setting and use the global setting.
Example	Configure a neighbor timeout of 220s under Port. Switch(config)#int vlan 9 Switch(config-if-vlan9)#ldp hold-time 220

ldp keepalive-interval

Command	ldp keepalive-interval <1-65535> no ldp keepalive-interval
Parameter	<1-65535> Time interval value (in seconds)
Default	Use global configuration.
Mode	Interface Mode
Usage Guide	After establishing a TCP session, LDP will send keepalives to each other to maintain a connection when there is no data, and this command is used to set the interval at which keepalives are sent. You should avoid setting the value too small and causing too many keepalive messages. The Command is configured for the port and can use a different parameter than the global. no operation to cancel the setting and use the global setting.
Example	Configure a continuous message transmission interval of 33 seconds under the port. Switch(config)#int vlan 9 Switch(config-if-vlan9)#ldp keepalive-interval 33

ldp keepalive-timeout

Command	ldp keepalive-timeout <30-65535> no ldp keepalive-timeout
Parameter	<30-65535> Time interval value (in seconds)
Default	Use global configuration.
Mode	Interface Mode
Usage Guide	After establishing a TCP session, LDP will send keepalives to each other to maintain the connection when there is no data, and if no data is received or keepalive within the time set by this command, the connection is considered to be disconnected. In general, you should set a keepalive send interval with this value greater than or equal to 3 times. The Command is configured for the port and can use a different parameter than the global. no operation to cancel the setting and use the global setting.
Example	The connection hold time under the interface is configured to be 200. Switch(config)#int vlan 9 Switch(config-if-vlan9)#ldp keepalive-timeout 200

ldp label-retention-mode

Command	ldp label retention mode {conservative liberal} no ldp label-retention-mode {conservative liberal}
Parameter	conservative conservative Mode liberal liberal Mode
Default	Use global configuration.
Mode	Interface Mode
Usage Guide	The label of the configuration interface is kept in Mode. Two ways: conservative and liberal. If the retention mode changes, re-establish the session connection on that interface. If the configuration is different from the global mode, the configuration on the interface shall prevail. The Command is configured for the port and can use a different parameter than the global. no operation to cancel the setting and use the global setting.
Example	The configuration label under the interface is set to Conservative Mode. Switch(config)#int vlan 9 Switch(config-if-vlan9)#ldp label-retention-mode conservative

ldp multicast-hellos

Command	ldp multicast-hellos no ldp multicast-hellos
Parameter	none
Default	Use global configuration.
Mode	Interface Mode
Usage Guide	LDP can discover its neighbors through multicast Hello packets, or it can specify neighbors through targeted peerCommand, which enables multicast Hello to discover neighbors. The no form does not send and receive multicast Hellos, but only determines neighbors through targeted peers. Configuring for ports allows you to use different parameters than global. no operation to cancel the setting and use the global setting.

Example	interface enables multicast-hellos <pre>Switch(config)#int vlan 9 Switch(config-if-vlan9)#ldp multicast-hellos</pre>

ldp targeted-peer-hello-interval

Command	ldp targeted-peer-hello-interval <1-65535> no ldp targeted-peer-hello-interval
Parameter	<1-65535> Time interval value (in seconds)
Default	Use global configuration.
Mode	Interface Mode
Usage Guide	LDP discovers neighbors and keeps connected by sending Hellos to specified destinations, the command can configure the time interval at which Hellos are sent to specified destinations, and its relationship with the targeted peer hold time should generally not exceed 1/3 of the targeted peer hold time. Configuring for interfaces allows the use of different parameters than globally. no operation to cancel the setting and use the global setting.
Example	Set the Hello send interval for the specified destination of the interface to be 255s. <pre>Switch(config)#int vlan 9 Switch(config-if-vlan9)#ldp targeted-peer-hello-interval 255</pre>

ldp targeted-peer-hold-time

Command	ldp targeted-peer-hold-time <3-65535> no ldp targeted-peer-hold-time
Parameter	<3-65535> Hold time value (in seconds)
Default	Use global configuration.
Mode	Interface Mode

Usage Guide	LDP discovers neighbors and keeps connected by sending a Hello for a specified destination, the command can configure the hold time of the neighbor generated by the specified destination, and its relationship with targeted-peer-hello-interval should be noted in relation to targeted-peer-hello-interval, which should usually be greater than or equal to 3 times the targeted-peer-hello-interval. Configuring for ports allows you to use different parameters than global. no operation to cancel the setting and use the global setting.
Example	Set the targeted-peer-hold-time of the interface to 50s. Switch(config)#int vlan 9 Switch(config-if-vlan9)# ldp targeted-peer-hold-time 50

loop-detection

Command	loop-detection no loop-detection
Parameter	none
Default	No loop detection.
Mode	LDP protocol configuration mode
Usage Guide	LDP can be set to detect the loop, and if it does, LDP does it in two ways, one is to see if the HOP-COUNT exceeds the allowed upper limit, and the other is to see if there are duplicate LSR-IDs on the path vector. Its no form is deconfigured.
Example	enable loop-detection. Switch(config)#router ldp Switch(config-router)#loop-detection

loop-detection-count

Command	loop-detection-count <1-255>
Parameter	<1-255> The maximum number of hops for loop detection

Default	255
Mode	LDP protocol configuration mode
Usage Guide	LDP can set whether to detect the loop, and if so, LDP can set the upper limit of the number of hops allowed through this command. This setting only takes effect if loop detection is set. Its no form reverts to its default value.
Example	The number of hops allowed when setting LDP loop detection is 200 Switch(config)#router ldp Switch(config-router)#loop-detection-count 200

multicast-hellos

Command	multicast-hellos no multicast-hellos
Parameter	none
Default	Enables LDP interfaces to send and receive multicast Hellos.
Mode	LDP protocol configuration mode
Usage Guide	LDP can discover its own neighbors via multicast, or it can specify neighbors through a targeted peerCommand, which enables neighbors to be discovered via multicast Hello. The no form does not send a multicast Hello, but only determines the neighbor through the targeted peer. Configure Global Mode to send and receive multicast hello packets and traverse all interfaces. If the property is configured on the interface, the interface takes precedence, and if the interface is not configured, apply the configuration to the interface. no form does not send and receive multicast Hello.
Example	enable multicast-hellos. Switch(config)#router ldp Switch(config-router)#multicast-hellos

propagate-release

Command	propagate-release no propagate-release
Parameter	none
Default	It is not enable.
Mode	LDP protocol configuration mode
Usage Guide	If the tag expires, the tag will not be sent upstream, but if the command is configured, the information of the invalid tag will still be sent upstream even if the tag is invalid. Its NO form configuration does not propagate the release of tags.
Example	enable propagate-release. Switch(config)#router ldp Switch(config-router)# propagate-release

request-retry

Command	request-retry no request-retry
Parameter	none
Default	No retrying.
Mode	LDP protocol configuration mode
Usage Guide	When LDP sends a label request to a downstream, if the downstream rejects it for some reason, LDP will retry up to 5 times after setting the property. The interval is set for request-retry-timeout. Its no form cancels the setting.
Example	enable request-retry. Switch(config)#router ldp Switch(config-router)#request-retry

request-retry-timeout

Command	request-retry-timeout <1-65535> no request-retry-timeout
Parameter	<1-65535> Time interval value (in seconds)
Default	5
Mode	LDP protocol configuration mode
Usage Guide	When LDP sends a label request to a downstream, if the downstream rejects it for some reason, LDP will retry up to 5 times after setting the request retry property. The interval is set for request-retry-timeout. Its no form reverts to its default value.
Example	Set the retry interval to 10s Switch(config)#router ldp Switch(config-router)#request-retry-timeout 10

router ldp

Command	router ldp no router ldp
Parameter	none
Default	LDP is not enabled by default.
Mode	Global Mode
Usage Guide	This Command can enable LDP globally and enter LDP protocol configuration mode no command cancel LDP
Example	Global Enable LDP. Switch(config)# router ldp

router-id

Command	router-id A.B.C.D no router-id
Parameter	A.B.C.D LDP router identifier
Default	Automatically obtained.
Mode	LDP protocol configuration mode
Usage Guide	The router ID uniquely identifies an LDP device on the network. Router-id is the router-id in the Hello message. noCommand deprovisioning
Example	Configure the router-id of LDP. Switch(config)#router ldp Switch(config-router)#router-id 10.10.10.10

show ldp

Command	show ldp
Parameter	none
Default	None.
Mode	All Mode
Usage Guide	This command is used to display information about the current configuration of LDP.
Example	Displays LDP information. Switch#show ldp Router ID : 0.0.0.0 LDP Version : 1 Global Merge Capability : Merge Capable 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 Address	: None
Import BGP Routes	: No

show ldp adjacency

Command	show ldp adjacency												
Parameter	none												
Default	None.												
Mode	All Mode												
Usage Guide	This command is used to display the adjacency information of the LDP and can be used for diagnostics and debugging.												
Example	Displays LDP adjacency information. Switch#show ldp adjacency <table><thead><tr><th>IP Address</th><th>Interface Name</th><th>Holdtime</th><th>LDP ID</th></tr></thead><tbody><tr><td>192.168.3.5</td><td>vlan1</td><td>15</td><td>10.10.0.18:0</td></tr><tr><td>192.168.4.5</td><td>vlan2</td><td>15</td><td>10.10.0.18:0</td></tr></tbody></table>	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
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										

show ldp downstream

Command	show ldp downstream

Parameter	none
Default	None.
Mode	All Mode
Usage Guide	Information used to display the downstream status of the current protocol maintenance.
Example	Displays all downstream information for this LSR. <pre> 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: </pre>

show ldp fec

Command	show ldp fec
Parameter	none
Default	None.
Mode	All Mode
Usage Guide	Used to display forwarding equivalent class information for current maintenance.
Example	Displays all forwarding equivalent information for this LSR. <pre> 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 > 192.168.9.61/32 Non-Existent None Connected FEC Statistics: Total entry is 1 </pre>

show ldp interface

Command	show ldp interface show ldp interface (vlan <1-4094> IFNAME)			
Parameter	<1-4094>	VLAN port number		
	IFNAME	Interface name		
Default	None.			
Mode	All Mode			
Usage Guide	The Command is used to display the LDP information on the interface, and the LDP information of the specified interface can be displayed with Parameter. Without parameter, all interface information is displayed.			
Example	Displays LDP information for this LSR or for all interfaces.			
	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

show ldp lsp

Command	show ldp lsp
Parameter	none
Default	None.
Mode	All Mode
Usage Guide	The Command is used to display the switch's label switch path information.
Example	Displays the tag swap path information for this LSR.
	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

show ldp session

Command	show ldp session show ldp session A.B.C.D																			
Parameter	A.B.C.D The peer address of the session																			
Default	None.																			
Mode	All Mode																			
Usage Guide	This Command is used to display the current LDP session information of this switch.																			
Example	Displays all LDP session information for this LSR. Switch#show ldp session <table><tr><td>Peer IP Address</td><td>IF Name</td><td>My Role</td><td>State</td><td>KeepAlive</td></tr><tr><td>192.168.11.50</td><td>vlan1</td><td>Passive</td><td>OPERATIONAL</td><td>30</td></tr><tr><td>192.168.13.60</td><td>vlan2</td><td>Passive</td><td>OPERATIONAL</td><td>30</td></tr></table>					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
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																

show ldp statistics

Command	show ldp statistics
Parameter	none
Default	None.

Mode	All Mode																																				
Usage Guide	This Command is used to display the current LDP statistics of this switch.																																				
Example	Displays LDP statistics for this LSR. Switch#show ldp statistics <table><tr><td>PacketType</td><td>Sent</td><td>Received</td></tr><tr><td>Notification</td><td>0</td><td>0</td></tr><tr><td>Hello</td><td>0</td><td>0</td></tr><tr><td>Initialization</td><td>0</td><td>0</td></tr><tr><td>Keepalive</td><td>0</td><td>0</td></tr><tr><td>Address</td><td>0</td><td>0</td></tr><tr><td>Address Withdraw</td><td>0</td><td>0</td></tr><tr><td>Label Mapping</td><td>0</td><td>0</td></tr><tr><td>Label Request</td><td>0</td><td>0</td></tr><tr><td>Label Withdraw</td><td>0</td><td>0</td></tr><tr><td>Label Release</td><td>0</td><td>0</td></tr><tr><td>Request About</td><td>0</td><td>0</td></tr></table>	PacketType	Sent	Received	Notification	0	0	Hello	0	0	Initialization	0	0	Keepalive	0	0	Address	0	0	Address Withdraw	0	0	Label Mapping	0	0	Label Request	0	0	Label Withdraw	0	0	Label Release	0	0	Request About	0	0
PacketType	Sent	Received																																			
Notification	0	0																																			
Hello	0	0																																			
Initialization	0	0																																			
Keepalive	0	0																																			
Address	0	0																																			
Address Withdraw	0	0																																			
Label Mapping	0	0																																			
Label Request	0	0																																			
Label Withdraw	0	0																																			
Label Release	0	0																																			
Request About	0	0																																			

show ldp targeted-peers

Command	show ldp targeted-peers				
Parameter	none				
Default	None.				
Mode	All Mode				
Usage Guide	The Command is used to display the currently configured LDP neighbor information.				
Example	Displays LDP neighbor information for the specified destination for this LSR configuration. <pre>Switch#show ldp targeted-peers</pre> <table> <tr> <th>IP Address</th><th>Interface</th></tr> <tr> <td>10.1.1.66</td><td>Vlan2</td></tr> </table>	IP Address	Interface	10.1.1.66	Vlan2
IP Address	Interface				
10.1.1.66	Vlan2				

show ldp upstream

Command	show ldp upstream
Parameter	none
Default	None.
Mode	All Mode
Usage Guide	This command is used to display the current LDP upstream information maintained by the switch.
Example	Displays all upstream information for this LSR. 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:

show mpls ldp discovery

Command	show ldp discovery show ldp discovery (vlan <1-4094> IFNAME)			
Parameter	<1-4094>	VLAN port number		
	IFNAME	Interface name		
Default	None.			
Mode	All Mode			
Usage Guide	This Command is used to display all or specified interfaces and label exchange information.			
Example	Displays all interfaces and their tag exchange information for this LSR.			
	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

show mpls ldp fec

Command	show mpls ldp fec
Parameter	none
Default	None.
Mode	All Mode
Usage Guide	This command is used to display the forwarding equivalent class information that is currently maintained.
Example	Displays all forwarding equivalent information for this LSR. <pre>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 > 192.168.9.61/32 Non-Existent None Connected FEC Statistics: Total entry is 1</pre>

show mpls ldp neighbor

Command	show mpls ldp neighbor
Parameter	none
Default	None.
Mode	All Mode
Usage Guide	The Command is used to display the adjacency information of the LDP and can be used for diagnostics.
Example	Displays all adjacency information for this LSR.

	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

show mpls ldp parameter

Command	show mpls ldp parameter
Parameter	none
Default	None.
Mode	All Mode
Usage Guide	The Command is used to display information about the current configuration of LDP.
Example	Displays some basic LDP properties in this LSR. <pre> Switch#show mpls ldp parameter Router ID : 0.0.0.0 LDP Version : 1 Global Merge Capability : Merge Capable 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 Address : None Import BGP Routes : No </pre>

show mpls ldp session

Command	show mpls ldp session															
Parameter	none															
Default	None.															
Mode	All Mode															
Usage Guide	Used to display the current LDP session information of this switch.															
Example	Displays LDP adjacency information. Switch#show mpls ldp session <table><tr><th>Peer IP Address</th><th>IF Name</th><th>My Role</th><th>State</th><th>KeepAlive</th></tr><tr><td>192.168.11.50</td><td>vlan1</td><td>Passive</td><td>OPERATIONAL</td><td>30</td></tr><tr><td>192.168.13.60</td><td>vlan2</td><td>Passive</td><td>OPERATIONAL</td><td>30</td></tr></table>	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
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												

targeted-hello-accept

Command	targeted-hello-accept targeted-hello-accept filter <1-99> no targeted-hello-accept
Parameter	<1-99> Access the list number
Default	Target-Hello packets are not received.
Mode	LDP protocol configuration mode
Usage Guide	By configuring the command, you can use the command in the access list to specify a target so that LDP can accept the target's Hello packet. noCancel the setting.
Example	Receives Hello packets sent from destinations allowed in Access List 1. <pre>Switch(config)#router ldp Switch(config-router)#targeted-hello-accept filter 1</pre>

targeted-peer

Command	targeted-peer A.B.C.D no targeted-peer A.B.C.D
Parameter	A.B.C.D Specify the IPv4 address of the destination's neighbor
Default	no targeted peer.
Mode	LDP protocol configuration mode
Usage Guide	LDP can automatically discover neighbors through multicast Hello or by manually configuring neighbors, which is used to manually configure neighbors. Add a targeted peer to establish a neighborhood relationship. Set up a neighbor for a specified destination, that is, establish an extended form of session. Its no form can remove the configuration.
Example	The LDP neighbor for the specified destination is configured to be 10.10.10.10 Switch(config)#router ldp Switch(config-router)#targeted-peer 10.10.10.10

targeted-peer-hello-interval

Command	targeted-peer-hello-interval <1-65535> no targeted-peer-hello-interval
Parameter	<1-65535> Time interval value (in seconds)
Default	15
Mode	LDP protocol configuration mode
Usage Guide	LDP discovers neighbors and keeps connected by sending Hellos to specified destinations, the command can configure the time interval at which Hellos are sent to specified destinations, and its relationship with targeted-peer-hold-time should generally not exceed 1/3 of targeted-peer-hold-time. If there is a configuration for a specific interface, the configuration does not take effect for the specific interface. Its no form reverts to its default value.

Example	Configure the Hello sending interval to be 50s Switch(config)#router ldp Switch(config-router)#targeted-peer-hello interval 50

targeted-peer-hold-time

Command	targeted-peer-hold-time <3-65535> no targeted-peer-hold-time
Parameter	<3-65535> Hold time value (in seconds)
Default	45
Mode	LDP protocol configuration mode
Usage Guide	LDP discovers neighbors and keeps connected by sending a hello for a specified destination, which can configure the hold time for neighbors discovered by a specified destination, noting its relationship to the targeted peer hello interval, which should generally be greater than or equal to 3 times the targeted peer hello interval. If there is a configuration for a specific interface, the configuration does not take effect for the specific interface. Its no form reverts to its default value.
Example	Configure the neighbor hold time to 50s Switch(config)#router ldp Switch(config-router)#targeted-peer-hold-time 50

transport-address

Command	transport-address A.B.C.D no transport-address
Parameter	A.B.C.D Loopback interface
Default	Automatically obtained.

Mode	LDP protocol configuration mode
Usage Guide	After LDP discovers a neighbor through multicast or Hello packets at specified destinations, it does not directly use the interface address that sent the message as the source address for establishing a TCP connection, but uses the transport-address carried in the Hello packet (this ensures that the connection is unique). Normally, LDP chooses the address of an interface as the transport-address. This Command determines the address to be used by configuring. The no form cancels the configuration and automatically obtains an interface address as the transport-address again. its no form cancels the configuration.
Example	Configure the use of 10.10.10.10 as the address used to establish the TCP connection <pre> Switch(config)#router ldp Switch(config-router)#transport-address 10.10.10.10 </pre>

3 Commands for Static LSP

nsm mpls ftn add

Command	mpls ftn-entry A.B.C.D/M LABEL A.B.C.D IFNAME no mpls ftn-entry A.B.C.D/M WORD A.B.C.D IFNAME						
Parameter	A.B.C.D/M	Masked forwarding equivalent class					
	LABEL	Outgoing label (16-1048575)					
	A.B.C.D	The next hop IPv4 address					
	IFNAME	Outgoing interface name					
	WORD	Outgoing label (16-1048575)					
Default	Not configured by default						
Mode	Global Mode						
Usage Guide	This command is used to configure the ftn table key of the static LSP. The configured interface must have been created, and label-switching must be enabled for the VLAN interface. no mpls ftn-entry A.B.C.D/M WORD A.B.C.D IFNAMECommand is used to delete the configured static ftn table.						
Example	The switch creates a static FTN Switch(config)#mpls ftn-entry 192.168.9.90/32 999 15.1.1.1 Vlan15 Switch(config)#show mpls ftn-table b FTN Entry Brief Information ----- ----- FEC Out-Label Out-intf Next hop Oper-code Op-State Vrf 192.168.9.90/32 999 Vlan15 15.1.1.1 Push Up 0						

nsm mpls ftn mask add

Command	mpls ftn-entry A.B.C.D A.B.C.D LABEL A.B.C.D IFNAME no mpls ftn-entry A.B.C.D A.B.C.D WORD A.B.C.D IFNAME						
Parameter	A.B.C.D	Forwarding equivalents					
	A.B.C.D	Forward the mask of the equivalent class					

	LABEL	Outgoing label (16-1048575)
	A.B.C.D	The next hop IPv4 address
	IFNAME	Outgoing interface name
	WORD	Outgoing label (16-1048575)
Default	Not configured by default	
Mode	Global Mode	
Usage Guide	This command is used to configure the ftn table key of the static LSP. The configured interface must have been created, and label-switching must be enabled for the VLAN interface. no mpls ftn-entry A.B.C.D A.B.C.D WORD A.B.C.D IFNAME Command is used to delete configured static ftn tables.	
Example	The switch creates a static FTN <pre>Switch(config)#mpls ftn-entry 192.168.9.90 255.255.255.255 999 15.1.1.1 Vlan15 Switch(config)#show mpls ftn-table b</pre> FTN Entry Brief Information <pre>----- ----- FEC Out-Label Out-intf Next hop Oper-code Op-State Vrf 192.168.9.90/32 999 Vlan15 15.1.1.1 Push Up 0</pre>	

nsm mpls ilm add

Command	mpls ilm-entry LABEL IFNAME LABEL IFNAME A.B.C.D (swap pop vpnpop) (A.B.C.D/M A.B.C.D A.B.C.D)	
Parameter	LABEL	Incoming label (16-1048575)
	IFNAME	Input interface name
	LABEL	Outgoing label (16-1048575)
	IFNAME	Outgoing interface name
	A.B.C.D	The next hop IPv4 address
	swap	Swap incoming label
	pop	Pop incoming label
	vpnpop	Pop incoming label and forward the VPN packet

A.B.C.D/M	The FEC used to create the ILM item, with a mask
A.B.C.D	The FEC used to create the ILM item
A.B.C.D	FEC mask

Default	Not configured by default
Mode	Global Mode
Usage Guide	This command is used to configure the ilm table entry of the static LSP. The configured interface must have been created, and label-switching is enabled for the VLAN interface, and the same input label cannot be configured. no mpls ilm-entry LABEL IFNAMECommand is used to delete the configured static ilm table. If the FEC address is not configured, it is 0.0.0.0/0
Example	The switch creates a static ILM <pre>Switch(config)#mpls ilm-entry 999 Vlan15 666 Vlan15 5.1.1.2 swap 192.168.9.90/32 Switch(config)#show mpls ilm-table In-Label Out-Label In-Intf Out-Intf Nexthop FEC 999 666 Vlan15 Vlan15 5.1.1.2 192.168.9.90/32</pre>

nsm mpls ilm delete

Command	no mpls ilm-entry LABEL IFNAME				
Parameter	<table> <tr> <td>LABEL</td><td>Incoming label (16-1048575)</td></tr> <tr> <td>IFNAME</td><td>Incoming interface name</td></tr> </table>	LABEL	Incoming label (16-1048575)	IFNAME	Incoming interface name
LABEL	Incoming label (16-1048575)				
IFNAME	Incoming interface name				
Default	Not configured by default				
Mode	Global Mode				
Usage Guide	This command is used to delete the ilm table entry of the static LSP. The configured interface must have been created, and label-switching must be enabled for the VLAN interface.				
Example	The switch deletes the static ilm <pre>Switch(config)#show mpls ilm-table In-Label Out-Label In-Intf Out-Intf Nexthop FEC 999 666 Vlan15 Vlan15 5.1.1.2 192.168.9.90/32 Switch(config)#no mpls ilm-entry 999 Vlan15</pre>				

```
Switch(config)#show mpls ilm-table
Switch(config)#
```

4 Commands for VPLS&VPWS

set PW ptag

Command	vc-ptag <ptag>
Parameter	<ptag> ptag during the packaging process of PW packets
Default	Not configured by default
Mode	Global Mode
Usage	This command is used to set the ptag during the PW packet encapsulation process
Guide	
Example	Switch(config)#vc-ptag 324 Switch(config)# Switch(config)#vc-ptag 0 Switch(config)#

create/delete PW class

Command	pw-class <class-name> no pw-class <class-name>
Parameter	<class-name> PW template naming
Default	Not configured by default
Mode	Global Mode
Usage	This Command is used to create/delete PW templates
Guide	
Example	Switch(config)#pw-class c1 Switch(config-pw-class)#show running-config current-mode ! pw-class c1 ! Switch(config-pw-class)#qu Switch(config)#no pw-class c1 Switch(config)# Switch(config)#

PW class transport mode

Command	transport-mode {ethernet vlan} no transport-mode
Parameter	ethernet The message is encapsulated in rawMode vlan The packet encapsulates taggedMode
Default	Not configured by default
Mode	PwClass Mode
Usage	This command is used to set the packet encapsulation method of the current PW template
Guide	
Example	Switch(config-pw-class)#show running-config current-mode ! pw-class c1 ! Switch(config-pw-class)# Switch(config-pw-class)# Switch(config-pw-class)#transport-mode ethernet Switch(config-pw-class)#show running-config current-mode ! pw-class c1 transport-mode ethernet ! Switch(config-pw-class)#no transport-mode Switch(config-pw-class)#show running-config current-mode ! pw-class c1 !

create/delete VFI

Command	vfi <vfi-name> [<vfi-id>] no vfi <vfi-name>
Parameter	<vfi-name> VFI instance naming <vfi-id> VFI instance number
Default	Not configured by default
Mode	Global Mode
Usage	This Command is used to create/delete VFI instances, and <vfi-id>without a parameter indicates an attempt to enter the VFI
Guide	
Example	Switch(config)#vfi v1 10 Switch(config-vfi)#show running-config current-mode ! vfi v1 10 ! Switch(config-vfi)#quit

Switch(config)#no vfi v1

Switch(config)#

create/delete PW

Command	peer A.B.C.D [pw-id <pw-id>] [no-split-horizon] [pw-class <class-name>] no peer A.B.C.D pw-id <pw-id> exit-peer	
Parameter	A.B.C.D	PW peer address
	pw-id <pw-id>	PW number, optional, defaults to 1
	no-split-horizon	Turn off horizontal splitting, optional, turn on horizontal splitting by default
	pw-class <class-name>	PW template, optional
Default	Not configured by default	
Mode	VFI Mode	
Usage Guide	This command is used to create/delete PW, exit-peer exit the PW Mode	
Example	<pre>Switch(config)#pw-class c1 Switch(config-pw-class)#transport-mode vlan Switch(config-pw-class)#exit Switch(config)#vfi v1 10 Switch(config-vfi)#peer 2.2.2.2 pw-id 100 no-split-horizon pw-class c1 Switch(config-vfi-2.2.2.2-100)# Switch(config-vfi-2.2.2.2-100)#show running-config current-mode ! peer 2.2.2.2 pw-id 100 no-split-horizon pw-class c1 exit-peer ! Switch(config-vfi-2.2.2.2-100)#exit-peer Switch(config-vfi)#no peer 2.2.2.2 pw-id 100 Switch(config-vfi)# Switch(config-vfi)#show running-config current-mode ! vfi v1 10 ! Switch(config-vfi)#</pre>	

create/delete back PW

Command	backup-peer A.B.C.D [pw-id <pw-id>] [pw-class <class-name>] no backup-peer A.B.C.D pw-id <pw-id>	
Parameter	A.B.C.D	Prepare PW peer address
	pw-id <pw-id>	Alternative PW number, optional, must be the same as the primary PW number

	pw-class <class- PW template, optional name>
Default	Not configured by default
Mode	VplsPw Mode
Usage	This Command is used to create/delete alternate PWs
Guide	
Example	<pre> Switch(config-vfi-2.2.2.2-100)#show running-config current-mode ! peer 2.2.2.2 pw-id 100 no-split-horizon pw-class c1 exit-peer ! Switch(config-vfi-2.2.2.2-100)#backup-peer 3.3.3.3 pw-id 100 pw-class c1 Switch(config-vfi-2.2.2.2-100)#show running-config current-mode ! peer 2.2.2.2 pw-id 100 no-split-horizon pw-class c1 backup-peer 3.3.3.3 pw-id 100 pw-class c1 exit-peer ! Switch(config-vfi-2.2.2.2-100)#no backup-peer 3.3.3.3 pw-id 100 Switch(config-vfi-2.2.2.2-100)#show running-config current-mode ! peer 2.2.2.2 pw-id 100 no-split-horizon pw-class c1 exit-peer ! Switch(config-vfi-2.2.2.2-100)# </pre>

enable/disable BFD

Command	vpls bfd enable no vpls bfd enable
Default	Not configured by default
Mode	VFI Mode
Usage	This Command is used to determine whether PW is BFD enabled in the current VFI instance
Guide	
Example	<pre> Switch(config-vfi)#show running-config current-mode ! vfi v1 10 peer 2.2.2.2 pw-id 100 no-split-horizon pw-class c1 exit-peer ! Switch(config-vfi)#vpls bfd enable Switch(config-vfi)#show running-config current-mode ! vfi v1 10 vpls bfd enable peer 2.2.2.2 pw-id 100 no-split-horizon pw-class c1 </pre>

```

exit-peer
!
Switch(config-vfi)#no vpls bfd enable

```

switch PW redundancy mode

Command	pw-redundancy {independent master} no pw-redundancy
Parameter	independent The local PW determines the forwarding status based on the forwarding status of the remote PE advertisement master The local PW determines the forwarding status according to the configured forwarding priority and notifies the remote end
Default	Not configured by default
Mode	VFI Mode
Usage	This Command is used for PW mode in the current VFI instance regarding redundant backups, or to restore the default mode
Guide	
Example	Switch(config-vfi)#pw-redundancy independent Switch(config-vfi)#show running-config current-mode ! vfi v1 10 pw-redundancy independent peer 2.2.2.2 pw-id 100 no-split-horizon pw-class c1 exit-peer ! Switch(config-vfi)#pw-redundancy master Switch(config-vfi)#show running-config current-mode ! vfi v1 10 pw-redundancy master peer 2.2.2.2 pw-id 100 no-split-horizon pw-class c1 exit-peer ! Switch(config-vfi)#no pw-redundancy Switch(config-vfi)#show running-config current-mode ! vfi v1 10 peer 2.2.2.2 pw-id 100 no-split-horizon pw-class c1 exit-peer !

PW MTU

Command	mtu <mtu-value> no mtu

Parameter	<mtu-value> The MTU value allowed by PW is 1500 by default
Default	Not configured by default
Mode	VFI Mode
Usage	This command modifies the MTU value of the PW in the current VFI instance
Guide	
Example	<pre> Switch(config-vfi)#mtu 1280 Switch(config-vfi)#show running-config current-mode ! vfi v1 10 mtu 1280 peer 2.2.2.2 pw-id 100 no-split-horizon pw-class c1 exit-peer ! Switch(config-vfi)#no mtu Switch(config-vfi)#show running-config current-mode ! vfi v1 10 peer 2.2.2.2 pw-id 100 no-split-horizon pw-class c1 exit-peer ! </pre>

create/delete l2-vc

Command	l2-vc A.B.C.D pw-id <pw-id> [group-id <group-id>] [pw-class <class-name>] [mtu <mtu-vlaue>] [secondary] no l2-vc A.B.C.D pw-id <pw-id>				
Parameter	A.B.C.D	The remote PW address			
	pw-id <pw-id>	PW number			
	group-id <group-id>	PW group number, optional			
	pw-class <class-name>	PW template, optional			
	mtu <mtu-value>	PW packet MTU, optional, defaults to 1500			
	secondary	To indicate that the current PW is a backup PW, there must be a master PW with the same PW number but with a different address.			
Default	Not configured by default				
Mode	Global Mode				
Usage Guide	This Command is used to create/delete PWs				
Example	Switch(config)#l2-vc 5.5.5.5 pw-id 200 group-id 20 pw-class c1 mtu 1280 Switch(config)#l2-vc 6.6.6.6 pw-id 200 pw-class c1 mtu 2180 secondary Switch(config)#show mpls l2-vc				
	VC ID	State	Type	In Label	Out
	Label	Endpoint			

	200	Down	VLAN	none	none
	5.5.5.5				
	200	Down	VLAN	none	none
	6.6.6.6				
Switch(config)#show ldp mpls-l2-circuit					
Transport	Client	VC	Trans	Local	Remote
Destination	Config				
VC ID	Binding	State	Type	VC Label	VC Label
Address					
200	None	Down	Vlan	N/A	N/A
5.5.5.5	Yes				
200	None	Down	Vlan	N/A	N/A
6.6.6.6	Yes				
Switch(config)#no l2-vc 5.5.5.5 pw-id 200					
Switch(config)#					

xconnect

Command	xconnect {l2-vc pw-id <pw-id> vfi <vfi-id>} [mode {ethernet vlan svid <svid>}] no xconnect {l2-vc pw-id <pw-id> vfi <vfi-id>} [mode {ethernet vlan svid <svid>}]								
Parameter	<table> <tr> <td>l2-vc pw-id <pw-id></td><td>VPWS PW number</td></tr> <tr> <td>vfi <vfi-id></td><td>VFI number</td></tr> <tr> <td>mode ethernet</td><td>The AC side message package is rawMode, optional</td></tr> <tr> <td>mode vlan svid <svid></td><td>The AC side packet is packaged as taggedMode, which is optional</td></tr> </table>	l2-vc pw-id <pw-id>	VPWS PW number	vfi <vfi-id>	VFI number	mode ethernet	The AC side message package is rawMode, optional	mode vlan svid <svid>	The AC side packet is packaged as taggedMode, which is optional
l2-vc pw-id <pw-id>	VPWS PW number								
vfi <vfi-id>	VFI number								
mode ethernet	The AC side message package is rawMode, optional								
mode vlan svid <svid>	The AC side packet is packaged as taggedMode, which is optional								
Default	Not configured by default								
Mode	Interface Mode								
Usage	This Command is used for AC side interface access								
Guide									
Example	<pre>Switch(config-if-ethernet1/0/25)#xconnect vfi 10 mode vlan svid 30 Switch(config-if-ethernet1/0/25)#show running-config current-mode ! Interface Ethernet1/0/25 xconnect vfi 10 mode vlan svid 30 ! Switch(config-if-ethernet1/0/25)#</pre>								

show mpls forwarding-table

Command	show mpls forwarding-table

Default	Not configured by default
Mode	All Mode
Usage	This Command displays the MPLS forwarding entry
Guide	
Example	Switch(config)#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 - unknown FTN

```

Code  FEC                      FTN-ID  Pri  Nexthop          Out-
Label  Out-Intf
L>    30.1.1.224/32          1      Yes  42.1.7.1          3
Vlan370
L>    42.1.7.0/24           2      Yes  0.0.0.0           3
Vlan370

```

Printed information	Explanation
Code	Item Source
FEC	Forwarding Equivalent
FTC-ID	Class Forwarding
Pri	Equivalent Class ID
Nexthop	Priority
Out-Label	Next Hop
Out-Intf	Outgoing Tag

show mpls ftn

Command	show mpls ftn-table {brief detail}
Parameter	brief Concise entry data detail Detailed entry data
Default	Not configured by default
Mode	All Mode
Usage	This Command displays the FTN table entry
Guide	
Example	Switch(config)#show mpls ftn-table brief FTN Entry Brief Information <pre> ----- FEC Out-Label Out-intf Next hop Oper-code Op-State Vrf 30.1.1.224/32 3 Vlan370 42.1.7.1 Push Up 0 42.1.7.0/24 3 Vlan370 0.0.0.0 Push Up 0 </pre> Switch(config)#show mpls ftn-table detail

FTN Entry Detail Information

```

FTN ID          : 1
VrfIndex        : 0
Fec             : 30.1.1.224/32
Nexthop addr    : 42.1.7.1
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   : Vlan370
Admin Status    : Up
Oper Status     : Up
Oper Code       : Push
  
```

Printed information	Explanation
FEC ID	Forwarding Equivalent Class ID
FEC	Forwarding Equivalent Class Out Tag
Out-Lable	Next Hop Operator
Out-Intf	AC Side Status
Next Hop/Nexthop addr	Vrf-ID Source Priority Status
Oper-code	Exp Bit
Op-state/Oper status	Tunnel ID
Vrf/VrfIndex	Protocol Type
Owner	Qos, Resource ID
Primary	Entering Label
Row Status	Entering the User Side Status
Exp-Bits	Forwarding Equivalent Class ID
Incoming DSCP	Forwarding Equivalent Class Out Tag
Tunnel ID	Next Hop Operator
Protected LSP id	AC Side Status
Qos Resource id	Vrf-ID Source Priority Status
In-Label	Exp Bit
In-interface	Tunnel ID
Admin Status	Protocol Type

show mpls ilm

Command	show mpls ilm-table																																																								
Default	Not configured by default																																																								
Mode	All Mode																																																								
Usage	This Command displays the ILM table entry																																																								
Guide																																																									
Example	SwitchA(config)#show mpls ilm-table <table><thead><tr><th>In-Label</th><th>Out-Label</th><th>In-Intf</th><th>Out-Intf</th><th>Nexthop</th><th>FEC</th></tr></thead><tbody><tr><td>640</td><td>3</td><td>Vlan19</td><td>Vlan21</td><td>21.1.1.12</td><td>22.1.1.0/24</td></tr><tr><td>641</td><td>3</td><td>Vlan19</td><td>Vlan21</td><td>21.1.1.12</td><td>30.1.1.150/32</td></tr><tr><td>642</td><td>643</td><td>Vlan19</td><td>Vlan21</td><td>21.1.1.12</td><td>30.1.1.182/32</td></tr><tr><td>643</td><td>3</td><td>Vlan21</td><td>Vlan19</td><td>19.1.1.12</td><td>23.1.1.0/24</td></tr><tr><td>644</td><td>3</td><td>Vlan21</td><td>Vlan19</td><td>19.1.1.12</td><td>24.1.1.0/24</td></tr><tr><td>645</td><td>3</td><td>Vlan21</td><td>Vlan19</td><td>19.1.1.12</td><td>30.1.1.162/32</td></tr></tbody></table> <table><thead><tr><th>Printed information</th><th>Explanation</th></tr></thead><tbody><tr><td>In-Label</td><td>Incoming label</td></tr><tr><td>Out-Label</td><td>Outgoing label</td></tr><tr><td>In-Intf</td><td>Incoming interface</td></tr><tr><td>Out-Intf</td><td>Outgoing interface</td></tr><tr><td>Nexthop</td><td>Next hop</td></tr><tr><td>FEC</td><td>Forwarding equivalent</td></tr></tbody></table>	In-Label	Out-Label	In-Intf	Out-Intf	Nexthop	FEC	640	3	Vlan19	Vlan21	21.1.1.12	22.1.1.0/24	641	3	Vlan19	Vlan21	21.1.1.12	30.1.1.150/32	642	643	Vlan19	Vlan21	21.1.1.12	30.1.1.182/32	643	3	Vlan21	Vlan19	19.1.1.12	23.1.1.0/24	644	3	Vlan21	Vlan19	19.1.1.12	24.1.1.0/24	645	3	Vlan21	Vlan19	19.1.1.12	30.1.1.162/32	Printed information	Explanation	In-Label	Incoming label	Out-Label	Outgoing label	In-Intf	Incoming interface	Out-Intf	Outgoing interface	Nexthop	Next hop	FEC	Forwarding equivalent
In-Label	Out-Label	In-Intf	Out-Intf	Nexthop	FEC																																																				
640	3	Vlan19	Vlan21	21.1.1.12	22.1.1.0/24																																																				
641	3	Vlan19	Vlan21	21.1.1.12	30.1.1.150/32																																																				
642	643	Vlan19	Vlan21	21.1.1.12	30.1.1.182/32																																																				
643	3	Vlan21	Vlan19	19.1.1.12	23.1.1.0/24																																																				
644	3	Vlan21	Vlan19	19.1.1.12	24.1.1.0/24																																																				
645	3	Vlan21	Vlan19	19.1.1.12	30.1.1.162/32																																																				
Printed information	Explanation																																																								
In-Label	Incoming label																																																								
Out-Label	Outgoing label																																																								
In-Intf	Incoming interface																																																								
Out-Intf	Outgoing interface																																																								
Nexthop	Next hop																																																								
FEC	Forwarding equivalent																																																								

show mpls l2-vc

Command	show mpls l2-vc [<pw-id>]																																		
Parameter	pw-id <pw-id>		VPWS PW ID																																
Default	Not configured by default																																		
Mode	All Mode																																		
Usage	This Command displays the VPWS PW status																																		
Guide																																			
Example	Switch(config)#show mpls l2-vc <table><thead><tr><th>VC ID</th><th>State</th><th>Type</th><th>In Label</th><th>Out</th></tr><tr><th>Label</th><th>Endpoint</th><th></th><th></th><th></th></tr></thead><tbody><tr><td>300</td><td>Up</td><td>VLAN</td><td>1281</td><td>1281</td></tr><tr><td>30.1.1.224</td><td></td><td></td><td></td><td></td></tr></tbody></table> <table><thead><tr><th>Printed information</th><th>Explanation</th></tr></thead><tbody><tr><td>VC ID</td><td>PW ID</td></tr><tr><td>State</td><td>state</td></tr><tr><td>Type</td><td>PE packet encapsulation type</td></tr><tr><td>In Label</td><td>Incoming label</td></tr></tbody></table>					VC ID	State	Type	In Label	Out	Label	Endpoint				300	Up	VLAN	1281	1281	30.1.1.224					Printed information	Explanation	VC ID	PW ID	State	state	Type	PE packet encapsulation type	In Label	Incoming label
VC ID	State	Type	In Label	Out																															
Label	Endpoint																																		
300	Up	VLAN	1281	1281																															
30.1.1.224																																			
Printed information	Explanation																																		
VC ID	PW ID																																		
State	state																																		
Type	PE packet encapsulation type																																		
In Label	Incoming label																																		

Out Label	Outgoing label
Endpoint	Endpoint

show mpls ldp

Command	show mpls ldp {discovery fec neighbor parameter session}				
Parameter	discovery	Display sources for locally generated LDP Discovery Hello PDUs			
	fec	Forwarding Equivalence Class			
	neighbor	Display LDP neighbor information			
	parameter	Display LDP configuration parameters			
	session	LDP session list			
Default	Not configured by default				
Mode	All Mode				
Usage	This command displays information about the LDP protocol for the MPLS domain				
Guide					
Example	Switch(config)#show mpls ldp discovery				
	Interface	LDP Identifier	Label-Switching Capability	Merge	
	Loopback	30.1.1.130:0	Disabled	N/A	
	Vlan1	30.1.1.130:0	Disabled	N/A	
	Vlan370	30.1.1.130:0	Enabled	Merge capable	
	Loopback15	30.1.1.130:0	Disabled	N/A	
	Switch(config)#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
	NL	11.1.1.0/24	30.1.1.224	Impl-null	Invalid
	NL	13.1.1.0/24	30.1.1.224	Impl-null	Invalid
	NL	24.1.1.0/24	30.1.1.224	Impl-null	Invalid
	E >	30.1.1.130/32	Non-Existent	None	
	Connected				
	NL>	30.1.1.224/32	30.1.1.224	Impl-null	42.1.7.1
	E >	42.1.7.0/24	Non-Existent	None	
	Connected				
	NL>	42.1.7.0/24	30.1.1.224	Impl-null	Connected
	E >	192.168.2.0/24	Non-Existent	None	
	Connected				
	FEC Statistics: Total entry is 7				
	Switch(config)#show mpls ldp neighbor				
	IP Address	Intf Name	Holdtime	LDP-Identifier	

42.1.7.1 Vlan370 15 30.1.1.224:0

Switch(config)#show mpls ldp parameter
Router ID : 30.1.1.130
LDP Version : 1
Global Merge Capability : Merge Capable
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 Address : LabelSpace 0 : 30.1.1.130 (In Use)
Import BGP Routes : No

Switch(config)#show mpls ldp session
Peer IP Address IF Name My Role State KeepAlive
30.1.1.224 Vlan370 Passive OPERATIONAL 30

show ldp vpls

Command

show ldp vpls [{<vfi-id> | detail}]

<vfi-id>	VFI ID, specify the VFI instance information

detail	Detailed data

Default

Not configured by default

Mode

All Mode

Usage

This Command displays the session information of the PW in the VFI and can specify a VFI instance

Guide

Example

Switch(config)#show ldp vpls

VPLS 10, Encapsulation Vlan, MTU 1500, Peer number 1, Peers :

PW-ID	Peer Address	State	Type	Label-Sent
Label-Rcvd	Config			
10	30.1.1.224	Up	Vlan	1280

show ldp mpls-l2-circuit

Command	show ldp mpls-l2-circuit [{<pw-id> detail}]					
Parameter	<pw-id>		VPWS PW ID			
	detail		Details			
Default	Not configured by default					
Mode	All Mode					
Usage	This command displays the VPWS PW status and allows you to specify a					
Guide	PW					
Example	Switch(config)#show ldp mpls-l2-circuit					
	Transport	Client	VC	Trans	Local	Remote
	Destination	Config				
	VC ID	Binding	State	Type	VC Label	VC Label
	Address					
	300	None	Up	Vlan	1281	1281
	30.1.1.224	Yes				

show vpls

Command	show vpls [{<vfi-name> detail}]																													
	<table><tr><td><vfi-name></td><td colspan="5">VFI name</td></tr><tr><td>detail</td><td colspan="5">Details</td></tr></table>						<vfi-name>	VFI name					detail	Details																
<vfi-name>	VFI name																													
detail	Details																													
Default	Not configured by default																													
Mode	All Mode																													
Usage	This command displays the VFI instance information and allows you to specify a VFI instance																													
Guide																														
Example	Switch(config)#show vpls <table><tr><th>Name</th><th></th><th>VPLS-ID</th><th>VPLS-MTU</th><th>Type</th><th></th></tr><tr><th>Peers</th><th>State</th><th></th><th></th><th></th><th></th></tr><tr><td>v1</td><td></td><td>10</td><td>1500</td><td>VLAN</td><td>1</td></tr><tr><td>Active</td><td></td><td></td><td></td><td></td><td></td></tr></table> Switch(config)#show vpls detail Virtual Private LAN Service Instance: v1, ID: 10, State: Active Group ID: 0, VPLS Type: VLAN, Configured MTU: 1500 Description: none Mesh Peers: 30.1.1.224 Up						Name		VPLS-ID	VPLS-MTU	Type		Peers	State					v1		10	1500	VLAN	1	Active					
Name		VPLS-ID	VPLS-MTU	Type																										
Peers	State																													
v1		10	1500	VLAN	1																									
Active																														

show vpls fib

Command	show vpls fib [<vfi-name>]				
	<vfi-name>		VFI name		
Default	Not configured by default				
Mode	All Mode				
Usage	This Command displays the VFI forwarding entry, which allows you to				
Guide	specify a VFI instance				
Example	Switch(config)#show vpls fib				
	Vfi-Name	PW-ID	In Label	Out Label	Nexthop
		300	1281	1281	30.1.1.224
	v1	10	1280	1280	30.1.1.224

show vfi mac-address-table

Command	show vfi mac-address-table
Default	Not configured by default
Mode	All Mode
Usage	This CommandVPLS learned MAC
Guide	

show vpls peer

Command	show vpls peer <vfi-name> {mesh spoke}					
	<vfi-name>		VFI name			
	mesh		MeshMode			
	spoke		SpokeMode			
Default	Not configured by default					
Mode	All Mode					
Usage	This Command displays the PW of different modes in VFI					
Guide						
Example	Switch(config)#show vpls peer v1 mesh					
	PW-ID	Peer Addr	In-Intf	In-Label	Out-Intf	Out-
	Label	Lkps/St				
	10	30.1.1.224	Vlan370	1280	Vlan370	1280
	2/Up					

5 MPLS L3VPN Table

address-family ipv4

Command	address-family ipv4 [unicast vrf <vrf-name> multicast labeled-unicast]	
Parameter	<unicast>	Unicast address family factor
	<vrf-name>	VPN routing/forwarding instance name
	<multicast>	Address Family modifier
	<labeled-unicast>	Labeled Unicast Address Family modifier
Default	The BGP VPN address family is not created	
Mode	BGP configuration mode	
Usage Guide	Configure BGP VPN address families	
Example	The following shows how to create and access the BGP VPNv4 address family view Switch(config)#router bgp 65001 Switch (config-router)#address-family ipv4 vrf vpn1 Switch (config-router-af)#sho run cu	

address-family vpnv4

Command	address-family vpnv4	
Parameter	none	
Default	none	
Mode	BGP configuration mode	
Usage Guide	This command is used to create BGP VPNv4 address families and enter the BGP VPNv4 address family view.	
Example	The following shows how to create and access the BGP VPNv4 address family view Switch(config)#router bgp 100 Switch(config-router)#address-family vpnv4 Switch(config-router-af)#	

address-family vpnv4 unicast

Command	address-family vpnv4 unicast	
Parameter	none	
Default	none	
Mode	BGP configuration mode	

Usage Guide	This command is used to create BGP VPNv4 address families and enter the BGP VPNv4 address family view.
Example	The following shows how to create and access the BGP VPNv4 address family view <pre>Switch(config)#router bgp 100 Switch(config-router)#address-family vpnv4 unicast Switch(config-router-af)#</pre>

allocate-label all

Command	allocate-label all no allocate-label all
Parameter	All All declared routing
Default	Label application is not enabled
Mode	BGP configuration mode
Usage Guide	Request MPLS labels for all declarable prefix routes. Send-label is the ability to send labels, and allocate-label is the ability to request labels.
Example	The following demonstration shows how to apply for MPLS tags for IPv4 unicast prefix 1.1.1.1/32 <pre>Switch(config)#router bgp 100 Switch (config-router)#neighbor 11.0.0.2 remote-as 100 Switch (config-router)#allocate-label all Switch (config-router)#address-family ipv4 unicast Switch (config-router-af)#network 1.1.1.1/32 Switch (config-router-af)#exit-address-family Switch (config-router)#address-family ipv4 labeled-unicast Switch (config-router-af)#network 11.0.0.2 activate Switch (config-router-af)#exit-address-family</pre>

exit-address-family

Command	exit-address-family
Parameter	none
Default	none
Mode	BGP VPNv4 configuration mode
Usage Guide	This command is used to exit the BGP VPNv4 address family view.
Example	The following shows how to exit the BGP VPNv4 address family view <pre>Switch(config-router-af)#exit-address-family Switch(config-router)#</pre>

ip route

Command	ip route <Des tination_prefix> <Destination_prefix_mask> {vlan <Vlan_ID> IFNAME} <nexthop_address> <1~255> no ip route <Des tination_prefix> <Destination_prefix_mask> {vlan <Vlan_ID> IFNAME} <nexthop_address> <1~255>	
Parameter	<Destination_prerix >	Prefix of the routing destination
	<Destination_prefix_mask >	Prefix of the routing destination mask
	<Vlan_ID>	Output interface VLAN number
	IFNAME	Interface name
	<nexthop_address>	The next hop router interface address
	<1~255>	The management distance of the route
Default	None	
Mode	Global Mode	
Usage Guide	The global route table configures a static route to the VPN site, and the outbound interface is the interface bound to the VRF. This command is generally used to configure the route of the Internet access VPN on the PE in the network of VPN access to the Internet.	
Example	The target IP is 20.20.20.0, the mask is 24-bit, the port is vlan 9, and the next hop is 20.20.20.23. Switch(config)#ip route 20.20.20.0 255.255.255.0 vlan 9 20.20.20.23 Switch(config)#	

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>]	
Parameter	<vrf name>	VRF name
	<ip prefix>	Destination IP address
	<mask>	Subnet mask, dot decimal format
	prefix length	Prefix length
	gateway-address	Next hop address
	null0	Black hole routing
Default	<1-255>	Manage distance
	none	
Mode	Global Mode	
Usage Guide	To configure static routes for a specified VRF, you must first configure a successful VPN route forwarding instance before using this command.	
Example	Configure the static route of VRF A, the destination IP is 10.1.1.10, the mask is 24 bits,	

and the next hop is 10.1.1.1, and the Manage distance is default:

Switch(config)# ip route vrf VRF A 10.1.1.10 255.255.255.0 10.1.1.1

ip vrf <vrf-name>

Command	ip vrf <vrf-name>	
	no ip vrf <vrf-name>	
Parameter	<vrf-name>	The name of the configured VPN instance is set in the range of 1~64
Default	none	
Mode	Global Mode	
Usage Guide	Configure the VPN instance with the appropriate name. There is no default VPN instance on a PE, and multiple VPN instances can be created on a PE. The name of the VPN instance is case-sensitive. Need to pay attention. VPN instances take effect only when RD is configured.	
Example	Switch(config)#ip vrf VRF-A Switch(config-vrf)#:	

ip vrf forwarding vrfNAME

Command	ip vrf forwarding <vrfName>	
	no ip vrf forwarding <vrfName>	
Parameter	<vrf-name>	The name of the configured VPN instance is set in the range of 1~64
Default	none	
Mode	Interface Mode	
Usage Guide	If the interface needs to access the Internet, you can configure this command. An interface can only be bound to one VRF, and a VRF can be bound to multiple interfaces.	
Example	Switch(config)#int vlan 9 Switch(config-if-vlan9)#ip vrf forwarding vpn1	

neighbor A.B.C.D active

Command	Neighbor <ip-address> active	
	No neighbor <ip-address> active	
Parameter	<ip-adress >	The BGP neighbor address should be the Loopback port IP address on the neighbor switch

	<as-num> Specify the BGP neighbor AS number
Default	BGP neighbors are not created
Mode	BGP vpnv4 configuration Mode
Usage Guide	In BGP Routing Configuration Mode, IP unicast is configured. Under the specified address family configuration mode, configure whether to swap the specified address family. If either the local or peer side does not enable this option, the address family route on the local end cannot be obtained by the peer, even if the corresponding address family route is disabled, it will be canceled after the setting is disabled.
Example	The following shows how to create and access the BGP VPNv4 address family view Switch (config)#router bgp 100 Switch(config-router)#address family vpnv4 unicast Switch(config-router af)#neighbor 3.0.0.1 active Switch(config-router af)#

neighbor A.B.C.D remote-as

Command	Neighbor <ip-address> remote-as <as-num> No neighbor <ip-address> remote-as <as-num>
Parameter	<ip-address > The BGP neighbor address should be the Loopback port IP address on the neighbor switch <as-num> Specify the BGP neighbor AS number
Default	BGP neighbors are not created
Mode	BGP configuration mode
Usage Guide	Use the command to add a new neighbor without switching
Example	The following shows how to create and access the BGP VPNv4 address family view 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 A.B.C.D send-label

Command	Neighbor <A.B.C.D> send-label [explicit-null] No neighbor <A.B.C.D> send-label [explicit-null]
Parameter	<A.B.C.D> BGP neighbor Ipv4 address <explicit-null> The label value is 0, and the last hop carries a 0 label, which is used to convey information such as exp
Default	The BGP VPN address family is not created
Mode	BGP configuration mode
Usage Guide	Enable send-label neighbor A.B.C.D send-label with peer Enable send-label neighbor A.B.C.D send-label explicit-null for the peer to display empty label mode
Example	The following demonstrates the creation and entry into the BGP VPNv4 address family

Mode.
PE2#config
PE2(config)#router bgp 200
PE2(config-router)#neighbor 3.3.3.3 remote-as 200
PE2(config-router)#neighbor 3.3.3.3 update-source 3.3.3.3
PE2(config-router)#neighbor 3.3.3.3 send-label

mpls label mode vpnv4

Command	Mpls label mode vpnv4(all-vrfs vrf WORD)(per-prefix per-vrf) No mpls label mode vpnv4(all-vrfs vrf WORD)
Parameter	<all-vrfs> All VRF instances <vrf WORD> A specific VRF instance Per-prefix In the VRF instance, apply a different label for each prefix prefix Per-vrf In the VRF instance, apply for the same label for the VRF instance
Default	The default is per-prefixMode
Mode	Global Mode
Usage Guide	Assign labels to all VRFs or special VRFs according to different modes (per prefix or per Vrf).
Example	The following shows how to create and access the BGP VPNv4 address family view Switch(config)# mpls label mode vpnv4 vrf vpn1 per-vrf

rd

Command	rd <ASN:nn_or_IP-address:nn>
Parameter	<ASN:nn_or_IP-address:nn > The IP address format identified by the router. The ASN is AS in the range of 1 4294967295. It can be expressed in decimal as 6553700 or as a separator, such as 100.100. IP address is an IP address of 4 bytes; nn is any number of 2 bytes long.
Default	Not configured by default
Mode	Ip vrf Mode
Usage Guide	RD is used to uniquely identify VPN routes, and VPN instances can be used to achieve address space independence, which can overlap addresses between different VPNs. Typically the setup consists of an AS number and an arbitrary number. RD cannot be deleted directly.
Example	Switch (config)#ip vrf VRF-A Switch (config-vrf)# rd 300:3 Switch (config-vrf)#

route-target

Command	route-target {import export both} <rt-value> no route-target {import export both} <rt-value>

Parameter	import	This means that the route is filtered at the entrance, that is, whether the VPN route can join the VRF
	Export	Indicates the Route-Target that needs to be attached when the route of the VRF is sent outward as a VPNv4 route, which is used for ingress filtering.
	Both	It means that import and export use the same Route-Target value
	<rt-value>	Indicates the route target value.
Default	Not configured by default	
Mode	Ip vrf Mode	
Usage Guide	An RT is a BGP extension group that filters VPN routes and controls VPN membership and routing rules for directly connected sites. For the configured import rule, iterate through the routes received by all BGP processes, add eligible routes (the route's exportroute target intersects with the importroute target of this VRF), add it to the BGP process under the VRF, and issue a route update message to the BGP private network neighbor under the VRF. For the configured export rule, iterate through all the BGP routes stored in the BGP process associated with the VRF, add an exportroutetarget to these routes, and then issue a route update message to all public network neighbors. and publish routing updates to the bgp private neighbors under this VRF.	
Example	Switch (config)#ip vrf VRF-A Switch (config-vrf)# rd 300:3 Switch (config-vrf)#	

show ip bgp vpnv4 all

Command	show ip bgp vpnv4 all																						
Parameter	none																						
Default	none																						
Mode	Global Mode																						
Usage Guide	This command is used to display network reachability information for all VPNv4 address families.																						
Example	Here's a demonstration of all the VPNv4 information. Switch#show ip bgp vpnv4 all <table><thead><tr><th>Network</th><th>Next Hop</th><th>Metric</th><th>LocPrf</th><th>Weight</th><th>Path</th></tr></thead><tbody><tr><td colspan="6">Route Distinguisher: 100:1 (Default for VRF 1)</td></tr><tr><td>*> 10.1.1.0/24</td><td>0.0.0.0</td><td></td><td></td><td></td><td></td></tr></tbody></table>					Network	Next Hop	Metric	LocPrf	Weight	Path	Route Distinguisher: 100:1 (Default for VRF 1)						*> 10.1.1.0/24	0.0.0.0				
Network	Next Hop	Metric	LocPrf	Weight	Path																		
Route Distinguisher: 100:1 (Default for VRF 1)																							
*> 10.1.1.0/24	0.0.0.0																						

show ip bgp vpnv4 all A.B.C.D

Command	show ip bgp vpnv4 all A.B.C.D		
Parameter	A.B.C.D	Entries in BGP routes	

Default	none
Mode	Global Mode
Usage Guide	This command displays network reachability information for the VPNv4 address family where the specified BGP route is located.
Example	The following shows the VPNv4 information where the BGP route is located <pre>Switch#show ip bgp vpnv4 all 10.1.1.0 Route Distinguisher: 100:1 (Default for VRF 1) Local 0.0.0.0 from (0.0.0.0) Origin incomplete, localpref 100, weight 32768, valid, internal, best Extended Community: RT:10:10 Last update: 00:08:48</pre>

show ip bgp vpnv4 all tags

Command	show ip bgp vpnv4 all tags
Parameter	none
Default	none
Mode	Global Mode
Usage Guide	This command is used to display the BGP label corresponding to the prefix in the network reachability information of the VPNv4 address family.
Example	<pre>Switch#show ip bgp vpnv4 all tag Network Next Hop In Label/Out Label Route Distinguisher: 100:1 (Default for VRF 1) *> 10.1.1.0/24 0.0.0.0 -/aggregate(1)</pre>

show ip bgp vpnv4 vrf NAME

Command	show ip bgp vpnv4 vrf NAME
Parameter	NAME VPN routing/forwarding instance name
Default	none
Mode	Global Mode
Usage Guide	This command displays the network reachability information of the VPNv4 address family where the name of the specified VPN routing/forwarding instance is located.
Example	Displays the filtered VPN routing/forwarding instance entries <pre>Switch# show ip bgp vpnv4 vrf Network Next Hop Metric LocPrf Weight Path Route Distinguisher: 100:1 (Default for VRF 1) *> 10.1.1.0/24 0.0.0.0</pre>

show ip bgp vpnv4 vrf NAME A.B.C.D

Command	show ip bgp vpnv4 vrf NAME A.B.C.D	
Parameter	NAME	VPN routing/forwarding instance name
	A.B.C.D	Entries in BGP routes
Default	none	
Mode	Global Mode	
Usage Guide	This command displays the network reachability information of the VPNv4 address family in the name of the VPN routing/forwarding instance where the route entry is located.	
Example	Displays the filtered VPN routing/forwarding instance entries	
	Switch#show ip bgp vpnv4 vrf 1 10.1.1.1	
	Route Distinguisher: 100:1 (Default for VRF 1)	
	Local	
	0.0.0.0 from (0.0.0.0)	
	Origin incomplete, localpref 100, weight 32768, valid, internal, best	
	Extended Community: RT:10:10	
	Last update: 00:13:10	

show ip bgp vpnv4 vrf NAME label

Command	show ip bgp vpnv4 vrf NAME label	
Parameter	NAME	VPN routing/forwarding instance name
Default	none	
Mode	Global Mode	
Usage Guide	This command is used to display the network reachability information of the VPNv4 address family where the MPLS tag is specified in the name of the VPN routing/forwarding instance.	
Example	Displays the filtered VPN routing/forwarding instance entries	
	Switch# show ip bgp vpnv4 vrf 1 label	
	Network	Next Hop In Label/Out Label
	Route Distinguisher: 100:1 (Default for VRF 1)	
	*> 10.1.1.0/24	0.0.0.0 -/aggregate(1)

show ip bgp vpnv4 rd WORD

Command	show ip bgp vpnv4 rd WORD				
Parameter	WORD	Routing separator			
Default	none				
Mode	Global Mode				
Usage Guide	This command displays the network reachability information of the VPNv4 address family where the RD is located.				
Example	Displays the filtered VPN routing/forwarding instance entries				
	Switch# show ip bgp vpnv4 rd 100:1				
	Network	Next Hop	Metric	LocPrf	Weight Path
	Route Distinguisher: 100:1 (Default for VRF 1)				
	*> 10.1.1.0/24	0.0.0.0			32768 ?

show ip bgp vpnv4 rd WORD A.B.C.D

Command	show ip bgp vpnv4 rd WORD A.B.C.D	
Parameter	WORD	Routing separator
	A.B.C.D	Entries in BGP routes
Default	none	
Mode	Global Mode	
Usage Guide	This command displays the network reachability information of the VPNv4 address family where the specified IP address is located in the RD.	
Example	Displays the filtered VPN routing/forwarding instance entries Switch#show ip bgp vpnv4 rd 100:1 10.1.1.1 Route Distinguisher: 100:1 (Default for VRF 1) Local 0.0.0.0 from (0.0.0.0) Origin incomplete, localpref 100, weight 32768, valid, internal, best Extended Community: RT:10:10 Last update: 00:18:01	

show ip bgp vpnv4 rd WORD label

Command	show ip bgp vpnv4 rd WORD label		
Parameter	WORD	Routing separator	
Default	none		

Mode	Global Mode									
Usage Guide	This command displays the network reachability information of the VPNv4 address family where the specified label is located in the RD.									
Example	Displays the filtered VPN routing/forwarding instance entries Switch#show ip bgp vpnv4 rd 100:1 label <table><thead><tr><th>Network</th><th>Next Hop</th><th>In Label/Out Label</th></tr></thead><tbody><tr><td colspan="3">Route Distinguisher: 100:1 (Default for VRF 1)</td></tr><tr><td>*> 10.1.1.0/24</td><td>0.0.0.0</td><td>-/aggregate(1)</td></tr></tbody></table>	Network	Next Hop	In Label/Out Label	Route Distinguisher: 100:1 (Default for VRF 1)			*> 10.1.1.0/24	0.0.0.0	-/aggregate(1)
Network	Next Hop	In Label/Out Label								
Route Distinguisher: 100:1 (Default for VRF 1)										
*> 10.1.1.0/24	0.0.0.0	-/aggregate(1)								

show ip bgp vpnv4 all summary

Command	show ip bgp vpnv4 all summary																																																																
Parameter	none																																																																
Default	none																																																																
Mode	Global Mode																																																																
Usage Guide	This command is used to display a brief information about network reachability for all BGP VPNv4 address families.																																																																
Example	Displays filtered brief VPN routing/forwarding instance entries Switch#show ip bgp vpnv4 all summary BGP router identifier 2.2.2.2, local AS number 100 BGP table version is 2 1 BGP AS-PATH entries 0 BGP community entries <table><tr><th>Neighbor</th><th>V</th><th>AS</th><th>MsgRcvd</th><th>MsgSent</th><th>TblVer</th><th>InQ</th><th>OutQ</th></tr><tr><th>Up/Down</th><th>State/PfxRcd</th><th></th><th></th><th></th><th></th><th></th><th></th></tr><tr><td>3.3.3.3</td><td>4</td><td>100</td><td>30</td><td>31</td><td>2</td><td>0</td><td>0 00:28:22</td></tr><tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table> Total number of neighbors 1 BGP VRF 1 Route Distinguisher: 100:1 BGP table version is 1 1 BGP AS-PATH entries 0 BGP community entries <table><tr><th>Neighbor</th><th>V</th><th>AS</th><th>MsgRcvd</th><th>MsgSent</th><th>TblVer</th><th>InQ</th><th>OutQ</th></tr><tr><th>Up/Down</th><th>State/PfxRcd</th><th></th><th></th><th></th><th></th><th></th><th></th></tr><tr><td>10.1.1.1</td><td>4</td><td>65001</td><td>0</td><td>0</td><td>0</td><td>0</td><td>never</td></tr><tr><td>Active</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table> Total number of neighbors 1	Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd							3.3.3.3	4	100	30	31	2	0	0 00:28:22	0								Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd							10.1.1.1	4	65001	0	0	0	0	never	Active							
Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ																																																										
Up/Down	State/PfxRcd																																																																
3.3.3.3	4	100	30	31	2	0	0 00:28:22																																																										
0																																																																	
Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ																																																										
Up/Down	State/PfxRcd																																																																
10.1.1.1	4	65001	0	0	0	0	never																																																										
Active																																																																	

show ip bgp vpnv4 rd WORD summary

Command	show ip bgp vpnv4 rd WORD summary									
Parameter	WORD		Routing separator							
Default	none									
Mode	Global Mode									
Usage Guide	This command displays a brief information about the network reachability BGP neighbor of the VPNv4 address family where the RD is located.									
Example	Displays filtered brief VPN routing/forwarding instance entries									
	Switch#show ip bgp vpnv4 rd 100:1 summary									
	BGP router identifier 2.2.2.2, local AS number 100									
	BGP VRF 1 Route Distinguisher: 100:1									
	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								
	10.1.1.1	4	65001	0	0	0	0	0	never	
	Active									
	Total number of neighbors 1									

show ip bgp vpnv4 vrf NAME summary

Command	show ip bgp vpnv4 vrf NAME summary	
Parameter	NAME	VPN routing/forwarding instance name
Default	none	
Mode	Global Mode	
Usage Guide	This command displays a brief information about the network reachability of the VPNv4 address family where the vrf is located, and the BGP neighbor.	
Example	Displays filtered brief VPN routing/forwarding instance entries Switch#show ip bgp vpnv4 vrf 1 summary BGP router identifier 2.2.2.2, local AS number 100 BGP VRF 1 Route Distinguisher: 100:1 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						
10.1.1.1	4	65001	0	0	0	0	never
Active							
Total number of neighbors 1							

show ip bgp labeled-unicast

Command	show ip bgp labeled-unicast [vrf] [summary]									
Parameter	Vrf	vrf name								
Default	None									
Mode	All Mode									
Usage Guide	Display BGP unicast information									
	show ip bgp labeled-unicast									
	Display BGP unicast label and other information									
	show ip bgp labeled-unicast summary									
	Display unicast label routing information under BGP vrf									
	show ip bgp labeled-unicast vrf 1									
	Display unicast label and other information under BGP vrf									
	show ip bgp labeled-unicast vrf 1 summary									
Example	Switch(config-router)#show ip bgp labeled-unicast summary									
	BGP router identifier 10.1.1.1, local AS number 100									
	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									
	1.1.1.1	4	100	127	151	1	0	0 02:05:39	0	
	15.1.1.2	4	200	24	47	1	0	0 00:22:24	0	
Total number of neighbors 2										
Switch(config-router)#show ip bgp labeled-unicast										
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S - stale										
	Network		Next Hop		In Label		Out Label			
*>	1.1.1.1/32		13.1.1.2		17(Vlan200)		3			
Switch(config-router)#										

show ip route vrf

Command	show ip route vrf <vrf-name> [bgp database]

Parameter	< vrf-name > VRF name
	< bgp > Represents routes introduced through BGP
	< database> IP routing table database
Default	None
Mode	All Mode
Usage Guide	Can be displayed for a specified routing protocol
Example	<pre> PE1(config)#show ip route vrf 1 bgp B 24.1.1.0/24 [200/0] via 30.1.1.182,00:03:57 tag:0 B 30.1.1.162/32 [200/0] via 30.1.1.182,00:03:57 tag:0 B 30.1.1.169/32 [20/0] via 21.1.1.1,vlan21,03:42:28 tag:0 Total routes are : 3 item(s) PE1(config)#show ip route vrf l database Codes:K-kernel,c-connected,S static,R- RIP,B- BGP 0- 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 *> 21.1.1.0/24 is directly connected, vlan21 tag:0 C *> 21.1.1.12/32 is local host, vlan21 tag:0 B *> 24.1.1.0/24 [200/0] via 30.1.1.182,00:04:02 tag:0 B *> 30.1.1.162/32 [200/0] via 30.1.1.182, 00:04:02 tag:0 B *> 30.1.1.169/32 [20/0] via 21.1.1.1,vlan21,03:42:33 tag:0 Total routes are : 4 item(s) </pre>

show ip vrf

Command	show ip vrf <vrf-name>
Parameter	< vrf-name > Vrf name
Default	None
Mode	All Mode
Usage Guide	This Command also exists in other routing protocols, and information about other routing protocol processes related to the VPN routing forwarding instance using this Command is also displayed.
Example	<pre> PE1(config)#show ip vrf 1 VRF 1, VRF ID:1,FIB ID 1 Router ID: 21.1.1.12 (automatic) Interfaces : Vlan21 VRF 1:(id=1): RIP is not enabled VRF 1:(id=1); OSPF is not enabled VRF 1:(id=1); BGP enabled IRF 1: default RD 100:1 Interfaces: Vlan21 Export VPN route-target communities RT:100:1 </pre>

```

Import VPN route-target communities
  RT:100:1
No import route-map
No export route-map
VPNv4 label allocation mode: per-prefix
PE1(config)#

```

6 Commands for Rsvp Configuration

router rsvp

Command	router rsvp no router rsvp
Parameter	- -
Default	By default, the RSVP protocol is not enabled
Mode	config
Usage Guide	This command can enable the rsvp protocol to support rsvp-related configurations No Command to deactivate the rsvp protocol.
Example	# config terminal (config)# router rsvp

enable-rsvp

Command	enable-rsvp disable-rsvp
Parameter	-
Default	Default the RSVP function is not enabled under the VLAN interface
Mode	vlan interface Mode
Usage Guide	This Command is used to enable the rsvp feature on the vlan interface disable-rsvp is used to deenable the rsvp feature

Example	<pre># config terminal (config)# interface vlan 1 (config-if-vlan1)#enable-rsvp</pre>

rsvp-trunk

Command	rsvp-trunk TRUNKNAME no rsvp-trunk TRUNKNAME
Parameter	TRUNKNAME The name of the user-created tunnel
Default	Default the created tunnel does not exist
Mode	Config
Usage Guide	This Command is used to create an rsvp te tunnel and the no form is used to delete the rsvp te tunnel
Example	<pre># config terminal (config)# rsvp-trunk t1</pre>

rsvp-path

Command	rsvp-path PATHNAME no rsvp-path PATHNAME
Parameter	PATHNAME The name of the user-created path
Default	Default path name does not exist
Mode	config
Usage Guide	This Command is used to create an explicit path for rsvp te and the no form is used to delete an explicit path for rsvp te
Example	<pre># config terminal (config)# rsvp-path p1</pre>

reservable-bandwidth

Command	reservable-bandwidth BANDWIDTH no reservable-bandwidth
Parameter	BANDWIDTH Reserve bandwidth
Default	By default, there is no reserved bandwidth configuration
Mode	vlan interface Mode
Usage Guide	This command is used to set the reserved bandwidth under interface, and the no form is used to calculate the RSVP path
Example	<pre># config terminal (config)# interface vlan 1 (config)#reservable-bandwidth 500</pre>

A.B.C.D loose

Command	A.B.C.D loose no A.B.C.D loose
Parameter	A.B.C.D Configure the IP address that the path needs to pass through
Default	There is no explicit path configuration by Default
Mode	rsvp-pathMode
Usage Guide	Loosely configured explicit paths, and the IP address needs to be unconfigured in the form of no link to pass
Example	<pre># config terminal (config)# rsvp-path p1 (config)# 3.1.1.2 loose</pre>

A.B.C.D strict

Command	A.B.C.D strict no A.B.C.D strict
Parameter	A.B.C.D Configure the IP address that the path needs to pass through
Default	There is no explicit path configuration by default
Mode	rsvp-pathMode
Usage Guide	Configure a strict explicit path and the link that the IP address needs to pass through
Example	<pre># config terminal (config)# rsvp-path p1 (config)# 3.1.1.2 strict</pre>

ext-tunnel-id A.B.C.D

Command	ext-tunnel-id A.B.C.D no ext-tunnel-id
Parameter	A.B.C.D ID of the tunnel extension
Default	The default identification uses LSR-ID
Mode	rsvp-trunk
Usage Guide	The Command is used to configure the id of the tunnel extension, identifying the no form and restoring the Default
Example	<pre># config terminal (config)# rsvp-trunk t1 (config-trunk)# ext-tunnel-id 1.1.1.30</pre>

from A.B.C.D

Command	from A.B.C.D no from	
Parameter	A.B.C.D	The IPv4 address of the tunnel incoming interface
Default	The default tunnel does not have an incoming interface address configuration	
Mode	rsvp-trunk Mode router-rsvp	
Usage Guide	The Command is used to configure the tunnel entrance of ipv4, and the no form is used to cancel the tunnel incoming interface address configuration	
Example	# config terminal (config)#rsvp-trunk t1 (config-trunk)#from 1.1.1.9 #configure terminal (config)#router rsvp (config-router)#from 1.1.1.9	

to A.B.C.D

Command	to A.B.C.D no to	
Parameter	A.B.C.D	The IPv4 address of the tunnel outgoing interface
Default	The default tunnel does not have an outgoing interface address configuration	
Mode	rsvp-trunk Mode	
Usage Guide	This command is used to configure the tunnel entrance of ipv4, and the no form is used to cancel the tunnel outgoing interface address configuration	
Example	# config terminal (config)#rsvp-trunk t1 (config-trunk)#to 1.1.1.19	

map-route A.B.C.D

Command	map-route <A.B.C.D A.B.C.D/M> no map-route <A.B.C.D A.B.C.D/M>	
Parameter	A.B.C.D	Prefix to be mapped
	A.B.C.D/M	Prefix to be mapped, plus mask
Default	The default tunnel does not have a mapped routing configuration	
Mode	rsvp-trunk Mode	
Usage Guide	The Command is used to configure the route mapping and the no form is used to unmap	
Example	# config terminal (config)#rsvp-trunk t1 (config-trunk)#map-route 1.1.1.19	

primary cspf

Command	primary cspf primary no-cspf	
Parameter	-	
Default	By default, CSPF is used	
Mode	rsvp-trunk Mode	
Usage Guide	The Command is used to configure the main link to use the cspf algorithm, and no-cspfParameter is used to cancel the cspf algorithm for the main link	
Example	# config terminal (config)#rsvp-trunk t1 (config-trunk)#primary cspf	

secondary cspf

Command	secondary cspf secondary no-cspf
Parameter	-
Default	By default, CSPF is used
Mode	rsvp-trunk Mode
Usage Guide	The Command is used to configure the standby link to use the cspf algorithm, and no-cspfParameter is used to cancel the cspf algorithm for the standby link
Example	<pre># config terminal (config)#rsvp-trunk t1 (config-trunk)#secondary cspf</pre>

primary bandwidth

Command	primary bandwidth BANDWIDTH no primary bandwidth
Parameter	BANDWIDTH Main link bandwidth attribute value
Default	The default primary link bandwidth is 0
Mode	rsvp-trunk Mode
Usage Guide	The Command is used to configure the main link bandwidth attribute value and the no form is used to cancel the bandwidth configuration for the main link
Example	<pre># config terminal (config)#rsvp-trunk t1 (config-trunk)#primary bandwidth 500</pre>

secondary bandwidth

Command	primary bandwidth BANDWIDTH no primary bandwidth
Parameter	BANDWIDTH The bandwidth value of the standby link
Default	The default standby link bandwidth is 0
Mode	rsvp-trunk Mode
Usage Guide	The Command is used to configure the standby link bandwidth attribute value of no to cancel the bandwidth configuration of the standby link
Example	<pre># config terminal (config)#rsvp-trunk t1 (config-trunk)#secondary bandwidth 500</pre>

primary path

Command	primary path PATHNAME no primary path
Parameter	PATHNAME Explicit path name
Default	By default, the standby link does not use an explicit path, but uses CSPF to calculate the path
Mode	rsvp-trunk Mode
Usage Guide	The Command is used to configure the explicit path of the main link, and the no form is used to cancel the explicit path configuration of the main link and restore the default
Example	<pre>#config terminal (config)#rsvp-trunk t1 (config-trunk)#primary path p1</pre>

secondary path

Command	Secondary path PATHNAME no secondary path
Parameter	PATHNAME Explicit path name
Default	The default unspare link configuration
Mode	rsvp-trunk Mode
Usage Guide	The Command is used to configure the standby explicit path, and the no form is used to deconfigure the alternate link
Example	<pre># config terminal (config)#rsvp-trunk t1 (config-trunk)#secondary path p2</pre>

rsvp-trunk-restart

Command	rsvp-trunk-restart
Parameter	-
Default	The default session is functioning normally
Mode	rsvp-trunk Mode
Usage Guide	This Command is used to restart the session of the rsvp trunk
Example	<pre># config terminal (config)#rsvp-trunk t1 (config-trunk)#rsvp-trunk-restart</pre>

primary cspf-retry-limit

Command	primary cspf-retry-limit <1-65535> no primary cspf-retry-limit
Parameter	<1-65535> Number of reattempts

Default	The default number of attempts is unlimited
Mode	rsvp-trunk Mode
Usage Guide	The Command is used to set the number of LSP attempts on the main link cspf in the form of no is used to remove the throttle and restore the default value
Example	<pre># config terminal (config)#rsvp-trunk t1 (config-trunk)#no primary cspf-retry-limit 20</pre>

secondary cspf-retry-limit

Command	<pre>secondary cspf-retry-limit <1-65535> no secondary cspf-retry-limit</pre>		
	<table> <tr> <td><1-65535></td><td>Number of reattempts</td></tr> </table>	<1-65535>	Number of reattempts
<1-65535>	Number of reattempts		
Default	The default number of retries is unlimited		
Mode	rsvp-trunk Mode		
Usage Guide	The Command is used to set the number of times the spare link cspf attempts to lsp, and the no form is used to remove the restriction and restore the default value		
Example	<pre># config terminal (config)#rsvp-trunk t1 (config-trunk)#no secondary cspf-retry-limit 20</pre>		

primary cspf-retry-timer

Command	<pre>primary cspf-retry-timer <1-600> no primary cspf-retry-timer</pre>		
Parameter	<table> <tr> <td><1-600></td><td>Retry interval</td></tr> </table>	<1-600>	Retry interval
<1-600>	Retry interval		
	-		
Default	The default CSPF retry interval is 30 seconds		
Mode	rsvp-trunk Mode		

Usage Guide	The Command is used to specify the retry interval for this LSP to perform CSPF calculations in the form of no, which is used to remove the restriction and restore the default value
Example	<pre># config terminal (config)#rsvp-trunk t1 (config-trunk)#no primary cspf-retry-timer 10</pre>

secondary cspf-retry-timer

Command	<pre>secondary cspf-retry-timer <1-65535> no secondary cspf-retry-timer</pre>
Parameter	<pre><1-600></pre> Retry interval
Default	The default CSPF retry interval is 30 seconds
Mode	rsvp-trunk Mode
Usage Guide	The Command is used to specify the Retry interval of this LSP to perform CSPF calculations in the form of no, which is used to remove the restriction and restore the default value
Example	<pre># config terminal (config)#rsvp-trunk t1 (config-trunk)#no secondary cspf-retry-timer 10</pre>

primary retry-limit

Command	<pre>primary retry-limit <1-65535> no primary retry-limit</pre>
Parameter	<pre><1-65535></pre> Number of reattempts
Default	The default number of attempts is unlimited
Mode	rsvp-trunk Mode

Usage Guide	The Command is used to set the Number of reattempts no form of the main link lsp, which is used to remove the restriction and restore the default value
Example	<pre># config terminal (config)#rsvp-trunk t1 (config-trunk)#no primary retry-limit 20</pre>

secondary retry-limit

Command	<pre>secondary retry-limit <1-65535> no secondary retry-limit</pre>		
	<table> <tr> <td><1-65535></td><td>Number of reattempts</td></tr> </table>	<1-65535>	Number of reattempts
<1-65535>	Number of reattempts		
Default	The default number of reattempts is unlimited		
Mode	rsvp-trunk Mode		
Usage Guide	The Command is used to set the Number of reattempts no form of the standby link lsp, which is used to cancel the restriction and restore the default value		
Example	<pre># config terminal (config)#rsvp-trunk t1 (config-trunk)#no secondary retry-limit 20</pre>		

primary cretry-timer

Command	<pre>primary retry-timer <1-600> no primary retry-timer</pre>		
Parameter	<table> <tr> <td><1-600></td><td>Timeout in seconds between successive Path message retries</td></tr> </table>	<1-600>	Timeout in seconds between successive Path message retries
<1-600>	Timeout in seconds between successive Path message retries		
	-		
Default	The default lsp Retry interval is 30 seconds		
Mode	rsvp-trunk Mode		
Usage Guide	Configures the retry timer for the primary LSP path. The timer specifies the interval in seconds between successive Path message retries when establishing an RSVP session.		
Example			

	<pre># config terminal (config)#rsvp-trunk t1 (config-trunk)#primary retry-timer 10</pre>

primary cspf-retry-timer

Command	<pre>primary cspf-retry-timer <1-600> no primary cspf-retry-timer</pre>
Parameter	<1-600> Retry interval
Default	The default lsp Retry interval is 30 seconds
Mode	rsvp-trunk Mode
Usage Guide	The Command specifies the Retry interval of this LSP to establish an rsvp session in the form of no to remove the restriction and restore the default value
Example	<pre># config terminal (config)#rsvp-trunk t1 (config-trunk)#primary cspf-retry-timer 10</pre>

primary record

Command	<pre>primary record primary no-record</pre>
Parameter	- -
Default	Default primary LSP enables path recording (RRO)
Mode	rsvp-trunk Mode
Usage Guide	The command records the path message path information of the main lsp, which can be viewed in the form of no through show rsvp session detail to cancel the record, and the actual path is not visible
Example	<pre># config terminal (config)#rsvp-trunk t1</pre>

(config-trunk)#primary record

secondary record

Command	secondary record secondary no-record
Parameter	- -
Default	Default LSP Enabled Path Recording (RRO)
Mode	rsvp-trunk Mode
Usage Guide	The command records the path message path information of the configurable lsp, which can be viewed in the form of no by show rsvp session detail to cancel the record, and the actual path is not visible
Example	# config terminal (config)#rsvp-trunk t1 (config-trunk)#secondary record

primary affinity

Command	primary affinity primary no-affinity
Parameter	- -
Default	By default, the primary LSP does not enable carrying resource information
Mode	rsvp-trunk Mode
Usage Guide	The Command is used to disable the function and restore the Default to the Session Attribute object that sends session attribute objects with resource dependency data with the enabled no-affinity of the configuration master
Example	# config terminal (config)#rsvp-trunk t1 (config-trunk)#primary affinity

secondary affinity

Command	secondary affinity secondary no- affinity
Parameter	- -
Default	By default, the backup LSP does not enable carrying resource information
Mode	rsvp-trunk Mode
Usage Guide	The Command is used to disable the function and restore the Default to the Session Attribute object that sends session attribute objects with resource dependency data with the enabled no-affinity of the configuration master
Example	# config terminal (config)#rsvp-trunk t1 (config-trunk)#secondary affinity

primary hop-limit

Command	primary hop-limit <1-255> primary hop-limit
Parameter	<1-255> The number of jumps is limited -
Default	By default, the primary LSP does not set a next hop limit
Mode	rsvp-trunk Mode
Usage Guide	The Command is used to limit the number of hops in the main lsp in the form of no to cancel the restriction and restore Default
Example	# config terminal (config)#rsvp-trunk t1 (config-trunk)#primary hop-limit 5

secondary hop-limit

Command	primary hop-limit <1-255> primary hop-limit
Parameter	<1-255> -
Default	By default, the backup LSP does not set a next hop limit
Mode	rsvp-trunk Mode
Usage Guide	The Command is used to limit the number of hops in the main lsp in the form of no to cancel the restriction and restore Default
Example	# config terminal (config)#rsvp-trunk t1 (config-trunk)#secondary hop-limit 5

update-type

Command	update-typet break-before-make update-typet make-before-break
Parameter	break-before-make BBM session refresh mode make-before-break MBB session refresh mode
Default	MBBMode is used by default
Mode	rsvp-trunk Mode
Usage Guide	The command uses the configuration tunnel session to refresh the mode, MBB and BBM are the new session is ready first and then the original session is interrupted, and the other is to directly disconnect and then create a new session
Example	# config terminal (config)#rsvp-trunk t1 (config-trunk)#update-type break-before-make

ack-wait-timeout

Command	ack-wait-timeout <1-65535> no ack-wait-timeout
Parameter	<1-65535> Confirm the message timeout time value -
Default	The default timeout value is 10
Mode	router-rsvp Mode
Usage Guide	The Command is used to configure the inter-session confirmation message timeout time value of no to cancel the user restriction and restore the default
Example	# config terminal (config)#router rsvp (config-router)# ack-wait-timeout 20

php

Command	php no-php
Parameter	- -
Default	php is used by default
Mode	router-rsvp Mode
Usage Guide	The command pops up the penultimate jump of the mpls tag in the rsvp-te protocol, and cancels the default if no-php pops up, and the penultimate one does not pop up
Example	# config terminal (config)#router rsvp (config-router)#no-php

cspf

Command	cspf no-cspf
Parameter	- -
Default	Enable CSPF by default
Mode	router-rsvp Mode
Usage Guide	The command is used to configure rsvp to enable cspf no form, which is used to configure rsvp, and cspf is not applicable
Example	# config terminal (config)#router rsvp (config-trunk)#cspf

show rsvp

Command	show rsvp
Parameter	- -
Default	None
Mode	All Mode
Usage Guide	This command is used to display rsvp protocol information
Example	# show rsvp RSVP Version : 1 Process uptime : 32 minutes RSVP Refresh Reduction : Enabled RSVP Message Acknowledgement : Disabled Bundle Send : Disabled NSM Connection : Up

CSPF Connection	: Down
CSPF usage	: Disabled
RSVP Refresh Timer	: 30
Keep Multiplier	: 3
Acknowledgement Await Timeout	: 10
Explicit-Null For Direct Conn	: Disabled
Local Protection	: Disabled
Hello Receipt	: Disabled
Hello Interval	: 2
Hello Timeout	: 7
Loop detection	: Enabled (all interface)
Ingress	: 1.1.1.9
Penultimate Hop Popping	: Enabled
Refresh PATH msg parsing	: Enabled
Refresh RESV msg parsing	: Enabled

show rsvp session

Command	show rsvp session show rsvp session up show rsvp session up detail show rsvp session down show rsvp session down detail
Parameter	up UP session down Sessions without UP
Default	None
Mode	All Mode
Usage Guide	This command is used to display rsvp protocol information
Example	<pre># show rsvp session detail Ingress (Primary) 10.10.21.3 From: 1.1.1.1, LSPstate: Up, LSPname: t1 Setup priority: 5, Hold priority: 5 CSPF usage: Disabled LSP Protection: None Label in: -, Label out: 16, Tspec rate: 10m, Fspec rate: 10m Tunnel Id: 1, LSP Id: 2, Ext-Tunnel Id: 1.1.1.1 Downstream: 10.10.23.2, eth0</pre>

	Path refresh: 5 seconds (due in 6772 seconds) Resv lifetime: 26 seconds (due in 25 seconds) Retry count: 0, intrvl: 30 seconds RRO re-use as ERO: Disabled Label Recording: Disabled Admin Groups: none Configured Path: p1 (in use) Configured Explicit Route Detail : 10.10.23.2/32 strict Session Explicit Route Detail : 10.10.23.2/32 strict Record route: <self> 10.10.23.2 10.10.21.3 Style: Shared Explicit Filter Traffic type: controlled-load Minimum Path MTU: 1500 LSP Type: ELSP_SIGNAL CLASS DSCP_value EXP_value

7 Commands for MPLS QOS

cos-exp mapping

Command	mls qos map cos-exp <0-7> to <0-7>																															
Parameter	COS-EXP	COS and EXP mapping tables																														
	<0-7>	COS Priority																														
	<0-7>	EXP Priority																														
Default	Not configured by default																															
Mode	CONFIG_MODE																															
Usage Guide	This Command is used to configure the COS-EXP Priority mapping table. By default, COS Priority 0-7 are mapped to EXP 0, that is, COS and EXP have no mapping relationship, and the COS-EXP relationship table can be set to 0 by unconfiguring																															
Example	The switch is configured with COS Priority2 mapped to EXP Priority3 <pre>Switch(config)#mls qos map cos-exp 2 to 3 Switch(config)#show mls qos maps cos-exp</pre> Ingress COS-TO-EXP map: <table><tr><td>COS: 0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr><tr><td colspan="8">-----</td></tr><tr><td>EXP: 0</td><td>0</td><td>3</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr></table>								COS: 0	1	2	3	4	5	6	7	-----								EXP: 0	0	3	0	0	0	0	0
COS: 0	1	2	3	4	5	6	7																									

EXP: 0	0	3	0	0	0	0	0																									

dscp-exp mapping

Command	mls qos map dscp-exp <0-63> to <0-7>										
Parameter	DSCP-EXP	DSCP and EXP mapping tables									
	<0-63>	DSCP Priority									
	<0-7>	EXP Priority									
Default	Not configured by default										
Mode	CONFIG_MODE										
Usage Guide	This Command is used to configure the DSCP-EXP Priority mapping table. By default, DSCP Priority0-63 is mapped to EXP 0, that is, DSCP-EXP mapping is not enabled, and the DSCP-EXP relationship table can be set to 0 by unconfiguring										
Example	The switch is configured with DSCP Priority10 mapped to EXP Priority2										
	Switch(config)#mls qos map dscp-exp 10 to 2										
	Switch(config)#show mls qos maps cos-exp										
	Ingress DSCP-TO-EXP map:										
	DSCP:EXP	0	1	2	3	4	5	6	7	8	9
	0:	0	0	0	0	0	0	0	0	0	0
	1:	2	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							

exp-exp mapping

Command	mls qos map exp-exp <0-7> to <0-7>						
Parameter	<table> <tr> <td>EXP-EXP</td><td>EXP and EXP mapping tables</td></tr> <tr> <td><0-7></td><td>EXP Priority</td></tr> <tr> <td><0-7></td><td>EXP Priority</td></tr> </table>	EXP-EXP	EXP and EXP mapping tables	<0-7>	EXP Priority	<0-7>	EXP Priority
EXP-EXP	EXP and EXP mapping tables						
<0-7>	EXP Priority						
<0-7>	EXP Priority						
Default	Not configured by default						
Mode	CONFIG_MODE						
Usage	This command is used to configure the EXP-EXP Priority mapping table						

Guide	By default, EXP Priority0-7 is mapped to EXP 0, that is, EXP does not have EXP-EXP mapping enabled, and the EXP-EXP table can be set to 0 by deconfiguring it
Example	The switch configuration is mapped to EXP Priority2 to EXP Priority6 Switch(config)#mls qos map exp-exp 2 to 6 Switch(config)#show mls qos maps exp-exp

```

Ingress EXP-TO-EXP map:
EXP: 0   1   2   3   4   5   6   7
-----
EXP: 0   0   6   0   0   0   0   0

```

exp-intp mapping

Command	mls qos map exp-intp <0-7><0-7><0-7><0-7><0-7><0-7><0-7><0-7>				
Parameter	<table> <tr> <td>EXP-INTP</td><td>EXP and internal Priority mapping tables</td></tr> <tr> <td><0-7></td><td>Internal Priority</td></tr> </table>	EXP-INTP	EXP and internal Priority mapping tables	<0-7>	Internal Priority
EXP-INTP	EXP and internal Priority mapping tables				
<0-7>	Internal Priority				
Default	Not configured by default				
Mode	CONFIG_MODE				
Usage Guide	This command is used to configure the EXP-INTP mapping table. The default EXP Priority0-7 are mapped to INTP 0, that is, EXP is mapped to INTP Priority0, and the EXP-INTP table can be set to 0 by unconfiguring				
Example	The switch is configured with EXP Priority mapping 0-7 mapping to INTP internal Priority 4 Switch(config)#mls qos map exp-intp 4 4 4 4 4 4 4 4 Switch(config)#show mls qos maps exp-intp Ingress EXP-TO-Internal-Priority map: <pre> EXP: 0 1 2 3 4 5 6 7 ----- INTP: 4 4 4 4 4 4 4 4 </pre>				

exp-dp mapping

Command	mls qos map exp-dp <0-2><0-2><0-2><0-2><0-2><0-2><0-2><0-2>				
Parameter	<table> <tr> <td>EXP-DP</td><td>EXP and discard the Priority mapping table</td></tr> <tr> <td><0-2></td><td>Discard Priority</td></tr> </table>	EXP-DP	EXP and discard the Priority mapping table	<0-2>	Discard Priority
EXP-DP	EXP and discard the Priority mapping table				
<0-2>	Discard Priority				
Default	Not configured by default				

Mode	CONFIG_MODE
Usage Guide	This Command is used to configure the EXP-DP mapping table. By default, EXP Priority 0-7 are mapped to DP 0, and the EXP-DP table can be set to 0 by unconfiguring.
Example	The switch is configured with EXP Priority mapping 4-7 mapped to DP Priority 2 <pre>Switch(config)#mls qos map exp-dp 0 0 0 0 2 2 2 2 Switch(config)#show mls qos maps exp-dp Ingress EXP-TO-Drop-Precedence map: EXP: 0 1 2 3 4 5 6 7 ----- DP: 0 0 0 0 2 2 2 2</pre>

8 Commands For Send-label

show ip bgp labeled-unicast

Command	show ip bgp labeled-unicast [vrf] [summary]																																																							
Parameter	Vrf	vrf name																																																						
Default																																																								
Mode																																																								
Usage Guide	Display BGP thin label pair routing information show ip bgp labeled-unicast Display BGP unicast label and other information show ip bgp labeled-unicast summary Display unicast label routing information under BGP vrf show ip bgp labeled-unicast vrf 1 Display unicast label and other information under BGP vrf show ip bgp labeled-unicast vrf 1 summary																																																							
Example	Switch(config-router)#show ip bgp labeled-unicast summary BGP router identifier 10.1.1.1, local AS number 100 BGP table version is 1 1 BGP AS-PATH entries 0 BGP community entries <table><thead><tr><th>Neighbor</th><th>V</th><th>AS</th><th>MsgRcvd</th><th>MsgSent</th><th>TblVer</th><th>InQ</th><th>OutQ</th></tr><tr><th>Up/Down</th><th>State/PfxRcd</th><th></th><th></th><th></th><th></th><th></th><th></th></tr></thead><tbody><tr><td>1.1.1.1</td><td>4</td><td>100</td><td>127</td><td>151</td><td>1</td><td>0</td><td>0 02:05:39</td></tr><tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>15.1.1.2</td><td>4</td><td>200</td><td>24</td><td>47</td><td>1</td><td>0</td><td>0 00:22:24</td></tr><tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></tbody></table> Total number of neighbors 2								Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd							1.1.1.1	4	100	127	151	1	0	0 02:05:39	0								15.1.1.2	4	200	24	47	1	0	0 00:22:24	0							
Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ																																																	
Up/Down	State/PfxRcd																																																							
1.1.1.1	4	100	127	151	1	0	0 02:05:39																																																	
0																																																								
15.1.1.2	4	200	24	47	1	0	0 00:22:24																																																	
0																																																								

```
Switch(config-router)#show ip bgp labeled-unicast
```

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S - stale

	Network	Next Hop	In Label	Out Label
*>	1.1.1.1/32	13.1.1.2	17(Vlan200)	3

```
Switch(config-router)#
```

neighbor A.B.C.D send-label

Command	neighbor <A.B.C.D> send-label [explicit-null]

Parameter	<A.B.C.D> BGP neighbor ipv4 address

Default	

Mode	Config Mode

Usage Guide	Enable send-label

neighbor A.B.C.D send-label with peer

Enable send-label

neighbor A.B.C.D send-label explicit-null for the peer to display empty label mode

Example	PE2#config

```
PE2(config)#router bgp 200
```

```
PE2(config-router)#neighbor 3.3.3.3 remote-as 200
```

```
PE2(config-router)#neighbor 3.3.3.3 update-source 3.3.3.3
```

```
PE2(config-router)#neighbor 3.3.3.3 send-label
```
